Facultad de Ciencias Sociales y Jurídicas

Grado en Derecho

Universidad de Jaén
Facultad de Ciencias Sociales y Jurídicas

Trabajo Fin de Grado

LA PROTECCIÓN DE DATOS EN LAS RELACIONES LABORALES

Alumna: Eva Martos Gouissem

Mayo, 2022

RESUMEN

La finalidad del presente trabajo, realiza un estudio sobre el tratamiento de los datos, proyectado en la protección de datos en un entorno laboral. Destaca el Reglamento General de Protección de Datos, desde un ámbito Europeo, en el que todas las empresas deben de estar sometidas a dicho Reglamento, y por tanto, se analiza el control y seguridad para minimizar los riesgos que puedan sufrir los datos de carácter personal.

PALABRAS CLAVE: Protección de datos, ámbito laboral, RGPD, riesgos, tratamiento de datos, seguridad.

ABSTRACT

The purpose of this work, carries out a study on the treatment of data, projected in the protection of data in a work environment. It highlights the General Data Protection Regulation, from a European scope, in which all companies must be subject to this Regulation, and therefore, it analyses the control and security to minimise the risks that personal data may suffer.

KEYWORDS: Data protection, work environment, GDPR, risks, data processing, security.

ÍNDICE

1. INTRODUCCIÓN: LA PROTECCIÓN DE DATOS EN EL ÁMBITO LABORAL.

1.1. CONCEPTO, FUNCIÓN Y CONTENIDO SOBRE LA PROTECCIÓN DE DATOS.

La evolución de la protección de datos surge como respuesta al avance de la informática y de la digitalización de nuestra sociedad, así como la utilización de las Tecnologías de la Información y de la Comunicación, denominadas TIC. Por protección de datos, se entiende cualquier información, a través de la cual, se identifica a una persona física, independientemente de si se hace de forma directa o indirecta, por tanto, el derecho a la protección de datos se configura como una facultad del ciudadano para poder oponerse a que ciertos datos personales vayan a ser tratados a un fin diferente del cual fue justificado. Asimismo, el objetivo principal de la protección de datos es proteger y asegurar los derechos propios de la persona la cual ha facilitado sus datos personales.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD), salvaguarda aquellos datos de carácter personal, los cuales son usados por grandes empresas, PYMES, franquicias, autónomos, asociaciones, etc. [1] El término "protección de datos" incluye un conjunto de técnicas jurídicas e informáticas, las cuales están encaminadas a garantizar los derechos de los ciudadanos sobre el control de sus datos personales y sobre la confidencialidad, integridad y disponibilidad. [2]

La Agencia Española de Protección de Datos (en adelante, AEPD), es la que se encarga de velar por el cumplimiento de la normativa de protección de datos y de este modo pues de controlar su aplicación. [3]

El Reglamento General de Protección de Datos (en adelante, RGPD) fue aprobado el 14 de abril de 2016, pero su implantación se hizo efectiva a partir de 2018, y su aplicación se enmarca en el ámbito de los países de la Unión Europea (en adelante, UE), aunque cada país tiene la posibilidad de poder elaborar sus propias leyes. Este Reglamento, se trata de una normativa contrastada en el ámbito europeo cuyo contenido trata sobre la

[1] Microlab, 2021, «¿Qué datos protege la LOPD y RGPD?» Disponible on line: https://microlabhard.es/que-datos-protege-la-lopd-y-rgpd/
[2] Universitat de Valencia, «Protección de Datos Personales », Disponible on line: https://www.uv.es/uvweb/servicio-informatica/es/normativa-procedimientos/proteccion-datos/preguntas-frecuentes-1285902056674.html
[3] «Agencia Española de Protección de Datos»,2021, Madrid, Disponible on line: https://www.aepd.es/es

protección de datos personales y, además indica las normas, en lo que respecta a la libre circulación de dichos datos. Dicho reglamento, tiene el objetivo de evitar el mal uso de la información básica de la ciudadanía, es decir, proteger el derecho de las personas a preservar sus datos personales y garantizar los derechos y libertades individuales recogidos en nuestro Ordenamiento Jurídico, así como, en nuestra Constitución Española.

El RGPD, debe de ser cumplido por las empresas las cuales estén establecidas en la UE y que realicen un tratamiento de datos personales como parte de sus actividades. También, deben cumplir el Reglamento, las empresas establecidas fuera de la UE que ofrezcan productos o servicios o realicen actividades de tratamientos de personas de la UE, en virtud del artículo 3 del RGPD. [4]

El procedimiento a seguir para llevar a cabo la adaptación al RGPD son:

a. Consentimiento expreso de los clientes.
b. Deber de informar.
c. Nombrar un delegado de Protección de Datos.
d. Firmar un contrato con Encargados del tratamiento.
e. Registro de actividades de tratamiento.
f. Análisis de riesgos.
g. Notificación de incidentes de seguridad.
h. Evaluación de impacto.
i. Privacidad del diseño por defecto.
j. Página web.
k. Nuevos derechos de los usuarios.

Por otro lado, los principios que señala el RGPD, en su artículo 5, destaca la protección de datos personales, los cuales deben de ser tratados de forma lícita, leal y transparente, recogidos con un fin legítimo y determinado, adecuado y limitado a la finalidad para la que ha sido recabada, y que se traten de datos exactos y actualizados. También, que los datos, sean conservados de forma que se permita la identificación del interesado solo durante el plazo necesario para el cumplimiento para cuyo fin fueron obtenidos. Y, finalmente que los datos sean tratados de forma que se garantice una cierta seguridad,

[4] «Ubicación de los datos personales», Disponible on line: https://ayudaleyprotecciondatos.es/guia-rgpd/#Principios_relativos_al_tratamiento_de_datos_personales

debiendo de ser protegidos en caso de pérdida de los mismos, robo, destrucción, etc., y garantizando de tal manera la integridad y confidencialidad de los datos personales.

1.2.ASPECTOS GENERALES.

1.1.1. TRATAMIENTO DE DATOS PERSONALES.

Destaca la falta de transparencia y la falta de información en lo que respecta al almacenamiento y uso de nuestros datos personales, de tal forma, que la ciudanía (se incluye a ciudadanos y trabajadores) es víctima de decisiones que desconocen por completo y además dichas decisiones a veces no se pueden controlar, debido a su desconocimiento. Actualmente, debido a la digitalización pues con la llegada del BIG DATA, hay nuevos dispositivos, los cuales, recaban datos personales, de modo que el tratamiento de estos datos, no cumplen en determinadas ocasiones con las exigencias legales.

El tratamiento de los datos personales, consiste en cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, que pueden hacerse por medio de procedimientos automatizados o no, como el registro, organización, estructuración, conservación, adaptación o modificación, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, interconexión, limitación, supresión o destrucción (artículo 4.2, RGPD).

El Tribunal de Justicia de la UE, manifiesta que compete al responsable del tratamiento garantizar que los datos personales sean tratados de forma lícita y leal, con un fin lícito y legítimo. Por tanto, el responsable debe adoptar todas las medidas necesarias para que los datos que no responden a los requisitos pertinentes pues sean suprimidos o rectificados. [5]

Los principios relativos al tratamiento de los datos personales, se regulan en el artículo 5 y en el artículo 39 del RGPD;

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

[5] Piñar Mañas, J.L., y Recio Gayo, M. (2018), *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea.* Wolters Kluwer. Madrid.

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines;

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales;

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

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Por consecuente, a los principios de calidad, proporcionalidad, finalidad, exactitud y actualidad, cancelación de oficio y licitud, el RGPD añade seis principios más, que son[6]:

- Principio de licitud, lealtad y transparencia: se prohíbe la recogida de datos a través de medios fraudulentos o ilícitos. El principio de licitud queda vinculado con el principio de transparencia, junto con el de información, ya que esta debe otorgarse de una manera compresible y accesible. Es decir, el tratamiento no deviene leal ni lícito si la información a tratar no se puede comprender ni es accesible. [7]
- Principio de minimización de datos: consiste en que lo datos personales serán proporcionados, adecuados, pertinentes y limitados a los que pueda resultar necesario en virtud a los fines para los que sean tratados. Además, no deben de

[6] Fernández Ramírez, M., Fernández Ramírez, M., (2021), *El derecho del trabajador a la autodeterminación informativa en el marco de la actual empresa ´´neopanóptica''*, Pamplona, Aranzadi, pp.195-196.
[7] *Ibídem*, pp.197-198.

recabarse más datos de los imprescindibles para llevar a cabo la actividad empresarial con ciertas garantías y otorgar más valor a los derechos del usuario. [8]

- Principio de limitación de la finalidad; consiste en que los datos personales deben de ser recabados con fines ciertos, legítimos y claros.
- Principio de exactitud; se caracteriza en que los datos obtenidos deben de ser exactos y si fuese preciso, pues actualizados. En relación a la exactitud de los datos, el afectado, podrá ejercitar su derecho de rectificación, acompañando, cuando sea necesario, la documentación que acreditase la inexactitud o información incompleta respecto a los datos que se van a tratar. [9]
- Principio de limitación en plazo de conservación; destaca que los datos deberán de ser cancelados cuando ya no sean útiles para la finalidad en la que estos se obtuvieron, y, el RGPD, limita el plazo de conservación y obliga al responsable a establecer plazos para la supresión o revisión de los mismos, en virtud del artículo 39.
- Principio de seguridad, integridad y confidencialidad: la seguridad de los datos, más que una obligación, es un principio del tratamiento de datos, y deberá de ser adecuada a los datos que se vaya a tratar, conforme al artículo 39 RGPD. [10]

En lo que respecta a datos que son especialmente protegidos, es decir, aquellos datos personales que revelan cierta información del interesado sobre su origen étnico o racial, opiniones políticas, afiliación sindical, salud, vida sexual, biométricos, etc., el artículo 9.1 RGPD, nos explica que solo se pueden tratar cuando concurran de manera simultánea con los siguientes requisitos:

- Que exista un consentimiento explícito por parte del interesado con objetivos específicos.
- Que aparezcan algunas de las circunstancias siguientes:
    - Cumplimiento de obligaciones y ejercicios de derechos en el ámbito del Derecho Laboral y de la seguridad y protección social.
    - Protección de intereses vitales del interesado.
    - Tratamiento efectuado en el ámbito de asociaciones cuya finalidad sea política, filosófica, religiosa o sindical.

[8] *Ibídem* ,198.
[9] *Ibídem*, p.202
[10] *Ibídem*, p. 204.

- Tratamiento de datos públicos.
- Tratamientos necesarios para firmar reclamaciones o efectuados por los tribunales en su función judicial.
- Por razón de interés público en el ámbito de la salud pública.
- Por razón de investigación científica o histórica o con fines estadísticos.

Pues bien, se trata de datos que pertenecen al núcleo más íntimo de la persona y se merecen por tanto una especial y mayor protección, teniendo de tal forma, el consentimiento del interesado sobre el tratamiento y además la prohibición que marque la ley, con los requisitos de seguridad y confidencialidad para poder garantizar un amparo sobre dichos derechos, ya que el propio tratamiento de datos debe de ser legítimo, es decir, cumplir con la base de legitimación del artículo 9 RGPD. [11]

Por otro lado, el trabajador, como cualquier interesado, goza del derecho de acceso, consagrado en el artículo 15 RGPD, y esto consiste en que el interesado puede conocer las informaciones que sobre él son objeto de tratamiento por el responsable del tratamiento. Es decir, el trabajador puede solicitar y obtener del responsable del tratamiento confirmación de si se es están tratando o no sus datos personales y en dicho caso pues información sobre los datos que están siendo objeto de tratamiento. Además, en lo que respecta al derecho de acceso, conforme al artículo 12.3 RGPD, el responsable del tratamiento debe facilitar al interesado el acceso a las informaciones en el plazo de un mes, contando desde que se recibe la solicitud.[12]

Además del derecho de acceso, también existen otros derechos subjetivos del trabajador, como el derecho de rectificación, actualización, supresión y oposición.[13]

El derecho de acceso, en relación al derecho a la información sobre los datos y su condición para poder ejercitar las demás prerrogativas del interesado, da lugar a obtener confirmación del responsable del tratamiento sobre si se interactúan o no con sus datos personales, sobre su finalidad, destinatarios, origen, posibilidades de defensa y existencia de decisiones automatizadas. [14] Destaca, la posibilidad de obligar al interesado a que este

[11] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación informativa…op.cit., p.* 202.
[12] Instituto Quatrecasas de Estrategia Legal en RRHH, 2020, *Documentos sobre el impacto de las nuevas tecnologías en la gestión de las personas y en las relaciones laborales,* Wolters Kluwer. Madrid.
[13] Rodríguez Escanciano, S,.(2019), *Derechos laborales digitales: Garantías e interrogantes* ,Pamplona (Aranzadi), p.107.
[14] Blázquez Agudo, E.M., (2018), *Aplicación práctica de la protección de datos en las relaciones laborales*, Wolters Kluwer, Madrid, p. 111.

detalle los datos o actividades de tratamiento a los que se refiere la solicitud, en caso de que el responsable, tenga una gran cantidad de información del afectado, y también, el límite de tiempo admitiendo que el responsable pueda denegar el acceso en repetición si no ha transcurrido el plazo de seis meses desde la solicitud anterior, excepto y si existe causa legítima. Por ello, se podrá ejercitar dicho derecho, cuando haya un interés legítimo del afectado, en relación a la naturaleza de los datos almacenados, finalidad, tiempo de permanencia de los datos, procesamiento de los mismos, o repercusión de los datos en la adopción de las decisiones de una empresa. [15]

El derecho de rectificación, introduce el poder corregir los datos inexactos o incompletos, que, es una obligación del responsable y prerrogativa exigible por el afectado, la cual, debe de corregirse sin dilación indebida y en un plazo máximo de un mes, en virtud del artículo 12.4 RGPD. [16]

El derecho de cancelación, se basa en que el interesado pueda solicitar al responsable el cese en el uso de sus datos personales, ya que considera que el tratamiento no se ajusta a lo expuesto en la normativa y también cuando los datos resultan inexactos, incompletos, inadecuados o excesivos, conforme al artículo 32.2 RGPD. Además, a que desaparezca cualquier enlace a esos datos.[17] Esto supone, en un primer modo, un reconocimiento de la pretensión de suprimir la información en el sitio web (abstenerse de dar difusión a esta información, siendo por medio de solicitud por parte del titular de los datos), y la entidad responsable, pues deberá elegir entre limitar el tratamiento conforme al artículo 18 RGPD, o suprimir la información conforme al artículo 17 RGPD, ponderando el alcance de este derecho con el derecho a la libertad de expresión, salud pública, deber de conservar los datos para cumplir una obligación legal y el interés público. [18] Tras esto, se puede concluir de forma de que el titular de un dato tiene derecho a que dicho dato sea suprimido o bloqueado, y que no sea alcanzable por medio de internet, cuando se produzca:

[15] Poquet Catala, R., (2013), *El actual poder de dirección y control del empresario*, Pamplona (Aranzadi), p.191.
[16] Rodríguez Escanciano, S,. *Derechos laborales digitales, op.cit..,* p.109.
[17] Goñi Sein, J.L., (1988), *El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder de control empresarial*, Civitas, Madrid, p. 124.
[18] Sánchez Trigueros, C. y Cuadros Garrido, M.E(2019), *La nueva regulación Europea y Española de protección de datos y su aplicación al ámbito de la empresa* (incluido el Real Decreto-Ley 5/2018), p.124.

- Que los datos ya no son necesarios en cuanto a la finalidad para los que fueron recogidos o tratados.
- El titular, retira el consentimiento de sus datos personales, haciendo uso de su derecho de oposición. [19]

Para dar lugar a reconocer el derecho al olvido, debe ejercitar el derecho de oposición, y este irá ante el responsable del tratamiento o ante la Agencia de Protección de Datos (búsqueda realizada a partir de su nombre como persona física, resultados obtenidos por medio del buscador, contenido de la información que le afecta)[20].

La Sala de lo Contencioso-administrativo, en la sentencia 11 de enero de 2019, garantiza la protección frente al derecho al olvido digital en casos en que la información propagada, y cuya localización se obtiene por medio de búsqueda de internet, tenga datos inexactos que afectan a la esencia de la publicación, comprendiendo que es la entidad proveedora la que debe cargar con este deber de garantía frente a la persona que ha sido afectada, vulnerando el derecho al honor, intimidad personal y familiar, y a la propia imagen. [21]

El derecho al bloqueo, consiste en que los datos estarán congelados e inaccesibles a los usuarios[22], teniendo que mantener de forma exclusiva a disposición de las Administraciones Públicas, Jueces y Tribunales, referente a la atención de las responsabilidades que puedan surgir.

Por ello, pues el responsable queda sometido a informar la rectificación y la supresión a cado uno de los destinatarios, excepto que sea imposible o haya una dificultad desproporcionada, en virtud del artículo 19 RGPD. [23]

1.1.2. INFORMACIÓN SOBRE EL TRATAMIENTO DE DATOS PERSONALES.

Según la Guía publicada por la Agencia Española de Protección de Datos, el responsable del tratamiento, normalmente es el empleador y este debe informar a las personas interesadas o que desempeñen el trabajo, de forma transparente, concisa, inteligible, y

[19] Davara Rodríguez, M.A.,(2014), *El derecho al olvido en internet*, El Consultor de los Ayuntamientos, núm.13, p.3.
[20] Diario La Ley, núm.8466,2015.
[21] Rec. 5579/2017.
[22] Preciado Domenech, C.H., (2017), *El derecho a la protección de datos en el contrato de trabajo,* Adaptado al nuevo Reglamento 679/2016, de 27 de abril, cit. P.294.
[23] Rodríguez Escanciano, S., (2019) *Derechos laborales digitales: garantías e interrogantes*, Aranzadi, Pamplona, p.113.

con un lenguaje claro y sencillo sobre el tratamiento de los datos que se están recopilando (conforme a los artículos 13 y 14 del RGPD). El objetivo del tratamiento de los datos personales, deben de tener una relación directa entre quienes tratan el dato y la entidad[24]. La base jurídica del tratamiento es el consentimiento, y este no debe de estar sometido a ningún vicio, tales como; error, violencia, intimidación y dolo, y si se da alguno de ellos pues esto da lugar a la anulabilidad del contrato. [25]

El deber de información se sitúa en el núcleo del contenido esencial del derecho a la protección de datos y constituye una garantía para el interesado, ya que podría conocer qué datos están siendo tratados de carácter personal y con quién están siendo compartidos.[26]

1.1.3. TRANSFERENCIAS INTERNACIONALES DE DATOS.

El RGPD, en materia de transferencias internacionales de datos, pues introduce la posibilidad de que se den garantías, las cuales han de ser ofrecidas por los exportadores de datos, independientemente de que los exportadores pues sean los responsables o bien los encargados del tratamiento. Y, que dichos datos exportados pues se lleven a cabo por medio de un código de conducta.[27]

Conforme a la Guía de la AEPD, se considera transferencia internacional de datos, aquellas transmisiones de datos personales/flujo de datos personales desde el territorio español hacia fuera del Espacio Económico Europeo (países de la Unión Europea más Liechtenstein, Islandia y Noruega), ya sea una comunicación de datos a otros responsables del tratamiento, en cuyo caso, el exportador de los datos y el importador de los datos serán los responsables del tratamiento. Los responsables y encargados del tratamiento de datos personales, pueden realizar transferencias internacionales sin la necesidad de autorización de la AEPD, siempre y cuando el tratamiento de los datos se

[24] «Guía de la Agencia Española de Protección de datos». Disponible on line: https://www.aepd.es/es/guias-y-herramientas/guias
[25]«Vicios del consentimiento», Disponible on line: https://www.conceptosjuridicos.com/vicios-del-consentimiento/#:~:text=Los%20agentes%20que%20protagonizan%20los,en%20los%20dos%20%C3%BAltimos%20casos).
[26]«Guía de la Agencia Española de Protección de datos». Disponible on line: https://www.aepd.es/es/guias-y-herramientas/guias
[27] García Mahamut, R., y Tomás Mallén, B.. (2019), *El RGPD. Un enfoque nacional y comparado*. Tirant lo Blanch. Valencia.

realice en función de lo dispuesto en el RGPD, a través de una decisión de adecuación y mediante la aportación de garantías, las cuales deben de ser adecuadas. [28]

1.1.4. CESIÓN DE DATOS A OTRAS EMPRESAS.

La cesión de datos a terceros, actualmente ha generado muchas sanciones desde que entró en vigor la normativa de RGPD, y dicho Reglamento amplió su alcance en lo que respecta a la privacidad sobre datos de carácter personal.

La cesión de datos consiste en proporcionar el acceso a los datos de una persona a un tercero interesado. Para llevar a cabo la cesión de datos personales, hay que cumplir dos requisitos; el primero es que la cesión de datos sea para cumplir con los objetivos y funciones de la empresa, entre las relaciones del cedente de datos y el cesionario de datos, y el segundo requisito es el previo consentimiento informado del interesado. Por tanto, el acceso de datos por cuenta de un tercero pues lleva consigo la prestación de un servicio por parte de una tercera empresa al responsable del fichero, que accede a los datos del mismo para el cumplimiento de la prestación contratada. De este modo, el responsable del tratamiento de los datos decide qué información se procesa y la base legal requerida, mientras que el encargado del tratamiento pues completa el procesamiento en nombre del responsable.

Para llevar a cabo una correcta cesión de datos, han de cumplirse tres requisitos:

- Traslados en función de una adecuación, esto quiere decir que el país que va a recibir los datos, los debe de proteger de forma adecuada.
- Transferencias sujetas a garantías apropiadas, es decir, que se establezcan medidas adecuadas de protección sobre esos datos.
- Reglas corporativas vinculantes, es decir, que existan unas normas a las que estén vinculadas tanto la empresa que cede los datos como la que adquiere los datos.

Sin embargo, hay excepciones a estas tres condiciones, tales como; si el individuo dio su consentimiento después de ser informado del riesgo, si es por interés público, etc.

El contrato de cesión de datos a terceros, debe de incluir cierta información básica, así como; identidad del destinatario al que se ceden los datos, finalidad de la cesión, duración del tratamiento y plazo de conservación de los datos, clases de interesados, datos

[28] «Garantías para las transferencias de datos personales a terceros países u organizaciones internacionales», 26 de noviembre de 2021, Disponible on line: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales

personales a los que se tendrán acceso, obligaciones del responsable y encargado del tratamiento.

Además, los terceros que tienen acceso a la información, deben aceptar los términos siguientes;

- Cumplir la política de seguridad de los sistemas de información electrónica de la empresa.
- Cumplimiento de la política de protección de datos de la empresa.
- Garantizar la seguridad continua de la información.
- Cumplir con la confidencialidad cuando un tercero tiene acceso a la información de la empresa.
- Acceso seguro y derechos de acceso necesarios para el mantenimiento en función del principio de privilegios mínimos.

Por otro lado, el consentimiento para la cesión de datos pues será nulo cuando la información dada al interesado no sea transparente, de tal forma que no conozca realmente la finalidad a la que se destinarán sus datos. Además, el tercero deberá de llevar a cabo la debida diligencia, una evaluación de riesgos y revisión de condiciones para garantizar que la empresa no estará expuesta a riesgos que puedan ser indebidos.

En lo que concierne a la cesión de datos de empresas del mismo grupo, pues las sociedades tienen personalidad jurídica plena e independiente entre sí, por ello todo intercambio de datos que se realice entre distintas empresas del mismo grupo empresarial pues se entenderá como una cesión de datos. Por tanto, se exige que cada empresa informe de la cesión y finalidad al afectado junto con la solicitud del consentimiento.

Al finalizar la relación contractual, el responsable del tratamiento de los datos personales, puede suprimir todos los datos personales al finalizar los servicios, o bien que el encargado del tratamiento pues devuelva dichos datos.

Por todo ello, una empresa no puede dar datos a otra empresa sin un previo consentimiento de la persona, excepto en casos previstos por la normativa, del tal modo que, no será necesaria la autorización para la cesión de datos a terceros cuando la misma sea autorizada por Ley, y cuando los datos sean necesarios para dar solución a problemas

relacionados con la salud pública o cuando los datos hayan sido recabados de una fuente pública y se respeten los derechos de los interesados. [29]

2. LA PROTECCIÓN DE DATOS EN LAS RELACIONES LABORALES.

2.1.EL DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS.

2.1.1. INTIMIDAD, PROTECCIÓN DE DATOS DEL TRABAJADOR Y USO DE MEDIOS TELEMÁTICOS.

Internet ha supuesto una gran revolución en el mundo de la información, característica que hace que la mayoría de las industrias de la comunicación estén en continua transformación.

El derecho a la intimidad, se trata de un derecho fundamental, consagrado en nuestro artículo 18 de la Constitución Española. Desde el punto de vista del TJUE, este derecho fundamental forma parte de los principios generales cuyo respeto también es garantizado por el Tribunal de Justicia de la UE. Pues bien, dicho Tribunal, hace manifestación expresa de reconocer el Derecho fundamental a la protección de datos como un Derecho autónomo e independiente del Derecho a la Intimidad. A su vez, el derecho a la vida privada, consagrado en el artículo 8 del Convenio Europeo de Derechos Humanos, constituye un Derecho fundamental protegido por el ordenamiento jurídico comunitario. Por tanto, si una persona decide someterse a ciertas pruebas para obtener un fin con ello, pues hay que respetar la vida privada y a su vez respetar la negativa del interesado en toda su extensión. Además, el TJUE, alega en la sentencia del caso "Nowak", de 20 de diciembre de 2017, que ''la protección del derecho fundamental al respeto de la intimidad pues conlleva que toda persona física pueda cerciorarse de que los datos personales que le competen son ciertos, exactos y se utilizan de forma lícita''.[30]

2.2.EL DERECHO A LA PRIVACIDAD EN UNA RELACIÓN LABORAL.

El artículo 87 LOPDGDD, establece que los empleados públicos y los trabajadores, tienen el derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por el empresario.[31] Por tanto, se deduce que no es que se reconozca el

[29] «Cesión de Datos a terceros». Disponible on line: https://protecciondatos-lopd.com/empresas/cesion-datos-terceros/

[30] Piñar Mañas, J. L.., y Recio Gayo, M., (2018),*El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*. Wolters Kluwer. Madrid.

[31] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación…op.cit*. p. 154.

derecho a la intimidad como tal, sino que se reconoce el derecho a la protección de la intimidad.

2.2.1. SISTEMAS BIOMÉTRICOS DE CONTROL EN EL HORARIO/REGISTRO DE JORNADA.

El sistema biométrico destaca por su sistema de control de acceso, y por tanto pueden contribuir a aumentar el nivel de seguridad y a facilitar, acelerar y simplificar los procedimientos de identificación y autenticación. El sistema de control de un horario es aquel con el que se supervisan las horas de entrada y de salida de los empleados de una empresa. El fin del mismo es evaluar el número de horas que trabajan, así como la puntualidad o las incidencias que se puedan producir a lo largo del día. Por tanto, la mediación biométrica es considerada uno de los mejores métodos de identificación humana por su fiabilidad y eficiencia.

Las ventajas que suponen para las empresas, pueden ser, tales como: seguridad, fiabilidad, celeridad en el control, y comodidad. Sin embargo, también, aparecen riesgos para los trabajadores, así como; la posibilidad de llevar a cabo un control total por parte de las empresas, la intrusión en los espacios de su privacidad, disolución de fronteras entre lo laboral y lo personal, posibilidad de construir perfiles con los datos obtenidos, acceso a la información personal sensible, o la pérdida del anonimato.

Tras ello, se dice que los datos biométricos digitalizados para facilitar e intensificar la eficacia de las normas tradicionales de control, y esto desencadena nuevos problemas derivados de los límites de que el derecho a la intimidad y a la autodeterminación informativa de los trabajadores, obliga a imponer el ejercicio de los poderes de dirección del empresario. [32]

En el "Documento de Trabajo sobre biometría" de 2003[33], el Grupo de Protección del artículo 29 de la Directiva 95/46/CE[34], reconoce la preocupación que hay sobre los daños biométricos, y manifiesta que *"una utilización amplia y sin control de la biometría es*

[32] SELMA PENALVA, A., *''El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores''* Revista doctrinal Aranzadi Social, núm.9, (2010).
[33] Documento de trabajo sobre biometría 2003. Realizado por el grupo de protección de las personas en lo que respecta al tratamiento de datos personales que fue creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.
[34] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

preocupante desde el punto de vista de la protección de los derechos y libertades fundamentales de las personas. Este tipo de datos es de una naturaleza especial, ya que tienen que ver con las características comportamentales y fisiológicas de una empresa y pueden permitir su identificación inequívoca".

2.2.1.1.DIFERENTES TIPOS DE TECNOLOGÍAS BIOMÉTRICAS.

Un sistema biométrico, se puede decir que es como un sistema automático que permite reconocer seres vivos a través de sus rasgos inherentes, es decir, los datos biométricos serían los datos personales obtenidos a partir de un tratamiento técnico específico, conforme a los artículos 4 y 4.14 RGPD.

Destaca, la Guía Española del Instituto Nacional de Ciberseguridad (en adelante, INCIBE) sobre Tecnologías Biométricas aplicadas a la Ciberseguridad, señala los diferentes tipos de reconocimientos biométricos. Sin embargo, en general, se puede considerar que hay dos tipos de rasgos biométricos a través de los cuales se puede llevar a cabo una autenticación biométrica:

- Rasgos fisiológicos, caracterizada por las características diferenciadoras del cuerpo humano de carácter principalmente fisiológica, tales como el rostro, huella dactilar, iris o geometría de la mano.
- Rasgos conductuales, que corresponden con el comportamiento de la persona, tales casos como la forma de escribir, la firma, voz, e incluso la forma de andar.

Hoy por hoy, los sistemas biométricos que más han avanzado en nuestra sociedad, desde el punto de vista tecnológico, son los que se caracterizan por los rasgos fisiológicos. De hecho, es habitual encontrarse en el mercado dispositivos basados en rasgos fisiológicos, tales como pueden ser cámaras de vídeo con reconocimiento de cara, acceso a ordenadores portátiles por medio de huella dactilar, sistemas de identificación de iris en aeropuertos, etc. Mientras que, los rasgos conductuales, siguen siendo objeto de investigación, como pueden ser la voz, forma de escribir, firma, manera de caminar, etc.

2.2.1.1.1. Reconocimiento de huella dactilar.

La huella dactilar, se trata, de un dato biométrico único de rasgo fisiológico, el cual, identifica a una única persona, conforme al artículo 4.14) RGPD; "«*datos biométricos*»: *datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o*

confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

La huella dactilar es una forma de control de los accesos a las dependencias empresariales, caracterizado por la epidermis del dedo, ya que cada individuo posee unas crestas y surcos que los diferencia. De este modo, cada huella otorga bastante información relevante sobre una persona. La huella dactilar situada por ejemplo en un ámbito empresarial, la convierte en una tecnología muy útil debido a su fácil integración, usabilidad, y bajos costes, por tanto, es un método oportuno para su implantación en las industrias.

También, el lector de huella digital para control de asistencia, tiene la función predominante de registro, y esto permite calcular ratios de personal, gestionar horarios, alta y bajas de personal y calendarios laborales con fiabilidad y eficiencia, lo cual ayuda a los departamentos de una empresa como es ''recursos humanos'' a la hora de tomar decisiones y mejora además la productividad y el rendimiento de la plantilla. Por ello, el método de la huella dactilar, es el más desarrollado y utilizado.[35]

De otro modo, además de la función que tiene de supervisar en las organizaciones productivas, también, está ligada a otros fines legítimos, como pueden ser: impedir el acceso de personas no autorizadas, prevención de riesgos laborales, detectar el consumo de productos que puedan generar peligro en el centro de trabajo, cumplimiento de los derechos de los trabajadores (como el respeto a la jornada estipulada). Aunque, según la sentencia de 4 de marzo de 2010, esto puede suponer una revelación de información sumamente sensible como son los datos étnicos de la persona.

En el tratamiento de la huella digital para el control de cumplimiento de la jornada laboral, destaca el Tribunal Supremo, que admitió la utilización de la palma de la mano como elemento identificativo a efectos del registro de horario, el cual tenía un fin legítimo y que la toma de la mano sería una medida adecuada y no excesiva, conforme a la STS, Sala de lo Contencioso Administrativo, de 2 de julio de 2007(RJ 2007,6598). Pero, el artículo 9 RGPD, adentra a que el tratamiento de datos biométricos se sitúa dentro de las categorías especiales de tratamiento de datos, es decir, que este posee una protección más intensa. Asimismo, el artículo 38.4 del Estatuto de los Trabajadores, no exige que tipo de registro deba de realizarse mediante control biométrico, entonces, por tanto, la empresa tendrá que acreditar que no existe un sistema de registro menos invasivo o solicitar el

[35] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación…op.cit.,* pp.33-36.

consentimiento del trabajador. De este modo, dentro de los pactos o acuerdos que aparezcan en la empresa sobre el registro de la jornada, pues deberá de haber un aspecto relacionado al ámbito de tratamiento de datos.

En consecuencia, a la hora de valorar la necesidad y proporcionalidad de ese tratamiento y si puede estar dentro del interés legítimo del empresario a controlar el acceso a las organizaciones productivas por parte de sus empleados, pues la normativa exige un estudio eficaz y estricto sobre la necesidad y proporcionalidad de los datos tratados y de si el objetivo previsto podría alcanzarse de la forma menos intrusiva posible. Esto quiere decir, que, si la finalidad que se quiere alcanzar en un determinado contexto puede ser lograda sin necesidad de llevar a cabo el tratamiento de un cierto dato, pues se debería elegir necesariamente esta posibilidad.

En general, el tratamiento de datos en el ámbito laboral, se realiza a través de disposiciones legislativas o de convenios colectivos, u otro tipo de normas específicas con el objetivo de garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores, conforme al artículo 88 RGPD, en virtud de la gestión, planificación y organización del trabajo.

De tal manera, las medidas de control que se basan en la recogida de huellas dactilares, deben de cumplir con los principios y preceptos de la legislación en vigor, además de la normativa laboral y también ha de gozar de las medidas de seguridad suficientes para intentar que el riesgo sea el menor posible y garantizar siempre la confidencialidad y seguridad de los datos obtenidos.

Para poder instalar un control de acceso con huella dactilar, pues la empresa deberá de tener en cuenta lo siguiente:

- Si el fin que se quiere obtener en un contexto se puede obtener sin necesidad de utilizar el tratamiento de un cierto dato, pues se debería de optar por esta posibilidad (principio de proporcionalidad). Se considera que además pueden existir otras medidas menos intrusivas que el método de la huella dactilar, como, por ejemplo, el registro de firmas de los trabajadores a la entrada y salida de la organización productiva.
- Si se cumple con el principio de calidad de datos conforme con el artículo 5.1 b) y el artículo 4.1 LOPDGDD, y junto con ello, los datos se pueden utilizar si son adecuados, pertinentes y no excesivos, dando lugar a una evaluación estricta de la

necesidad y de la proporcionalidad de los datos tratados y de si el fin perseguido podría alcanzarse de la forma menor intrusiva posible.

- Conforme al artículo 35 RGPD, se deberá realizar una Evaluación de Impacto de Protección de Datos (en adelante, EIPD) para tener en cuenta las implicaciones de la tecnología empleada.
- Si es necesario recabar el consentimiento de los afectados para el tratamiento. Aunque no sea necesario el consentimiento expreso de los trabajadores, pues estos deben de ser informados, principalmente del objetivo de los datos biométricos.
- También, la recogida de la huella dactilar ha de implicar un procedimiento que otorgue una mayor garantía de seguridad a favor de los datos biométricos, caracterizados por datos que se transforman en códigos alfanuméricos imposibles de descifrar (procedimiento de conversión inmediata a un carácter alfanumérico).[36] De esta forma, la AEPD en su informe 0065/2015[37], manifiesta que en función a los principios de proporcionalidad y minimización, lo correcto sería que esos datos biométricos estuviesen recogidos en una tarjeta inteligente en poder del usuario, sin ser incorporados al sistema informático de la empresa, ya que se tratan de medios más proporcionales.
- Requerimientos tecnológicos para un funcionamiento adecuado de software, pudiendo garantizar la máxima confidencialidad de los datos, sin que pueda dar lugar a una suplantación de identidad.[38]

2.2.1.1.2. Reconocimiento facial.

En 1883, aparecen las bases del sistema de reconocimiento facial, con Alphonse Bertillon, y destacan: la distancia de los ojos, la simetría o diferentes rasgos faciales. El rostro facial uno de los principales elementos que se utilizan para reconocer a una persona, de forma que, una máquina es capaz de poder identificar los rasgos de una persona y almacenarlos en su base de datos. Y esto, es posible, gracias a la identificación de un individuo mediante un análisis de los rasgos biométricos de su rostro a partir de una imagen o fotografía.

El reconocimiento facial puede ser utilizado para la vigilancia general, mediante cámaras de vídeo, mediante el cual se puede decir que este sistema es poco intrusivo y apenas

[36] Cfr. Sentencia de la Audiencia Nacional, de 4 de marzo de 2010, en la que se indica que los sistemas no incorporarán el dato de la huella digital sino el vinculado con un identificador numérico obtenido a partir de la misma que se almacena en las tarjetas de proximidad de los empleados.
[37] De 9 de marzo de 2016.
[38] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación… op.cit*., pp. 36-41.

exige participación del usuario. [39]De todos modos, el reconocimiento facial es un medio técnico específico que permite la identificación de una persona física.

Conforme al artículo 4.1 RGPD, una imagen es un dato de carácter personal por ser una información sobre una persona física identificada o identificable, y, por ende, su tratamiento queda protegido por la normativa reguladora del derecho fundamental de protección de datos.[40] Asimismo, el RGPD, en su artículo 9, otorga a los datos biométricos y a otros datos como los de salud, filiación sindical, religión, etc., una mayor protección, calificándolos como "*categorías especiales"*. Pero, en virtud del artículo 9.1 RGPD, solo los datos biométricos dirigidos en identificar a una persona de forma unívoca, constituyen categorías especiales de datos, conforme al Informe de la AEPD 0036/2020[41] y el Comité Europeo de Protección de Datos en las Directrices 3/2019 sobre videovigilancia. [42]

Hay que tener en cuenta que, un uso ilimitado del reconocimiento facial puede conllevar consecuencias irreversibles, de imposible reparación, en la sociedad, haciendo hincapié en la sensible y numerosa información que dicha tecnología permite recabar. Sobre todo, cuando su uso, se extiende al sector privado y a empresas que desean utilizar dicha tecnología, no solo con fines de seguridad, sino también para conocer mejor a sus clientes, sabiendo el grado de satisfacción, talla de ropa, etc.

Un ejemplo, sería la empresa de supermercados Mercadona, que está siendo investigada de oficio por la AEPD, a partir de la implantación de los sistemas de reconocimiento facial en 40 comercios de la misma. La empresa, lo anunció en julio de 2020, y permitía reconocer a personas con una orden de alejamiento de sus centros comerciales o sus empleados. Esto se producía a través de un escaneo en menos de un segundo y cotejaba la información, gracias al sistema de reconocimiento que contrastaba los rostros de los clientes con los de una base de datos de la cadena del supermercado. Pero, Mercadona, alegó que después del escaneo, se procedía a suprimir las imágenes. Por tanto, el fin era impedir el acceso a personas que aparecieran en sus bases de datos, para evitar robos en

[39] Moreno Díaz, A.B.,(2004), *Reconocimiento Facial Automático mediante técnicas de visión tridimensional*, ed. Universidad Politécnica de Madrid, p. 22.
[40] El derecho a la propia imagen es un derecho fundamental protegido por la Ley Orgánica 1/1982, de Protección Civil del Derecho al Honor, Intimidad Personal y Familiar y a la Propia Imagen.
[41] Informe 0036/2020,p.18, el RGDP no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, porque el artículo 9.1 se refiere a los ''datos biométricos dirigidos a identificar de manera unívoca a una persona física'',
[42] Directrices 3/2019, p.18.

los supermercados. Y, tras el escaneo, el propio sistema pues emitía una notificación a las autoridades solicitando su actuación.

A esto, se añade, que la empresa que desarrolló el software, decía que, aunque se eliminen las fotografías tras el escaneo, pues se ejecuta un tratamiento no autorizado de esa información.

De otro modo, cuando el uso de medidas de reconocimiento facial conlleva un tratamiento de categorías de datos especiales, esos datos, solo pueden ser tratados en determinadas expresiones previstas en la normativa europea del RGPD.[43]

Por otro lado, el Comité Económico Social y Europeo (en adelante, CESE),[44] manifiesta que "*Las nuevas tecnologías de reconocimiento facial, suponen una amenaza para nuestra intimidad*". A medida que esta tecnología se vuelva más barata y fácilmente accesible para todos, podría en última instancia llevar a una situación en la que ya no se pueda caminar por la calle o ir de compras de manera anónima. La amenaza a la intimidad y la autonomía es aún mayor cuando estas tecnologías se utilizan para la elaboración de perfiles o la atribución de puntos en función del comportamiento de la persona. El CESE insiste en que las personas tengan derecho a ser anónimas también en los espacios públicos. Los beneficios que otorgan como el reconocimiento facial y otras tecnologías, son muchos, pero el gran reto de los legisladores, en concreto el Europeo, consistirá en poder regular esta tecnología tratando de no sesgar el desarrollo natural de la sociedad, y teniendo en cuenta los derechos y libertades de los ciudadanos, tanto los que puedan ser vulnerados actualmente, como los que podrían serlo en un futuro tras el avance de la tecnología.[45]

2.2.1.1.3. Reconocimiento de iris y retina.

Desde un aspecto biométrico, el escaneo de iris y retina son denominados como tecnologías de identificación "oculares", es decir, que se basan en los rasgos fisiológicos

[43] Mercadona podría exponerse a una sanción de 20 millones de euros o el 4% del volumen de negocios anual de la empresa si esta cantidad fuese mayor ya que al tratarse de datos de categorías especiales, implica que los consumidores pueden ser identificados de forma directa, única e inequívoca.
[44] Comité Económico y Social Europeo (CESE), La revolución digital teniendo en cuenta las necesidades y los derechos de los ciudadanos. (2019/ C 190/03), p.2.
[45] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación…op.cit*., pp.42-47.

únicos de los ojos para identificar una persona. Aunque ambas comparten una parte del ojo para fines de identificación, son bastantes diferentes respecto a su funcionamiento. [46]

El reconocimiento del iris es la técnica de identificación biométrica más moderna y a la vez, más fiable, ya que cada ojo es único. Los patrones del iris, vienen marcados desde el propio nacimiento y con el transcurso del tiempo no cambian. Además, contienen una gran cantidad de información y tienen más de 200 propiedades únicas, es por ello que sería muy complicado poder confundir a dos personas utilizando ese patrón.

Para poder llevar a cabo ese reconocimiento, se utiliza una cámara de infrarrojos, que hace una fotografía al ojo, y a través de ella se obtienen los detalles del iris.[47] Los sistemas biométricos de reconocimiento del iris, pueden obtener la información necesaria a partir de diferentes distancias, que van desde unos pocos centímetros hasta cerca de un metro, y este proceso no requiere el contacto físico entre el sujeto a identificar y la máquina. También, la tasa de error de este sistema es de las más bajas dentro de todo el conjunto de los diferentes sistemas biométricos de identificación. Un ejemplo sería que cientos de millones de personas, se han registrado en sistemas de reconocimiento de iris por razones de conveniencia y seguridad.

La tecnología de reconocimiento de iris y retina es muy costosa y no siempre de fácil uso, ya que los empleados deben tener previamente un cierto manejo para poder saber controlar con dicho reconocimiento. [48] Este procedimiento evita falsificaciones y engaños, y , el uso de gafas o lentillas no afecta al funcionamiento del sistema.

Los dispositivos de iris, deben de contar con una base de datos que almacene la información de las personas a las que se tiene interés en reconocer, ya que, de lo contrario, no tendría sentido su uso. Como sistema de control tiene una fase de verificación en la que se realiza un estudio de la información obtenida del iris de una persona, para compararla con la información guardada en la base de datos del sistema de

[46] Cfr. Cruz Rangel, L., ´´Biometría de iris vs. retina, sí, en realidad son diferentes´´, ID Noticias, 13 de agosto de 1014; Nieto ,L.A., ´´Biometría de iris vs. Retina / Estudio Tecnológico", publicado el 28 de mayo de 2020.

[47] CORTÉS OSORIO, J.M., MEDINA AGUIRRE, F.A. y MURIEL ESCOBAR, J.M., ´´*Sistemas de seguridad basados en biometría*", Scientia et Technica Año XVII, No 46 (diciembre-2010). Universidad Tecnológica de Pereira, p.99.

[48] El Iris Access 3000 LG, es un modelo comercial disponible para el gran público, y su precio varía según las necesidades de cada empresa. Pero un sistema básico se encuentra entre los 10.000-14.000 euros.

reconocimiento biométrico, y, verificar que el individuo que quiere acceder o extraer algún tipo de información puede hacerlo.

El reconocimiento de retina, es un sistema biométrico de identificación, ya que la retina al igual que la huella dactilar, es única en cada individuo. El escáner biométrico de la rutina se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma. Que cada patrón sea único y que se mantenga igual a lo largo del tiempo, crea una alta seguridad. La retina se escanea a través de una cámara de infrarrojos. Lo más destacado, considerado como ventaja es el entramado de capilares que atraviesa la retina, lo que da lugar a una mayor fiabilidad. La principal diferencia es que mientras que un sistema identificador de huella dactilar almacena unos 40 puntos característicos de una persona, pues el sistema identificador de retina almacena más de 200 puntos característicos. Por tanto, sería casi imposible falsificar una imagen del patrón vascular de retina, entonces no da lugar a la suplantación de identidad. El padrón resultante de las variaciones es convertido a código informático y se guarda en una base de datos.

Desde el punto de vista jurídico, el sistema de reconocimiento de retina, se considera un sistema de control mucho más invasivo que el reconocimiento del iris.

De este modo, igualmente, el problema que plantean este tipo de sistemas es que, una vez divulgados estos datos, quedan comprometidos para siempre, al igual que ocurre con la huella dactilar, ya que, nadie puede renovar su iris, su retina, o huella dactilar. [49]

2.2.1.1.4. Reconocimiento de la geometría de la mano y vascular.

La tecnología de reconocimiento de la geometría de la mano utiliza la forma de la mano para confirmar la identidad de la persona. Para la captura de la muestra de la mano, se utilizan una serie de cámaras que toman imágenes en 3D desde diferentes ángulos. Los rasgos característicos excluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea en general. Aquí, el individuo debe situar su mano abierta sobre un escáner específico y el sistema biométrico la reconoce desde la forma y geometría de la misma.

En aproximadamente un segundo, los sistemas de autenticación basados en el análisis de la geometría de la mano, pueden determinar si una persona es quien dice ser. Estos

[49] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación…op.cit.,* pp.48-50.

sistemas, son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (ej. Adelgazamiento), y son capaces de identificar adecuadamente a un usuario cuya muestra se tomó con bastante antelación, es decir, años atrás, pero que ha ido accediendo al sistema con regularidad.

Por otro lado, la biometría vascular surgió con la necesidad de tener una tecnología orientada a mejorar el rendimiento de los dispositivos biométricos digitales. De otro modo, resulta casi imposible copiar el patrón de las venas que tenemos en nuestra mano, ya que el elemento de identificación está dentro del cuerpo.

En lo que concierne a la biometría vascular, aquí se obtiene el patrón biométrico desde la geometría del árbol de venas del dedo o de las muñecas, es por ello que se dice que es muy difícil robar la identidad. Este, es un método bastante costoso, aunque tiene la ventaja de hacer casi imposible el robo de identidad, por tanto, al utilizar las personas este sistema pues no dejan rastro de sus características biométricas. [50]

En lo que respecta al tratamiento del reconocimiento de la geometría de la mano y vascular, los únicos datos sensibles que podría derivarse del patrón de venas se refieren al estado de salud del trabajador, pero hasta hoy día, no se ha realizado ninguna evaluación formal sobre este tema.[51]

Por otro lado, antes que se hubiese aprobado el RGPD, pues el Tribunal Supremo, admitió el uso de la palma de la mano como elemento identificativo a efectos de registrar el horario, con un fin legítimo y dicha medida, pues era considerada adecuada, pertinente y no excesiva. Sin embargo, actualmente no se considera de la misma manera. [52]

El RGPD considera que, los datos biométricos, obtenidos por medio de técnicas de identificación biométrica y verificación biométrica, como categorías especiales de datos siempre que se relacione a un interesado identificado, conforme al artículo 4.14 RGPD.

2.2.1.1.5. Reconocimiento de la voz.

El control y registro de jornada laboral por voz es uno de los sistemas biométricos más seguros para la autenticación del trabajador. Cada individuo tiene unos rasgos físicos únicos de su aparato fonador: fosas nasales, cavidad bucal, tráquea, etc., que la diferencian que la voz sea un rasgo que nos caracterice de forma individual. La

[50] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas (00720/12/ES WP193), p.19.
[51] *Ibídem*, p.20.
[52] Cfr. STS de 2 de julio, de 2007.

singularidad de la voz, se conforma con el tono y la pronunciación de cada persona que habla, haciéndola singular y exclusiva. De tal modo que, la voz es un patrimonio único de cada persona.

Para utilizar un sistema de biometría de voz, en primer lugar, lo que hay que hacer es obtener la huella vocal. Las aplicaciones de reconocimiento de voz usan sistemas de IA (redes neuronales) para poder identificar las diferentes voces de las personas.

La fiabilidad de este sistema en considerada bastante alta. Pero, aún siguen existiendo dificultades para reconocer la forma natural de hablar de determinadas personas, y este sistema tiene la ventaja de que el dispositivo de adquisición es solo un micrófono, y por ello, no requiere inversiones adicionales. [53]

En lo que respecta a su tratamiento de esos datos, los dispositivos de reconocimiento de voz pueden integrarse de forma fácil "…*sin el respeto de las obligaciones de protección de datos del responsable del tratamiento*". [54]

2.2.1.2.EL RÉGIMEN JURÍDICO DE LOS DATOS BIOMÉTRICOS.

El dato biométrico está protegido al ser un elemento de identificación único de la persona indeleble e inmutable.

En el marco jurídico de la privacidad de la UE, constituido por el RGPD y dentro del marco internacional del Convenio 108 del Consejo de Europa, pues los datos biométricos se consideran datos sensibles y se encuentran sujetos a una protección especial en la que reciben un nivel superior de protección. Por ello, al tener un nivel de garantía superior en todos los aspectos, pues quedan sometidos a una regulación más estricta, la cual podría ser más restrictiva, ya que los Estados miembros, deben mantener o introducir condiciones adicionales, al igual que limitaciones, al tratamiento de respectivos datos, en virtud del artículo 9.4 RGPD. [55]

Respecto a la admisión del tratamiento de esos datos de carácter restrictivo, destaca el artículo 51 RGPD: " *Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente*

[53] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación… op.cit.,* p.52.
[54] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas (00720/12/ES WP193), p.26.
[55] Rodríguez-Piñero Royo, M.,(2019) ''Las facultades de control de datos biométricos del trabajador'', *Temas Laborales,* núm 150,p.98.

Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento .Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales. "

Por ello, el tratamiento de esos datos, pues otorgan información que queda estrechamente relacionada a una persona, y además permite identificar de forma inequívoca al individuo. Destaca la siguiente concepción de los datos biométricos respecto al transcurso en el tiempo de las tecnologías biométricas:

- Identificación biométrica: consiste en la identificación de una persona a través de un sistema biométrico, en cuyo proceso se comparan los datos biométricos con una serie de plantillas biométricas almacenadas en una base de datos.
- Verificación/ autenticación biométrica: la verificación de una persona a través de un sistema biométrico es por medio de un proceso de comparación entre sus datos biométricos con una única plantilla biométrica almacenada en un dispositivo.

Toda referencia realizada hacia los datos biométricos, en un principio se clasifican en datos personales, pero no en datos sensibles.

En lo que concierne al consentimiento del trabajador en el ámbito laboral sobre el tratamiento de datos, se puede decir que la legitimación del tratamiento por medio del consentimiento no es lo más recomendable, debido al desequilibrio que existe, con carácter general, entre en empleado y el empleador, y en muy pocas ocasiones los

trabajadores pueden prestar su consentimiento de forma libre[56], tal y como manifiesta el RGPD.

De este modo, vemos que existe un riesgo en relación del tratamiento de esos datos, que recae en los derechos y libertades de los trabajadores, y por esto se tienen que tener en cuenta dos sistemas para realizar el tratamiento de forma adecuada:

- En primer lugar, un tratamiento de datos biométricos caracterizado por el responsable, el cual debe de realizar una responsabilidad proactiva, es decir, que las empresas conozcan los tratamientos de datos personales, y "*exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo*", en virtud de la AEPD. De tal modo que el empleador debe buscar el medio menos invasivo hacia el empleado, y debe de optar por un tratamiento no biométrico a ser posible. Teniendo en cuenta las implicaciones del uso de las nuevas tecnologías, la observación sistemática de los hábitos de los trabajadores y el tratamiento de datos biométricos (categoría especial), pues habría que analizar su impacto en la protección de datos, (EIPD) y así estudiar tanto la legitimidad del tratamiento y su proporcionalidad (esencial para cubrir esa necesidad y no solo ser el más adecuado o rentable), como la determinación de los riesgos que existen y las medidas que hay para poder moderarlos, de acuerdo con el artículo 35 RGPD. Entonces, se debe evaluar de la forma en el que el sistema analizado puede evitar los tres riesgos que se nombran a continuación:
    - 1. Destaca la usurpación de identidad, sobre todo en el caso de la autenticación e identificación. El dispositivo biométrico no debe de ser burlado por una suplantación y debe garantizar que la persona que realiza la correspondencia es exactamente la persona registrada en el sistema.
    - 2. El segundo riesgo, es el desvío de la finalidad de esos datos, que puede darse por el responsable del tratamiento de datos o por un tercero.
    - 3. Finalmente, se encuentra el riesgo definido por la violación de esos datos, que requiere acciones especiales en el contexto de los datos biométricos en función del tipo de datos en peligro.

[56] VID STS, Sala de lo Social, 4086/2015, de 21/09/2015.

- En segundo lugar, un tratamiento de datos biométricos llevado a cabo directamente por el interesado, ligado la especial naturaleza de los datos biométricos, en virtud del RGPD, vinculado con la atención a la proporcionalidad y a la propia minimización del dato, es decir, que solamente sea objeto de tratamiento en lo imprescindible para cumplir el objetivo buscado. Se podría lograr un sistema donde el dato biométrico estuviese bajo el control del trabajador y no bajo el control del responsable, de modo que, el sistema solo integrase el registro horario junto a la identificación del trabajador, por ejemplo, usando la huella dactilar en su teléfono móvil.

El Dictamen 3/2012 del DT29, señala que "*Al analizar la proporcionalidad de un sistema biométrico propuesto, hay que considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor, sería la probabilidad de que el sistema sea eficaz para responder a la necesidad en virtud de los caracteres específicos de la tecnología biométrica que se va a utilizar. Y un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Y el cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado*".[57]

Asimismo, en el contexto laboral, el tratamiento de datos personales, pues destaca lo siguiente conforme la Recomendación del Comité de Ministros: *''La recopilación y posterior procesamiento de los datos biométricos solo se deberían emprender cuando hay que proteger los intereses legítimos de empresarios, empleados o terceros, solo si no hay otros medios menos intrusivos disponibles. El tratamiento de los datos biométricos se debe basar en métodos científicamente reconocidos y debe estar sujeto a los requisitos de estricta seguridad y proporcionalidad*".

El principio de limitación de la finalidad, debe de tolerarse junto con los otros principios de protección de datos, sobre todo, los principios de necesidad, proporcionalidad y minimización de datos, a la hora de definir los distintos fines de una aplicación. De hecho, el interesado, podrá cuando sea posible elegir entre los diferentes fines de una aplicación

[57] De 27 de abril de 2012, ´´Sobre la evolución de las tecnologías biométricas".

con múltiples funcionalidades, específicamente si uno o varios de ellos exigen el tratamiento de datos biométricos. [58]

El principio de minimización (los representantes legales de los trabajadores (RLT) a la hora de negociar los sistemas de registro, deben elegir sistemas de control menos invasivos, sin intentar utilizar y tratar datos especialmente protegidos, pudiendo alcanzar el mismo objetivo), se basa en la necesidad, el de proporcionalidad se basa en el beneficio resultante de la aplicación de una medida invasiva frente al beneficio esperado de control (es decir, que no hay otros medios alternativos que produzcan una menor injerencia en la intimidad del trabajador que el control por datos biométricos).

La AEPD y distintos tribunales, confirman que los datos biométricos se pueden usar por las empresas siempre que cumplan los requisitos del triple juicio, es decir, idoneidad, justificación y necesidad. En el caso del control de acceso a zonas que tengan una seguridad reforzada, pues será motivado por tanto el uso de este tipo de sistemas.

Se entiende que el sistema de control horario de los trabajadores por medio de los datos biométricos, podrían estar implantados en función de determinados riesgos o por los servicios que presten los trabajadores (como centros de trabajo o instalaciones que deben de tener una serie de restricciones, tales como, acceso, defensa seguridad, centrales nucleares, etc.), entonces sería proporcional tener un sistema biométrico de control horario, con las siguientes garantías;

- Reforzar las obligaciones legales preventivas de privacidad en el diseño y por defecto y de la EIPD. El Comité Europeo de Protección de Datos (CEPD, en adelante), marca dos criterios en relación al tratamiento sometidos a EIPD, (hacer evaluación de impacto en relación a la privacidad cuyo fin es identificar y analizar cómo la privacidad de los datos pueda verse mermada por ciertas acciones) y son:
    - El tratamiento de datos biométricos con el fin exclusivo de identificar a forma inequívoca a una persona, por sí solo no representa un alto riesgo que obligue a realizar una EIPD.
    - Sí será obligatoria la EIPD cuando el tratamiento del dato biométrico, se realice de forma conjunta con:

[58] Vid. Dictamen 4/2007 (WP136), realizado por el GT29, p.7.

  - Control laboral (implica evaluación sistemática y vulnerabilidad o desequilibrio de fuerzas en el titular de los datos tratados frente al trabajador).
  - Datos de geolocalización (rastreo de la geolocalización o el comportamiento de una persona).
  - Datos genéticos (cualquier tratamiento de datos genéticos diferente del realizado por un profesional de la salud, para la prestación de asistencia médica directa al interesado).
  - Tratamiento que implique el uso de nuevas tecnologías o la aplicación novedosa de tecnologías ya existentes.
  - Tratamientos "invisibles" para el interesado. Tratamiento de datos personales que no se han obtenido de forma directa por el interesado.
  - Tratamiento de datos de niños u otras personas vulnerables.

- Idoneidad y proporcionalidad en el propio sistema biométrico. Quiere decir, que se debe asegurar que no es posible implantar otro sistema de registro menos intrusivo (principio de minimización), y, además, debe de cumplir con las garantías adicionales, señaladas por la AEPD, que deben aplicarse para proteger el tratamiento de esos datos (como, por ejemplo: imposibilidad de interconexión de la base de datos biométricos con otras bases).
- Información a los RLT (representación legal de los trabajadores) y a los propios trabajadores. El derecho de información previa a los RLT, viene regulado en los artículos 64.5 ET y 11, 87-90 RGPD, y determina que el empresario deberá negociar su implantación. El artículo 64 del ET, reconoce al Comité de Empresa el derecho a emitir informe sobre "la implantación y revisión de sistemas de control del trabajo ". Por tanto, hay que explicar e informar la necesidad, adecuación, motivos y conveniencia de implantar respectivo sistema, garantizando que no existe otro método más respetuoso en relación al derecho de intimidad de las personas, para conseguir el mismo objetivo, el control horario (principio de minimización y proporcionalidad).

La AEPD publica un documento en relación al uso de la biometría y cómo afectan a la protección de datos. Dicho documento, está dirigido a responsables, encargados y delegados de Protección de Datos. El acceso no autorizado a datos biométricos en un

sistema permitiría el acceso en el resto de los sistemas que utilicen dichos biométricos, y esta una vez que ha sido comprometida, no se puede cancelar. También, se alerta de que la información biométrica se almacenada a lo largo del tiempo de forma mayor en más entidades y dispositivos, por tanto, esto aumenta la probabilidad de poder dar lugar a una brecha de seguridad sobre información biométrica. [59]

2.2.2. SISTEMAS DE CONTROL DE LA ACTIVIDAD LABORAL.

El sistema de control de la actividad laboral, consiste en el tiempo que a cambio de la retribución el trabajador se pone a disposición del empleador, y el empleador a cambio del pago del salario al trabajador pues se apropia de la disponibilidad de su tiempo. El tiempo de trabajo se caracteriza también por la organización del trabajo, empleo o a la propia persona del trabajador física y socialmente. [60]

Se entiende que las empresas quieren saber en qué invierten el tiempo sus trabajadores y por ello controlan la actividad laboral. De esta manera, pues disponen de distintos métodos y sistemas de control. En un primer lugar, la finalidad de los empresarios es bloquear el acceso a ciertas páginas web, tales como redes sociales, música, películas, etc.

Sin embargo, el control que lleva a cabo la empresa sobre el trabajador, puede excederse en lo que compete a la mera comprobación del cumplimiento de las obligaciones laborales básicas, y extenderse fuera del ámbito de la buena fe contractual. Entonces, esos medios de control y vigilancia podrían encabezarse en observar si el empleado utiliza los recursos empresariales con fines personales, y si podrían afectar a la esfera íntima de la persona o a procesos que deberían de estar al margen del alcance del poder de dirección. [61]

2.2.2.1.CONTROL DEL USO DEL ORDENADOR.

Existe un choque entre el derecho a la intimidad de los trabajadores y las facultades de vigilancia y control de la actividad laboral en el ámbito de las tecnologías de la información y comunicación implantadas en la empresa (correo electrónico, Internet, etc.), ya que es un cauce que encamina la información de carácter profesional, personal y

[59] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación… op.cit.,* pp.53-62.
[60] Moreno Vida, M.N., *Las facultades de control fuera de la jornada de trabajo…op cit*., núm.150*,* p.162.
[61] Rodríguez Cardo, I.A., *Política empresarial previa y supresión de la expectativa de privacidad: una reflexión crítica sobre las facultades de control del ordenador utilizado por el trabajador*, Temas Laborales, núm. 126, (2014), pp.170 y 171; Fernández Villazón, L.A., Las facultades empresariales de control de la actividad laboral. Pamplona, Aranzadi, 2003, p.184 y ss.

privada. [62] De hecho, decenas de millones de trabajadores, que usan su ordenador, pues son espiados por sus empresas, debido a la incorporación en las empresas las masivas tecnologías de la información y del conocimiento. [63]

Tanto el Tribunal Constitucional como el Tribunal Supremo, señalan que los intereses en juego son, el derecho a la intimidad y al secreto de las comunicaciones del empleado, y también, el derecho empresarial a verificar el cumplimiento por parte del trabajador de sus obligaciones laborales, conforme al artículo 20.3 ET. Por ello, el derecho a la intimidad es determinante a la hora de advertir al trabajador en cuanto a las correctas reglas de uso sobres los instrumentos informáticos, los cuales, hayan sido facilitados al trabajador.

De este modo, el control que realiza la empresa, debe siempre respetar los principios y criterios de proporcionalidad en virtud de la Constitución Española y por la interpretación que realizan los órganos judiciales.

El TEDH, en 2019, en virtud del artículo 87 LOPDGDD, manifiesta que, en la protección de la intimidad, el empresario solo podrá acceder a los contenidos derivados del uso de estos dispositivos, a efectos de controlar el cumplimiento de las obligaciones laborales por parte de los empleados y de garantizar la integridad de respectivos dispositivos. De forma que, esa facultad de control, debe de ir acompañada de las siguientes obligaciones empresariales:

- Impera respecto al control del correo electrónico del trabajador, aquella que requiere la prohibición expresa de uso personal del mismo y además se tiene que dar una advertencia clara y previa al control (principio de transparencia) que afecte a la intimidad o al secreto de las comunicaciones de la menor forma posible (principio de proporcionalidad), tanto a la intensidad del control como a los medios técnicos utilizados (principio de minimización). [64]

[62] Carrizosa Prieto, E., ´´El control empresarial sobre el uso de los equipos informáticos y la protección del derecho a la intimidad de los trabajadores. Sentencia del Tribunal Supremo, Sala de lo Social, de 6 de octubre de 2011", *Temas Laborales*, núm.116, (2012), p. 266.
[63] Verdú Macia, V., (2002) "Espionaje sobre el empleado", El País, Edición Andalucía, 7 de abril, núm.11, (Disponible en https://elpais.com/diario/2002/04/07/domingo/1018151560_850215.html)
[64] Rodríguez Escanciano, S., (2019), ''Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de protección de datos", en Revista Vasca de Gestión de Personas y Organizaciones Públicas, núm. 16, p. 114.

- Los empleados, tienen que ser informados de los criterios de uso que se establezcan, y dicho control debe de estar justificado, y de producirse este, pues deberá de tener unas garantías efectivas a favor del trabajador. Dicha información, debe de ser clara y transparente y ha de realizarse antes de que se active y comience el control.[65] Existe un deber de informar a los trabajadores sobre los criterios de uso de los dispositivos digitales. [66]
- La LOPDGDD, establece límites en lo que respecta al poder supervisión empresarial para poder proteger el derecho de la intimidad de los trabajadores y empleados públicos tanto en el uso de los dispositivos digitales puestos a disposición por su empresario, conforme al artículo 87, entonces hay que respetar la intimidad del empleado reconocida en virtud de los usos sociales y los derechos contemplados constitucionalmente. [67]
- Hay que establecer, los criterios de utilización de los dispositivos digitales, con la participación de los representantes de los trabajadores si los hubiese.
- En el caso de que se permita el uso de los dispositivos con fines privados, pues el acceso a los mismos por parte del empresario, tiene que cumplir unas condiciones, como especificar los usos autorizados y que aparezcan ciertas garantías para salvaguardar la intimidad de los empleados, como, por ejemplo, sería determinar los periodos en que los dispositivos podrán utilizarse para esos fines privados. [68]

Dentro de los sistemas de control de la actividad laboral, en especial, del control del uso del ordenador, destacan los Proxys de bloqueo y Firewalls o cortafuegos:

- Proxys de Bloqueo:

Las empresas pueden controlar las comunicaciones o el uso privado de Internet en el trabajo, monitorizar las comunicaciones de los trabajadores y sancionarlos por el uso personal que hagan de los instrumentos informáticos, siempre que se hayan advertido a estos sobre el alcance y finalidad de ese control.

[65] Valdés Dal-Ré,F., ‘’Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa”. Revista de Derecho Social, Nº.79, (2017), p.15 y ss.
[66] Quílez Moreno, J.M., (2019) ,*La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores*. Revista Española de Derecho del Trabajo, núm.21, Estudios Editorial Aranzadi, S.A.U., Cizur Menor, p.10.
[67] Moreno Pérez, J.L. y Ortega Lozano, P.G., (2019),“El control empresarial del correo electrónico del trabajador”. *Temas Laborales*, núm,. 150, p.156.
[68] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación…op.cit.,* pp.62-68.

Para garantizar la vigilancia hacia los trabajadores sin interferir en el derecho a su privacidad, pues las empresas deben seguir de forma obligatoria los siguientes pasos:

- Comunicar el control de Internet, y deberá de quedar constancia de ello por escrito, independientemente de la forma en que se comunique.
- Delimitar qué está prohibido y qué no, de forma detallada y clara.
- Especificar los dispositivos de vigilancia que se quieran implantar en la empresa.

El control del ordenador, se puede hacer por medio de la instalación de filtros o proxys. Un proxy, es una herramienta que hace de intermediaria entre un ordenador y una dirección web, es decir, a través de un servidor proxy, un equipo de la red empresarial está conectado de forma directa a internet, filtrando y distribuyendo el acceso al resto de equipo de la empresa. Destaca el Proxy transparente, caracterizado por su desconocimiento por parte de los usuarios sobre su existencia. Y el proxy funciona por medio de sistemas tales como:

- Whitelist: se fija un listado de direcciones web permitidas, las cuales serán las únicas a las que pueda acceder el trabajador.
- Blacklist: establece un listado de direcciones web no permitidas, por tanto, quedarían restringidas y el trabajador no podría acceder a ellas.

En general, las funciones de un proxy son: controlar el acceso a Internet de los trabajadores, registrar el tráfico, filtrar información para no contestar a solicitudes que el proxy deteste que están prohibidas o son peligrosas, mantener el anonimato de los clientes y mejorar el rendimiento de la red gracias a la memoria caché que integra el proxy.

- Firewalls o cortafuegos:

Consiste en una fórmula en la que la empresa puede evitar la utilización extralaboral de Internet por parte de sus trabajadores, por tanto, se restringe el uso del mismo abiertamente con conocimiento de estos. Es un dispositivo de seguridad informática situado entre la red interna de una empresa e Internet y tiene el fin de evitar accesos no autorizados desde fuera de la red de la empresa. Estos dispositivos vienen incluidos en el sistema operativo del ordenador, cuya característica es la facilitación que tiene para poder bloquear cualquier tipo de programa o web desde el mismo ordenador.

Las funciones de control del ordenador cuando es usado por el trabajador son: eliminar el acceso a redes sociales, bloqueo de todo tipo de chats, bloqueo de descargas desde Internet, restricción de la utilización de las Webs (se bloquean por sectores, como, chat, búsquedas de empleo, compras online, etc.), restricción de las descargas, etc.

También, el firewall, puede rastrear, de modo que, el empresario puede tener conocimiento de los sitios que son visitados por un empleado concreto. Asimismo, las empresas pueden llevar a cabo un control sin repercutir negativamente en el ambiente laboral.

Las empresas pueden utilizar para garantizar una ejecución adecuada del trabajo de sus trabajadores los siguientes mecanismos:

- Insertar un filtro de palabras clave, es decir, la empresa puede integrar palabras clave prohibidas.
- Insertar un filtro de URLs, es decir, la empresa incorpora un sitio web específico el cual no podrá ser consultado por sus trabajadores.
- Insertar un filtro de tipo de archivos. Consiste en filtrar por tipo de archivos, y sirve para evitar que los empleados dediquen su tiempo de jornada laboral a descargar por ejemplo música o vídeos de ocio. [69]

2.2.2.2.CONTROL CON CÁMARAS DE VÍDEO.

Actualmente, las cámaras se encuentran en una infinidad de espacios, y sobre ello hay diferentes opiniones. Unos dicen que estos dispositivos, otorgan seguridad en todos los aspectos, y otros opinan que sienten cierto temor de verse sometidos a una constante vigilancia. Dicho temor, se debe a que las cámaras no están solo vigiladas por policía, gobiernos, motivos de seguridad, etc. sino que muchas cámaras se encuentran en manos privadas, sobrepasando los valores y principios de la ética y lo lícito.

Un sistema de videovigilancia es una estructura de captación de imágenes, e incluso, sonido, en un ámbito geográfico específico, cuyas imágenes captadas pueden ser reproducidas. Por tanto, la instalación de estos sistemas no debe ser algo eventual, sino que debe concretarse a fines motivados.

El retrato de una persona, en la que lo identifique o pueda ser identificado, pues se trataría de un dato de carácter personal, que puede ser objeto de tratamiento para distintas

[69] *Ibídem,* pp.69-72.

finalidades. [70] La videovigilancia, tenía el fin de garantizar la seguridad de los bienes, instalaciones y de las personas, pero hoy día se ha convertido además en un medio de control laboral muy frecuente y efectivo, que genera conflictos y disputas entre trabajadores y empresas. Con el gran aumento de las capacidades y tratamientos que pueden hacerse por medio de las imágenes, pues esto da lugar a que aumenten los riesgos derivados de la videovigilancia, debido a que podría dar lugar a la creación de perfiles.

Sin embargo, el GT29, entiende que no es una medida proporcional estos tratamientos en función de los derechos y libertades de los trabajadores, por ello, se entiende que sería ilícito.

En lo que concierne a los medios informáticos y tecnológicos, pues la jurisprudencia ha establecido criterios sobre los aspectos de acceso y las condiciones que permitirán utilizar los datos obtenidos como prueba válida a los efectos de acreditar los incumplimientos, pero no sucede lo mismo cuando el control empresarial de la conducta de los empleados se lleva a cabo para acreditar incumplimientos. [71]

En general, se permite a la empresa que pueda tratar las imágenes conseguidas por medio de sistemas de videovigilancia con el fin de supervisar a los empleados en el desempeño de sus funciones, siempre que estos hayan sido informados expresamente, clara y concisa. Se parte de la base de que tener imágenes de personas, a través de los medios digitales, pues es un dato de carácter personal, y por consecuente pues tiene un régimen de garantías respecto de los derechos inherentes, como pueden ser: el derecho a la intimidad, al honor, a la imagen, protección de datos implícito en el derecho a la limitación legal respecto del uso de la informática para asegurar el honor y la intimidad personal y familiar de los ciudadanos, y el ejercicio de sus derechos fundamentales que no son renunciables por situarse en una relación laboral, y por ende estos deben de respetarse.

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

[70] Vid. ´´Guía sobre el uso de videocámaras para seguridad y otras finalidades ", 2018, p.4.
[71] González González, C., (2018) *,Control empresarial de la actividad laboral mediante la videovigilancia y colisión de derechos fundamentales del trabajado,.* Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", Aranzadi Digital, nº1, Estudios y comentarios. Aranzadi, SAU, Cizur Menor, p.1.

de los trabajadores con discapacidad". Entonces, el empresario, garantizando por sus intereses legítimos, podrá controlar el grado de cumplimiento de las tareas que tiene cada trabajador, aunque el conflicto se produce entre el derecho al control laboral y a los derechos de los trabajadores, tales como el derecho a la intimidad, consagrado en el artículo 18.1 CE, y a la protección de datos, consagrado en el artículo 18.4 CE.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), tiene el fin de sancionar el uso de los datos personales para objetivos incompatibles con aquellas para las que los datos hubieran sido obtenidos, por esto, el sistema de videovigilancia con el fin de realizar un control laboral, pues debe de estar relacionado con este objetivo o no en la propia seguridad patrimonial del centro de trabajo. [72]

El artículo 20 bis ET, reconoce el derecho de intimidad de los empleados frente al uso de dispositivos de videovigilancia y geolocalización. Aunque el artículo 89 LOPDGDD, regula de forma expresa el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. Se reconocen las siguientes pautas legales:

- El poder de dirección y control del empleador sobre el desarrollo de la actividad laboral por parte de sus empleados, se podrá llevar a cabo por el tratamiento de las imágenes obtenidas por medio de sistemas de cámaras o videocámaras siempre que estas estén de forma legal, en virtud del artículo 20.3 ET, y con los límites del artículo 89.1 LOPDGDD. [73]
- El empresario, debe de informar de forma previa, clara, expresa y concisa a sus trabajadores sobre el uso de estos dispositivos. Se debe expresar que dichas imágenes tienen el objetivo de preservar la seguridad de las personas, bienes o instalaciones, y que pueden ser tratadas para controlar el correcto desempeño de la actividad laboral de los empleados.
- Si por medio de un sistema de videovigilancia, se capta que se está cometiendo un acto ilícito por los trabajadores, pues se entenderá cumplido el deber de informar cuando se hubiera colocado un distintivo informativo en un espacio suficientemente visible (cartel de videovigilancia) indicando que la zona está

[72] BOE NÚM,.298, de 14 de diciembre de 1999.
[73] Artículo 22.4 LOPDGDD.

videovigilada e identificando, la existencia del tratamiento de los datos, las condiciones , identidad del responsable y la posibilidad de ejercitar los derechos de acceso, rectificación, limitación del tratamiento y la supresión de los datos.

- La recopilación de imágenes, de carácter generalmente personal, debe garantizar el principio de calidad de los datos. Estos datos, se podrán obtener para su tratamiento cuando sean adecuados, pertinentes y no excesivos respecto al ámbito y a los objetivos legítimos que se hayan obtenido. Por tanto, el uso de cámaras clandestinas, deben de restringirse al máximo, pudiendo solo estar en situaciones graves y excepcionales. En general, las grabaciones, en virtud de la AEPD, se pueden conservar durante un mes, excepto si estas son necesarias para la investigación judicial de un posible delito, que, en este caso, se podrá almacenar durante un periodo de tiempo más largo.
- La información que se ha recogido por estos medios, no será apta como prueba en un juicio ni tampoco cuando se enfoque a un trabajador en pleno delito ilícito, excepto si se coloca un dispositivo informando de que hay sistemas de vigilancia y el procedimiento para ejercitar sus derechos. Destaca el caso López Ribalda y otros vs España. En el caso López Ribalda, se pusieron cámaras ocultas para vigilar a los trabajadores de un supermercado, y fueron pillados detrayendo género. Posteriormente, estos reconocieron su participación y fueron despedidos, pero lo impugnaron ya que alegaron la vulneración al derecho a la intimidad, y el TEDH falló diciendo que la medida era desproporcionada y vulneraba el derecho a la intimidad, ya que no se informó a los empleados de la instalación de cámaras de videovigilancia.
- Se deben de respetar los principios de proporcionalidad e intervención mínima. La proporcionalidad se debe evaluar si el uso de estos dispositivos es necesario para alcanzar el objetivo querido a conseguir, no existiendo otra medida que la sustituya y menos invasiva, y que sea equilibrada, conllevando beneficios para el interés general. La videovigilancia, como sistema permanente y continuado de control, no será admisible de forma general en las empresas, [74] ya que presenta

[74] Mercader Uguina, J.R., (2019), *Protección de datos y garantía de los derechos digitales en las relaciones laborales,* p.139; y García Murcia,J. y Rodríguez Cardo, I.A., *La Protección de los datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo,* Revista Española de Derecho del Trabajo, núm.216,p.39.

problemas para la privacidad de los trabajadores, como es la forma continuada de grabar la conducta del empleado.

- Está prohibido la instalación de sistemas de grabación de sonidos o de videovigilancia en lugares de descanso de los empleados, excepto si se exige por razones de seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo.

Teniendo en cuenta la guía de la AEPD ; "Guía sobre el uso de videocámaras para seguridad y otras finalidades", pues es un modelo que destaca por el registro de actividades. Manifiesta:

- Se debe de informar de la existencia de un sistema de videovigilancia, de forma personal a los trabajadores, o por medio de representantes sindicales, asegurando la recepción de la información. Entonces se deberá de poner un cartel visible en los accesos a las zonas que se encuentren vigiladas, indicando de forma clara la identidad del responsable de la instalación, ante quién y dónde pueden dirigirse para ejecutar los derechos que establece la legislación de protección de datos y dónde se puede tener más información respecto al tratamiento de datos de carácter personal.
- Los sistemas de videovigilancia que se encuentren en la empresa para llevar a cabo un sistema de control, solo se instalarán cuando haya una conexión de proporcionalidad entre el fin a conseguir y el modo en el que se traten las imágenes, no existiendo otra medida más adecuada.
- Las cámaras solo captarán imágenes de los espacios imprescindibles para el control laboral. Por tanto, no se instalarán cámaras en espacios de baños, vestuarios, descanso de los trabajadores, etc.
- No se registrarán conversaciones privadas.

Sin embargo, se produjo un impacto en la jurisprudencia, como consecuencia de la sentencia mencionada anteriormente, tal y como es la Sentencia de la Gran Sala del TEDH de 17 de octubre de 2019, Asunto Ribalda y otros, 1874/13 y 8567/13, debido a su fuerza aplicativa, conforme al artículo 10.2 CE, repercusiones sustantivas y procesales. Tanto el

TC y el TS, debieron de adaptar sus criterios a las exigencias informativas de respectiva sentencia[75]. Destaca sobre esta sentencia:

- Los límites inherentes al control empresarial por medio de la videovigilancia son, el respeto de los derechos fundamentales del empleado y los derechos a la intimidad, a la imagen y a la protección de datos personales. De este modo, la medida de control solamente será válida si supera el juicio de proporcionalidad, es decir, si aprueba que sea un sistema idóneo, necesario y proporcional.
- Hay que informar sobre el alcance de la medida, y esta debe de informarse de forma expresa del objetivo del sistema instalado, teniendo que concretar el empleador el fin sancionador si se realiza incumplimientos laborales por parte de los trabajadores.
- Se debe de otorgar dicha información en el momento exacto de cuando se instalan las cámaras, y también cada vez que se contrate a un trabajador en la empresa.
- Llevar a cabo la instalación de cámaras en el centro de trabajo, sin informar de ello a los empleadores, los cuales, quedarán sometidos a vigilancia, o a sus representantes, pues no es legal, y no deviene lícita por grabar un acto de una comisión de un acto ilícito.
- Un acto ilícito, es aquel que acto contrario, el cual contrapone el Ordenamiento Jurídico, constituyendo de tal forma un delito, y esto incluye como, por ejemplo, incumplimientos de las obligaciones laborales e infracciones administrativas.
- En una vigilancia diaria, la instalación de cámaras ocultas, no supone una vulneración desorbitada de la intimidad del empleado cuando esté justificada por existir "indicios" de que se están cometiendo actos ilícitos, como la comisión de actos graves que afecten al patrimonio o seguridad de la empresa o de sus trabajadores (no de infracciones laborales de escasa importancia), que, por medio de otros sistemas de control menos invasivos, pues no podrían detectarse.
- Según la LOPDGDD, si las cámaras de vigilancia captan negocios ilícitos flagrantes, pues la prueba es válida, aunque no se haya informado exactamente como se debía y solo aparezca que se está ante una zona videovigilada. Esto quiere decir que el empleado que cometió el acto ilícito pues puede ser sancionado, pero esto fue superado tras la sentencia del TEDH.

[75] González González,C., *Control empresarial de la actividad laboral mediante la vigilancia…op.cit.*, pp.17-18.

- El RGPD, alega el deber de informar sobre la finalidad del tratamiento de los datos personales, asegurando el derecho de la protección de datos. Y no llevar a cabo el deber de informar de la finalidad de las cámaras de videovigilancia pues conlleva que la LOPDGDD no respeta el derecho a la privacidad y a la protección de datos personales, en virtud de respectiva sentencia.

Por ende, la regulación normativa, y las interpretaciones judiciales tanto del TC como del TS, pues establecen unas bases de mínimos, las cuales, aseguran la efectividad probatoria de las imágenes y los derechos fundamentales de los empleados. Sin embargo, la sentencia del TEDH impuso el deber de informar que tiene la empresa en relación a las garantías propias del derecho a la protección de datos. [76] De hecho, la Jurisdicción de los Social, ha adaptado sus interpretaciones y en sus resoluciones pues ya entiende la prueba ilícita cuando no se cumplen los protocolos que aseguran los derechos fundamentales de los empleados. Una sentencia destacada, sería la Sentencia del Juzgado de lo Social nº3 de Pamplona[77], caracterizado por un despido disciplinario de un empleado debido a su intervención en un conflicto con otro empleado, y declaró la nulidad de la prueba que consistía en grabaciones de vídeo, ya que vulneraban el derecho a la intimidad y a la protección de datos del empleado. El Juzgado resolvió diciendo que cuando se trata de la vulneración del derecho a la protección de datos, en virtud del artículo 18.4 CE, lo relevante es el deber que tiene la empresa de informar a los trabajadores como medio único de alcanzar una protección efectiva del derecho de autodeterminación informativa inherente al derecho a la protección de datos.[78]

2.2.2.3.LA GRABACIÓN DE SONIDO.

El audio, la voz, aparece reconocido dentro del RGPD bajo el carácter de dato personal, ya que, por medio de esta pues se puede reconocer a una persona. Da lugar a la protección de varios derechos tales como: el derecho que se reconoce al empresario vía ET de que pueda valerse de medidas de control para la actividad laboral (instalación de cámaras de grabación de vídeo y/o audio, y el derecho a la protección de datos de los trabajadores.

Según el TC, la instalación de micrófonos que permite la grabación de audio continuado entre trabajadores, trabajadores y clientes, pues son acciones que sobrepasan las

[76] González González ,C., *Control empresarial de la actividad laboral mediante la videovigilancia…op.cit.,* p.18.
[77] Sentencia 52/2019, de 18 de febrero (Rec. 875/2018).
[78] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación…op.cit.,* p.73-82.

facultades recogidas en el ET. Entonces, dichas grabaciones pues se dan en espacios donde hay tanto conversaciones privadas, como conversaciones que carecen de interés empresarial.

Destaca la sentencia, STC 98/2000 [79], caracterizada por un caso de vigilancia conocida e informada, en la que era relevante la instalación por la empresa "Casino de la Toja" de un sistema de captación y grabación de sonido en ciertas zonas del centro de trabajo (caja y ruleta francesa), había vulnerado el derecho a la intimidad personal del empleado. La empresa instaló el sistema de grabación de sonido, aunque ya había un sistema de grabación de imágenes, y lo realizó por mera seguridad. El sistema instalado, no fue acreditado en lo que concierne a la instalación, permitiendo una audición continuada e indiscriminada respecto a todas las conversaciones. Teniendo en cuenta el principio de proporcionalidad pues el TC, entiende que el sistema no atendía al criterio de necesidad, ya que la empresa tenía otros sistemas instalados de videovigilancia, por tanto se da el amparo a la persona trabajadora, en virtud de la medida desproporcionada, ya que se obtenían conversaciones privadas, tanto de los clientes como de los empleados del casino, siendo conversaciones totalmente ajenas a la empresa y por ende insignificantes respecto del control del cumplimiento laboral. [80]

Sin embargo, existe la posibilidad de forma cierta y excepcional, el poder instalar como medida preventiva un sistema de vigilancia ante un incumplimiento laboral, sin tener el deber de informar al trabajador que es vigilado. Esto aparece con la TSJ de Madrid, en la Sentencia de 9 de febrero de 2015[81], aplicando el argumento de la "instalación y grabación puntual ante sospechas de incumplimiento"[82], en casos de "instalación puntual y temporal de una cámara tras acreditadas razonables sospechas de incumplimientos contractuales que se emplea con la exclusiva finalidad de verificación de tales hechos ". Aunque, las grabaciones indiscriminadas de voz pueden ser tenidas como desproporcionadas al tener una gran intromisión en el derecho a la intimidad [83].

[79] De 18 de abril de 2000 (Rec. Amparo 4015/1996). Vulneración del derecho a la intimidad personal: instalación de aparatos de captación y grabación del sonido en el centro de trabajo que no es imprescindible para la seguridad y buen funcionamiento de la empresa.
[80] Ibídem, p.85.
[81] Sentencia TSJ de Madrid, Sala de lo Social, N.º 84/2015. (Rec. 886/2014)
[82] STC 186/2000, de 10 de julio.
[83]STSJ de Cataluña, de 22 de mayo, de 2015.

2.2.2.4.SISTEMAS DE GEOLOCALIZACIÓN.

Los sistemas de geolocalización, son aquellos, que facilitan la obtención de cualquier dato tratado en una red de comunicaciones electrónicas, que señala la posición geográfica del terminal del usuario de un servicio de comunicaciones electrónicas disponible para el público[84]. La geolocalización, aporta información adicional en relación al trayecto, tiempo invertido, tiempos de parada o de espera, etc., además de facilitar la ubicación. Es por ello, que se considera como una forma de control a distancia de la prestación laboral en los numerosos casos en los que la supervisión personal directa es imposible, complicada o menos eficiente o incluso más costosa. Entonces pues este sistema se enfoca a los trabajos que se caracterizan por estar fuera del espacio de control del empleador (como, por ejemplo, los barrenderos, empresas de transporte y reparto, agentes de Correos, etc.) y también se enfoca a los trabajos por motivos de seguridad (atender alguna emergencia que tenga el empleado) o de cercanía al cliente (se desplaza el técnico más próximo a la vivienda del cliente).

En relación con España, pues es la que menos avanzada está en su implantación, mientras que, en otros países, se utiliza de forma frecuente dicha instalación de vigilancia empresarial como sistema de control. Se regula en el artículo 90 LOPDGDD. Asimismo, puede dar lugar un despido disciplinario de un trabajador, en caso de que no active el dispositivo GPS del móvil para poder localizarlo durante su jornada laboral, enfocando pues el incumplimiento del empleado en la buena fe contractual y el abuso de confianza[85]. Sin embargo, pues las empresas en ciertas veces, registran el comienzo y finalización de la jornada de trabajo, pero también pues chequean al empleado en su tiempo privado de ocio.

De otro modo, destaca el riesgo que se tiene tras tener un seguimiento que resulte invasivo para la intimidad del trabajador, siempre que este esté activado y fuera de la jornada laboral, conforme al GPS (Global Positioning System) y el GMS (Global System for Mobile Communication).[86]

[84] Vid. Apartado 9 del Anexo II (Definiciones) de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, los datos de localización.
[85] STSJ Andalucía, Sala de lo Social, 18 de septiembre de 2017 (REC.770/2017).
[86] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación…op.cit.,* p.86.

El GT29, en Dictamen 13/2011 sobre los servicios de geolocalización[87] manifestaba, que hay que elegir los medios menos intrusivos que faciliten las funciones de control laboral, dando la opción al trabajador de poder desactivar cualquier dispositivo de vigilancia fuera de las horas de trabajo.

Desde la perspectiva jurídica, los datos de localización, pues son datos de carácter personal, dada por una persona física identificada o identificable, sometida a la normativa de la protección de datos. Dichos datos, tienen un carácter sensible, por ello, están especialmente protegidos (además de los datos genéticos y biométricos). La legitimación del tratamiento de estos datos, se encuentran en base a la ejecución de un contrato conforme al artículo 6 RGPD y el artículo 90 LOPDGDD en virtud del artículo 20.3 ET, en el que se permite al empleador que adopte las medidas adecuadas de vigilancia y control para acreditar el cumplimiento del empleado respecto de sus obligaciones y deberes laborales, teniendo en cuenta la consideración a su dignidad humana. Igualmente, aunque exista esta legitimación, pues hay que ofrecer el derecho de información, es decir, los datos que utiliza la empresa para sancionar pues tienen un carácter personal, y el haberlos obtenido sin saberlo el trabajador, pues vulneraría su intimidad personal, en virtud del artículo 18.1 CE, junto con el derecho a la protección de datos personales (artículo 18.4 CE).

Para poder desempeñar las funciones de control del artículo 20 ET, los empresarios, deben de informar de forma expresa, clara y sin lugar a dudas a los trabajadores, sobre la existencia y características de estos dispositivos, siempre que estas funciones se llevan a cabo dentro del marco legal y con los límites inherentes al mismo en su caso [88]. También, deberán de informarle sobre los derechos de acceso, rectificación, limitación del tratamiento y supresión (arts. 12-15,89 y 90 LOPDGDD). De este modo, se establece una obligación de información idéntica a la que se exige ante el uso de sistemas de grabación de sonido o videovigilancia.

Hay que tener en cuenta que una geolocalización indiscriminada del empleado, podría dar lugar al acceso a información íntima y sensible sin el consentimiento de su titular. [89]

[87] Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes. (881/11/ ES WP 185).
[88] STSJ Madrid de 21/03/2014. (Rec. 1952/2013).
[89] La Confederación de Consumidores y Usuarios (CECU), como parte de una acción coordinada por la Oficina Europea de Uniones de Consumidores, ha denunciado la política de geolocalización de Google ante la AEPD. Esta geolocalización viene impuesta en ciertos móviles, y CECU acusa a Google de tener

Una de las consecuencias respecto a la aplicación de normas de protección de datos, es la de revalorizar y reforzar el derecho a la información que tienen los titulares de datos y que al tener que darse en un momento exacto, lo convierte en un requisito para la licitud de la recogida y del tratamiento del dato. [90] Se declara la licitud de estos sistemas mediante nuestra jurisprudencia[91], siempre que exista una información hacia los empleados tanto de su instalación como el objetivo que pretende la misma. De tal modo que, cualquier dato puede ser recogido de forma lícita cuando se haya dado la previa información que recae sobre el empresario conforme al artículo 90.2 LOPDGDD (información previa sobre la instalación del GPS y de su finalidad, sometido a la jornada laboral y no cuando finaliza la jornada laboral).

En conclusión, pues la utilización de estos sistemas de geolocalización se vincula con la jurisprudencia obtenida tanto nacional como Europea, sobre el ejercicio de las facultades empresariales de dirección y control sobre la jornada laboral, en tanto que ni toda captación de los datos de que se trata es lícita con la mera condición de que se haya informado de ella, es decir, que la información es un requisito previo y necesario, pero tras este pues hay que realizar un análisis procediendo al juicio de ponderación e intervención mínima frente a la causa de justificación manifestada por el empleador.

3. EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA DEL TRABAJADOR.

3.1. TRATAMIENTO DE LOS DATOS PERSONALES DEL TRABAJADOR Y TRATAMIENTO DE DATOS PERSONALES EN LOS SUPUESTOS ESPECIALES.

El conjunto de datos, tiene su principal aspecto, en la falta de transparencia y de información, conforme a cómo se almacenan y se usan nuestros datos, estando sometidos a decisiones que desconocemos y que no podemos controlar. Con la llegada del BIG DATA, actualmente estamos en constante relación con dispositivos que obtienen datos

datos sensibles sin consentimiento explícito. Debido a su sistema de geolocalización, Google podría conocer la religión de un individuo por haber asistido a un determinado lugar de culto.

[90] González Ortega, S., *Las facultades de control a distancia… op.cit.,* p.66.

[91] STC 292/2000, entre otras.

personales[92], por ello, el tratamiento de los mismos, es inevitable conforme a las exigencias legales de hoy en día.

Los principios relativos al tratamiento de los datos personales, vienen reguladas en el artículo 5 y en el artículo 39, los cuales, han sido mencionados anteriormente.

Por otro lado, respecto al tratamiento de los datos personales del empleado en supuestos especiales, pues este se caracteriza en que generalmente, pueden suponer un riesgo mayor en su privacidad. Viene regulado en la LOPDGDD. Según el GT29, hay diferentes casos en los que se produce dicho tratamiento, y destacan:

- Tratamiento de datos durante un proceso de selección; a la hora de realizar una selección a un trabajador, da lugar a la cesión de una gran cantidad de datos personales por parte de los candidatos a esa oferta de empleo, por medio de un Currículum Vitae (en adelante, CV), en la entrevista personal o a través de un cuestionario. Dicho tratamiento de datos, varía en función de la forma en la que llega el CV, y respecto a ello, la AEPD:
    - Si la empresa recibe el CV tras poner un anuncio para desempeñar un trabajo concreto, la AEPD manifiesta que el anuncio publicado debe informar del contenido del artículo 5 LOPD.
    - SI el CV se entrega en mano, se le puede pedir al que solicita desempeñar ese puesto de trabajo que firme un consentimiento para el tratamiento de datos.
    - En el caso de un portal de empleo online, suele darse una cláusula relativa a la protección de datos de los candidatos.
    - Si el CV se remite por correo postal o electrónico, se le puede remitir información a través del mismo.
    - Si el CV se presenta en un mostrador u oficina de atención, el candidato, deberá de ser informado en el lugar, ya sea por medio de carteles, documento de acuse de recibo, etc.
    - Si la empresa introduce el CV en su base de datos, debe de informar al candidato en el mes siguiente, excepto si el mismo ya ha sido informado anteriormente.

[92] Bastidas Cid, Y.V., *El cumplimiento de los principios del tratamiento de datos personales establecidos en el RGPD de la unión europea en proyectos de Big Data* , Informática y Derecho: Revista Iberoamericana de Derecho Informática, nº6, 2019, p.29.

  - Los datos personales que aparecen el CV, tienen que estar actualizados, por tanto, si transcurre más 24 meses sin haber sido verificados, pues entonces han de ser eliminados.
  - Excepto si el candidato o empleado den su consentimiento, la empresa no puede remitir del CV a otra empresa del grupo, ya que, de tal modo, se estaría haciendo una cesión de datos personales a un tercero, es por ello, que requiere previamente el consentimiento del trabajador o candidato.

En el proceso de selección de un candidato, la empresa no podrá pedir referencias sobre el mismo a sus empresarios anteriores, excepto si se tiene el consentimiento del mismo o bien existe una finalidad legítima, como contrastar los datos que aparecen en el CV de un candidato.

- Tratamiento de datos de redes sociales de los trabajadores. Se caracteriza en que estas buscan información sobre futuros candidatos para desempeñar un puesto de trabajo antes de ser contratado. Como norma general, no se debería de realizar el tratamiento de los perfiles de los trabajadores en redes sociales. El GT29[93], menciona los siguientes requisitos para que el tratamiento de los datos obtenidos por medio de redes sociales sea conforme a la ley:
  - Los empresarios no deben considerar que si el perfil de una persona en redes sociales es de acceso público pues está permitido que traten esos datos para sus propios objetivos.
  - Los empresarios pueden recoger y tratar datos personales relativos a las personas que demandan empleo siempre que dicha recopilación sea necesaria y adecuada, para poder llevar a cabo el trabajo solicitado.
  - No cabe ningún fundamento jurídico en el que un empresario solicite "amistad" a los trabajadores, ni viceversa.

Por tanto, se prohíbe que las empresas consideren esa información sin tener previamente el consentimiento de la persona afectada. De hecho, la Recomendación CM/Rec (2015) 5 del Comité de Ministros del Consejo de Europa, establece que los empresarios tienen el deber de abstenerse a poder exigir o pedir a un trabajador o candidato a optar a un empleo tener acceso a determinadas informaciones que el mismo publique y comparta por medio de las redes sociales.

[93] Dictamen GT29 2/2017.

De tal modo, tras todo lo mencionado anteriormente, se hace hincapié en los requisitos para poder efectuar un tratamiento de datos de carácter laboral, como son los de proporcionalidad, minimización de datos, transparencia, etc. Y, a la hora de utilizar el interés legítimo como fundamento jurídico, pues que el tratamiento devenga totalmente necesario a un fin legítimo, ajustado a los principios de proporcionalidad y subsidiariedad.

En consecuente y en virtud de la doctrina de los tribunales, el empleador puede tratar datos de las redes sociales del candidato al empleo o de un trabajador, siempre que se pueda acreditar que hay un fin legítimo, el cual, sea pertinente a realizar dicha actuación y que la información esté publicada en abierto. De lo contrario, se entiende que no hay cierta legitimidad cuando dicha publicación aparece como restringida el acceso a la misma. [94]

- Tratamiento de datos derivado de la monitorización de las tecnologías de la comunicación e información dentro del lugar de trabajo. El GT29, verifica que los actuales desarrollos tecnológicos toleran nuevas maneras de monitorización más intrusivas e invasivas para constituir un fundamento legal para el tratamiento, independientemente de la tecnología a utilizar. En tal caso, se debe de comunicar a los trabajadores las políticas de uso de los sistemas en el trabajo. También, dicho Dictamen dice que la prevención debe de estar por encima de la detección, es decir, es más conveniente evitar un uso indebido por medios técnicos que utilizar recursos para detectar el uso indebido. [95]
- Tratamiento de datos derivado de la monitorización de las tecnologías de comunicación e información fuera del lugar de trabajo:
    - Trabajo desde casa o en remoto. Hay que adoptar las medidas técnicas necesaria, sin dar a entender que el empresario puede instalar medidas de seguridad como un software que registre pulsaciones de teclas y movimientos de ratón, qué aplicaciones se han usado y durante cuánto tiempo, etc.
    - Utilización de herramientas propias (BYOD). Para evitar el control de la información privada, hay que establecer medidas pertinentes para diferenciar entre el uso privado y corporativo del dispositivo. Por ello, hay

[94] Cfr. STSJ de Galicia de 25 de abril de 2013.
[95] Fernández Ramírez, M*., El derecho del trabajador a la autodeterminación…op.cit.,* p. 214.

que realizar un informe de evaluación de riesgos y de evaluación del impacto en la vida privada del trabajador.

  - Gestión de dispositivos móviles. Esta permite localizar dispositivos, aumentar aplicaciones o configuraciones, y eliminar datos de forma remota. Dicho dictamen GT29, manifiesta que hay que realizar un informe de evaluación de impacto antes de instalar una tecnología de este carácter, con el fin de ver si la tecnología a querer implantar es necesaria, y en el caso de que lo fuese, pues si el tratamiento de datos resultante, cumple con los principios de proporcionalidad y subsidiariedad. Además, los empleados deberán estar informados sobre qué seguimiento se realiza y las consecuencias que tiene para los mismos.
  - Dispositivos wearables. Si los empleados usan este dispositivo, puede dar lugar al tratamiento de datos de salud, y este está prohibido en virtud del artículo 8 de la Directiva. También, aunque el trabajador otorgue su consentimiento expreso, será complicado legitimar dicho tratamiento debido a la desigualdad inherente a la relación laboral y a los datos de la salud. Por lo tanto, el tratamiento sería ilegal.

- Tratamientos que impliquen la cesión de datos a terceros. Actualmente, hay empresas que facilitan datos de sus trabajadores a sus clientes y dichos datos pueden considerarse excesivos. Además, el consentimiento del trabajador, no puede considerarse libre, y deriva de ello que no se puede legitimar el tratamiento de sus datos. Aunque, el GT29 alega que para que el tratamiento de datos tenga un fundamento jurídico óptimo, este tendrá que ser proporcional. [96]

3.2.EL DERECHO DE INFORMACIÓN Y PRINCIPIO DE TRANSPARENCIA.

El derecho de información, se sustenta en el derecho fundamental como es el derecho a la intimidad personal del trabajador (artículo 18.1 CE), y al derecho a la protección de datos de carácter personal (artículo 18.4 CE). El TC, manifiesta que "*el deber de información previa forma parte del contenido esencial del derecho a la protección de datos*"[97]. El deber de informar, está vinculado con el principio de transparencia, y debe

[96] *Ibídem*, p. 215
[97] SSTC 29/2013 y 39/2016.

de tenerlo en cuenta el empresario, en el tratamiento de los datos personales para asegurar los derechos de sus empleados.

El deber de transparencia y el deber de informar, vienen regulados en los arts. 12,13 y 14 RGPD.

Hay que comprobar si el empleado ha sido informado de forma previa sobre la posibilidad de que el empresario puede tomar medidas para supervisar su correspondencia y otras comunicaciones, así como si al empleado se le han otorgado garantías adecuadas, sobre todo, cuando dichas medidas de supervisión pueden tener un carácter intrusivo, por medio de la información del seguimiento de un procedimiento o protocolo en los supuestos en los que fuese necesario la intervención del dispositivo.

Por ello, el empleador debe informar, de forma previa a la puesta en funcionamiento del sistema, sobre el objetivo del control empresarial en captar imágenes a los trabajadores y a la representación sindical, a través de un medio que asegure que la información ha sido recibida. Siempre respetando la dignidad e intimidad de los trabajadores.

La información, puede ser otorgada por medio del contrato de trabajo, cláusula contractual, etc., y respecto si se tratase de dispositivos digitales, pues incorporarlo en una política corporativa de uso de medios informáticos, siendo debidamente comunicada a los trabajadores de la empresa.

Respecto a la información que debe proporcionarse a los interesados, comprende: la información sobre el responsable del tratamiento y la finalidad del tratamiento[98], indicando:

- Debe de ser concisa, transparente, inteligible y de fácil acceso, con un lenguaje comprensible, claro y sencillo, y la información será dada por escrito o por otros medios, si fuese necesario, a través de medios electrónicos.
- Tiene que ser concretada, a través de la colocación de un dispositivo informativo en un lugar suficientemente visible, los caracteres y el alcance del tratamiento de datos que iba a realizarse. Se facilita al trabajador la información básica y se le indica al mismo tiempo la dirección electrónica, sitio web u otro medio, para que pueda ver la restante información, conforme a los arts. 11 y 22.4 LOPDGDD. Además, la información debe de tener la identidad del responsable, finalidad del

[98] González González, C*., Control empresarial de la actividad laboral…op. cit.,* p. 22.

tratamiento, posibilidad de ejercer los derechos de los arts. 15-22 RGPD y la eventualidad de que los datos puedan ser usados para elaborar perfiles y su derecho de oposición.

- Si la información procede de un tercero, entonces, la información básica tendrá que incluir la categoría de los datos y las fuentes de las que procedan dichos datos. Por consiguiente, el principio de transparencia obliga a que la información y comunicación que se realiza al trabajador sea accesible y comprensible.

El hecho de no ser el consentimiento del trabajador la base que legitima este tratamiento de datos personales, da lugar a que el empleador tenga una obligación y un deber de información hacia el trabajador que se observa como una pieza clave y esencial en la licitud de los sistemas de control. [99]

3.3.CONSERVACIÓN DE LOS DATOS DEL TRABAJADOR.

En general, muchas empresas, optan por borrar los datos personales una vez que finaliza la relación con el interesado, debido al miedo por las altas sanciones que manifiesta la normativa. Sin embargo, otras empresas optan, bien por desconocimiento o bien por temor a quedarse sin uno de sus de sus activos más importantes, como son, los datos personales, optan por conservar respectiva información sin tiempo limitado, es decir, de forma indefinida. De este modo, escasas empresas tienen en sus procesos internos procedimientos caracterizados por comprobar cuándo un dato ya no es relevante y debe ser bloqueado y destruido.

El RGPD establece, que, una vez acabado el tratamiento por cuenta del responsable, el encargado debe devolver o suprimir los datos personales, salvo si el Derecho de la Unión obliga a conservar los datos. La norma no establece un tiempo de conservación de forma expresa, sino que los datos deberán de ser cancelados si ya se acabó la finalidad con la que fueron recabados y no existe obligación alguna para el afectado. Destaca el artículo 32 LOPDGDD.

Asimismo, puede dar lugar a la problemática de que, los archivos que se conservan durante bastante tiempo, tienen el riesgo de vulnerar la privacidad y las leyes de protección de datos. Sin embargo, los que se destruyen demasiado rápido, podría contravenir la ley de prueba electrónica.

[99] Fernández Ramírez, M., *El derecho del trabajador a la autodeterminación…op.cit.,* pp. 219-221.

De entre todos los documentos que se deben de guardar durante cuatro años, están: el contrato de trabajo, resúmenes mensuales de los registros de jornada, recibos de salarios, copia de documentos de identidad de ciudadanos extranjeros, datos relativos a trabajadores temporales, datos de candidatos no seleccionados y comunicación del contenido de los contratos y de sus copias básicas a los Servicios Públicos de Empleo. Hay que tener en cuenta que, en nuestro país, las acciones que pueda iniciar de oficio la Seguridad Social o Hacienda contra las empresas, no prescriben hasta pasados 5 y 4 años respectivamente. [100]

4. EXTINCIÓN DE LA RELACIÓN LABORAL.

La extinción de la relación laboral consiste en el cese de forma definitiva de las obligaciones tanto por el empleador como por el empleado en un contrato de trabajo (una o varias personas dar su consentimiento para obligarse entre ambas), entendiendo este en la obligación recíproca de trabajar y remunerar o retribuir por el trabajo efectivo realizado.

La extinción de la relación laboral, puede darse por cumplimiento (expiración del tiempo pactado o cumplimiento de la condición resolutoria), desaparición, jubilación, o por decisión de las partes (mutuo acuerdo, voluntad del trabajado, o voluntad del empresario).[101]

El derecho a la protección de datos, también tiene un enfoque en el momento que surge la extinción de la relación laboral. Destaca:

- La carta de despido, puede comprender datos personales de la persona la cual ha sido despedida y de terceros (como los clientes) cuando estos sean adecuados y oportunos para su objetivo, y no datos personales que no sean importantes.
- Debe de haber medidas de seguridad, con el fin de que la carta de despido no sea alcanzable por terceras personas no legitimadas.
- Tras el cese de la relación, hay que llevar a cabo el proceso de bloqueo de los datos, en virtud del artículo LOPDGDD. Sin embargo, el tratamiento de los datos tras la extinción de la relación laboral puede ser admisible si hay otra base jurídica,

[100] *Ibídem,* pp. 221-223.
[101] «Extinción de las relaciones laborales», Wolters Kluwer, Disponible on line: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAASNjc3MTtbLUouLM_DxbIwMDS0NDA1OQQGZapUt-ckhlQaptWmJOcSoAmb8qKTUAAAA=WKE

> como sucede en el caso de que el empleador demostrase un interés legítimo y que las personas extrabajadoras hayan sido informadas del alcance del control de forma adecuada. De tal modo que, el empleador puede obtener el consentimiento del empleado para contactar en un futuro. El empresario, debe informarlas, y ellas tendrán un libre consentimiento para otorgarlo o no. Además, la comunicación de datos de un empleador anterior a uno nuevo, pues precisa el consentimiento del empleado. [102]

En lo que concierne a los datos, pues a la hora de llevar a cabo la extinción laboral, casi en todos los casos, se produce un uso de los datos personales del trabajador. Con la extinción del contrato laboral, desaparece el tratamiento de los datos del trabajador. Por tanto, en ese momento y a partir del mismo, pues no hay contrato cuya ejecución sea necesaria la recogida y el tratamiento, en virtud del artículo 6.1.b) RGPD. Esto quiere decir, que, si los datos fueron obtenidos con un objetivo determinado, y posteriormente se da el cumplimiento del contrato, que ya este deviene cesado, pues no va a poder darse el tratamiento de forma compatible, ya que se produce la extinción de la relación laboral que se tenía pactada, en virtud del artículo 5.1.b) RGPD. Además, el artículo 17.1 RGPD, manifiesta que el trabajador tendrá derecho a obtener la supresión de sus datos personales, cuando estos ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otros modos.

El artículo 32 de la LOPDGDD, señala que el responsable del tratamiento deberá bloquear los datos cuando procesa a su rectificación o supresión, en lugar de eliminarlos directamente.

De tal modo, el empleador, queda obligado a bloquear los datos, conforme al artículo 32.1 LOPDGDD, "1. *El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión. 2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de*

[102] Guía «La protección de datos en las relaciones laborales» (2021) ; Disponible on line: https://seu.uib.cat/digitalAssets/635/635869_la-proteccion-de-datos-en-las-relaciones-laborales.pdf

prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos".

De otro modo, una vez que se extingue la relación laboral, pueden surgir reclamaciones judiciales o extrajudiciales del trabajador o de las administraciones públicas por infracciones administrativas que deriven de datos personales del trabajador, por tanto, cada una de estas responsabilidades tiene un plazo de prescripción específico, establecidos en la normativa que resulte de aplicación y con la finalidad de exigencia de ciertas responsabilidades derivadas del tratamiento.

Por tanto, el bloqueo, aparece como un paso previo al borrado definitivo, en virtud en los casos tasados por la Ley. Y, dicho bloqueo posee efectos parecidos al borrado, pero no da lugar al borrado físico de los datos. [103]

5. CONCLUSIONES.

El derecho a la protección de datos, consagrado en el artículo 18.4 CE, deriva de nuestra vida privada e intimidad, en relación al avance de las nuevas tecnologías. De este modo, el avance tecnológico se entendía en un determinado contexto histórico que facilitaba la intromisión de terceras personas en lo que compete a información protegida, tales como conversaciones telefónicas, domicilio, registros privados, etc. Por ello, dieron lugar nuevas leyes caracterizadas en proteger los datos personales, protegiendo la transmisión de datos que hacen identificar a una persona. Por tanto, se deduce los derechos de acceso, rectificación, cancelación y oposición, respecto a la protección de datos y enfocado al ámbito laboral, ya que proporciona garantías y seguridad en cualquier actividad. Además, también los ordenamientos jurídicos han ido evolucionado conforme al avance de la tecnología, optando por garantizar derechos y estableciendo exigencias para las empresas, con respecto al tratamiento de los datos, intentando evitar así vulneraciones en los derechos de las personas.

De igual modo, pienso que la regulación actual, nos muestra cierta preocupación directa sobre una serie de derechos, en la que aún nos queda por avanzar. Además, la protección de datos, poco a poco, está tomando una posición cada vez más importante en el derecho, destacando la transcendencia social e institucional conforme a nuestros últimos días, y

[103] «Plazos de conservación y bloqueo», (2020) , Disponible on line: https://www.uria.com/documentos/circulares/1348/documento/12062/UM-nota.pdf?id=12062

aunque sea un campo considerado relativamente nuevo, está evolucionado de una forma abismal.

Asimismo, destaca, el anonimato, es decir, el secreto de los datos de una persona, respecto a su personalidad e inviolabilidad de la dignidad personal por el mero hecho de ser persona.

Hay que tener en cuenta el Data Privacy (protección de datos-derecho a proteger), el cual protege los datos de la utilización indebida, regulando su uso, borrado total o parcial, tratamiento de los datos, almacenamiento, etc. Y el Data Protection (herramienta para proteger) que son las políticas de seguridad establecidas para asegurar el correcto funcionamiento del Data Privacy.

Tras lo expuesto, para avanzar más sobre el tratamiento de los datos personales, esto, corresponden a los poderes públicos y autoridades competentes para promover garantías y otorgar una mayor seguridad jurídica respecto a la protección de datos, y deberán de perseguir finalidades estratégicas para aumentar la calidad de los datos personales. Y en lo que concierne a la UE, se intenta armonizar el nivel de protección para todos los Estados que forman parte, reforzando así el control sobre los datos de las personas, y garantizando un equilibrio entre los datos personales de los trabajadores y los nuevos avances de la tecnología. Es decir, que, para salvaguardar los derechos de las personas, pues es necesario que el derecho esté al mismo nivel tanto de la evolución tecnológica como de la social.

En conclusión, se está avanzando bastante respecto a la forma de tratamiento de los datos personales, gracias a ciertas aplicaciones tecnológicas, como sería el Big Data, y por ello hay que tener en nuestra sociedad un equilibro entre el derecho y que los datos personales no sean transferibles de forma fácil entre empresas, sin considerar nuestros derechos fundamentales. Por tanto, gracias al RGPD, pues se ha dado un paso más, de forma muy bien encaminada, pero que aún nos queda por avanzar, debido al gran avance de la tecnología, y por eso, tenemos que estar en constante actualización para estar en el mismo nivel que dichos avances.

6. BIBLIOGRAFÍA.

"Agencia Española de Protección de Datos", Madrid, Disponible on line: https://www.aepd.es/es

"Cesión de Datos a terceros" Disponible on line: https://protecciondatos-lopd.com/empresas/cesion-datos-terceros/

"Extinción de las relaciones laborales", Wolters Kluwer, Disponible on line: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAASNjc3MTtbLUouLM_DxbIwMDS0NDA1OQQGZapUt-ckhlQaptWmJOcSoAmb8qKTUAAAA=WKE

"Garantías para las transferencias de datos personales a terceros países u organizaciones internacionales", 26 de noviembre de 2021, Disponible on line: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales

"Plazos de conservación y bloqueo", Disponible on line: https://seu.uib.cat/digitalAssets/635/635869_la-proteccion-de-datos-en-las-relaciones-laborales.pdf

"Ubicación de los datos personales", Disponible on line: https://ayudaleyprotecciondatos.es/guia-rgpd/#Principios_relativos_al_tratamiento_de_datos_personales

BASTIDAS CID, Y.V., "El cumplimiento de los principios del tratamiento de datos personales establecidos en el RGPD de la unión europea en proyectos de Big Data ", *Informática y Derecho: Revista Iberoamericana de Derecho Informático* (segunda época), nº6, 2019, pp.15-48.

BLÁZQUEZ AGUDO, E.M., "El límite a los derechos fundamentales a la libertad de empresa", *en Aplicación práctica de la protección de datos en las relaciones laborales*. Editorial Wolters Kluwer, 2018. Madrid.

CARRIZOSA PRIETO, E., "El control empresarial sobre el uso de los equipos informáticos y la protección del derecho a la intimidad de los trabajadores. Sentencia del Tribunal Supremo, Sala de lo Social, de 6 de octubre de 2011", Temas Laborales, núm.116, (2012), p. 251-267.

CORTÉS OSORIO, J.M., MEDINA AGUIRRE, F.A. y MURIEL ESCOBAR, J.M., "Sistemas de seguridad basados en biometría", *Scientia et Technica*, Año XVII, N.º 46 (diciembre-2010). Universidad Tecnológica de Pereira, p.99.102.

CUERVO, J., Documento de trabajo sobre biometría, 13 de junio 2003. Disponible on line: https://www.informatica-juridica.com/documento-trabajo/documento-trabajo-biometria/

CRUZ RANGEL, L., ´´Biometría de iris vs. retina, sí, en realidad son diferentes´´, ID Noticias, 13 de agosto de 1014; NIETO, L.A., ´´Biometría de iris vs. Retina / Estudio Tecnológico", publicado el 28 de mayo de 2020.

DAVARA RODRÍGUEZ, M.A., "El humanismo tecnológico", Datos personales. Org. Revista de la Agencia de Protección de Datos de la Comunidad de Madrid, en aplicación al "El derecho al olvido en internet", El Consultor de los Ayuntamientos, núm.13, 2014, p.3.

Fernández Ramírez, Marina, "*El derecho del trabajador a la autodeterminación informativa en el marco de la actual empresa ´´neopanóptica",* Aranzadi, Pamplona, 2021.

GARCÍA MAHAMUT, R.., Y TOMÁS MALLÉN, B., ''El RGPD. Un enfoque nacional y comparado''. Tirant lo Blanch. Valencia, 2019.

GONZÁLEZ GONZÁLEZ, C., ´´Control empresarial de la actividad laboral mediante la videovigilancia y colisión de derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", *Aranzadi Digital,* núm.1, (2018), Estudios y comentarios. Aranzadi, SAU, Cizur Menor, p.1-37.

GONZÁLEZ ORTEGA, S., "Las facultades de control a distancia del trabajador: geolocalizadores y tacógrafos", *Temas Laborales*, núm.150, (2019), pp.45-70.

GOÑI SEIN, J.L., El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder de control empresarial, ed. Civitas, Madrid, 1998. "La nueva regulación Europea y Española de protección de datos y su aplicación al ámbito de la empresa.

Instituto Quatrecasas de Estrategia Legal en RRHH, "Documentos sobre el impacto de las nuevas tecnologías en la gestión de las personas y en las relaciones laborales". Wolters Kluwer. Madrid, 2020.

Instituto Quatrecasas, Documentos sobre el impacto de las nuevas tecnologías en la gestión de las personas y en las relaciones laborales, Wolters Kluwer, Madrid, 2020.

Universitat de Valencia, "Protección de Datos Personales, Disponible on line: https://www.uv.es/uvweb/servicio-informatica/es/normativa-procedimientos/proteccion-datos/preguntas-frecuentes-1285902056674.html

MERCADER UGUINA, J.R., "El mercado de trabajo y el empleo en un mundo digital". *Revista de Información Laboral*, núm.11, Editorial Aranzadi, Cizur Menor, (2018)

- "López Ribalda II: un camino de ida y vuelta", (2019).
- "Protección de datos y garantía de los derechos digitales en las relaciones laborales", ED. Francia Lefebvre. Claves Prácticas, Madrid, (2019).
- "Datos biométricos en los centros de trabajo", Trabajo y derecho: nueva revista de actualidad y relaciones laborales, N.º Extra 11, (2020).

MORENO DÍAZ, A.B., Reconocimiento facial automático mediante Técnicas de Visión Tridimensional, ed. Universidad Politécnica de Madrid, 2004.

MORENO PÉREZ, J.L. y ORTEGA LOZANO, P.G., "El control empresarial del correo electrónico del trabajador". Temas Laborales, nú,. 150, (2019),p.156.

MORENO VIDA, M.N., "Las facultades de control fuera de la jornada de trabajo: desconexión digital y control del trabajador", *Temas Laborales*, núm.150, (2019).

PIÑAR MAÑAS, J. L., Y RECIO GAYO, M., 2018. "El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea". Wolters Kluwer. (2018), Madrid.

POQUET CATALA, R., E. "El actual poder de dirección y control del empresario" Pamplona (Aranzadi), 2013, p.191

PRECIADO DOMENECH, C.H., "La videovigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos de carácter personal", *Revista de Derecho Social*, n.77, (2017).

- "El derecho a la protección de datos en el contrato de trabajo". Adaptado al nuevo Reglamento 679/2016, de 27 de abril, cit. P.294.

QUÍLEZ MORENO, J.M., "La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores". *Revista Española de Derecho del Trabajo*, núm.21, (2019), Estudios Editorial Aranzadi, S.A.U., Cizur Menor.

RODRÍGUEZ CARDO, I.A., "Política empresarial previa y supresión de la expectativa de privacidad: una reflexión crítica sobre las facultades de control del ordenador utilizado por el trabajador", Temas Laborales, núm. 126, (2014), pp.170 y 171; y FERNÁNDEZ VILLAZÓN, L.A., Las facultades empresariales de control de la actividad laboral. Pamplona, Aranzadi, 2003, p.184 y ss.

RODRIGUEZ ESCANCIANO, S., "Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de protección de datos", *en Revista Vasca de Gestión de Personas y Organizaciones Públicas*, núm. 16, (2019), p. 114.

RODRÍGUEZ-PIÑERO ROYO, M., "Las facultades de control de datos biométricos del trabajador", *Temas Laborales*, núm.150, (2019),p.91-109.

SELMA PENALVA, A., "El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores'' *Revista doctrinal Aranzadi Social*, núm.9, (2010), Presentación Editorial Aranzadi, pp. 27-36.

VALDÉS DAL-RÉ,F., "Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa". *Revista de Derecho Social*, Nº.79, (2017), p.15-35.

VERDÚ MACIA, V., "Espionaje sobre el empleado", El País, Edición Andalucía, 7 de abril, núm. 11, (2002). Disponible on line: https://elpais.com/diario/2002/04/07/domingo/1018151560_850215.html

"Vicios del consentimiento", Disponible on line: https://www.conceptosjuridicos.com/vicios-delconsentimiento/#:~:text=Los%20agentes%20que%20protagonizan%20los,en%20los%20dos%20%C3%BAltimos%20casos