Confidencialidad y Protección de datos personales en Derecho Laboral

Marina Paula Martin Agostinho Simões Fernández

Palmito Books

Título: Confidencialidad y Protección de datos personales en Derecho Laboral

© Marina Paula Martins Agostinho Simões Fernández, 2025

Reservados todos los derechos

De acuerdo con lo dispuesto en el art. 270 del Código Penal, podrán ser castigados con penas de multa y privación de libertad quienes reproduzcan o plagien, en todo o en parte, una obra literaria, artística o científica, fijada en cualquier tipo de soporte sin la preceptiva autorización.

Palmito Books®

Publicado en formato digital

1ª edición: febrero 2025

ISBN: 979-13-87676-19-3

DOI: 10.56533/XQGZ3536

URL: https://doi.org/10.56533/XQGZ3536

ÍNDICE

I. Resumen....7
II. Metodología....9
III. Evolución de la protección de los datos personales de los trabajadores....10
IV. Las fuentes jurídicas en materia de protección de datos personales....12
4.1 La Constitución Española de 1978....12
4.2 Leyes Orgánicas de Protección de los Datos....13
4.3 Reglamento Europeo de Protección de Datos (RGPD)....15
4.4 Novedades del RGPD....16
4.5 El Análisis de Riesgo....17
4.6 Viejos y Nuevos Derechos de los ciudadanos: la responsabilidad pro activa....18
4.7 El consentimiento del Reglamento General de Protección de Datos....20
V. Protección de datos biométricos....23
VI. Excepciones al tratamiento de datos personales....24
6.1 Interés publico....24
6.2 Intereses legítimos....25
6.3 Cumplimiento de una obligación legal....26
6.4 La protección de las víctimas de acoso laboral....27
6.5 Protección de datos de Salud....28
VII. Obligación del empresario de información de las medidas de vigilancia y control....29
VIII. Uso de grabaciones de cámaras de seguridad por las Administraciones Públicas....34
IX. Uso de grabaciones de voz....36
X. La privacidad y el acceso al Correo Electrónico....38
XII. Conclusiones....39
XIII. Bibliografía....40

Abreviaturas

AEPD- Asociación Española de Protección de Datos

CE- Constitución Española

CEPD- Comisión Europea de Protección de Datos

EM- Estado Miembro

ET- Estatuto de los Trabajadores

HIV- Human Imunodeficiency Virus

LO- Ley Orgánica

LOPD- Ley Orgánica de Protección de Datos

LOPDGDD- Ley Orgánica de Protección de Datos y de Garantías y Derechos Digitales

LORTAD- Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal

OCDE- Organización para la Cooperación y Desarrollo Económicos

OIT- Organización Internacional del Trabajo

R- Resolución

RD- Real Decreto

RGPD- Reglamento General de Protección de Datos

RTC- Resolución del Tribunal Constitucional

RTS- Resolución del Tribunal Supremo

SIDA- Síndrome de Imunodeficiencia Humana Adquirida

STC- Sentencia del Tribunal Constitucional

STS- Sentencia del Tribunal Supremo

TIC- Tecnologías de Información y Comunicación

UE- Unión Europea

I. Resumen

Los derechos de los trabajadores han experimentado grandes modificaciones y han contribuido a asegurar en la actualidad, la protección de datos confidenciales legalmente protegidos en numerosos textos legales. La Organización Internacional del Trabajo creada en 1919, a través de su original estructura tripartita se han logrado acuerdos entre empleadores, trabajadores y Sindicatos, de forma a asegurar los derechos y garantías de los trabajadores y la mejoría de las condiciones laborales.

Aunque el tratamiento de los datos personales y su confidencialidad estén previstos en la Constitución Española y en Leyes Orgánicas, Directivas Comunitarias y por aplicación directa del Reglamento Europeo de Protección de Datos, la posición de subordinación y dependencia de los trabajadores en relación al empleador público o privado y la variabilidad de situaciones socio laborales y jurisprudenciales revisten de inseguridad jurídica este tema tan sensible y actual.

Palabras Llave: confidencialidad, protección, datos personales, derechos laborales

Confidentiality and Protection of Personal Data in Labor Law

II. Summary

The rights of workers have undergone major changes and have contributed to ensure today, the protection of confidential data legally protected in numerous legal texts. The International Labor Organization created in 1919, through its original tripartite structure, agreements have been reached between employers, workers and unions, in order to ensure the rights and guarantees of workers and the improvement of working conditions.

Although the treatment of personal data and its confidentiality are provided for in the Spanish Constitution and in Organic Laws, Community Directives and by direct application of the European Data Protection Regulation, the position of subordination and dependence of workers in relation to the public or private employer and the variability of socio-labor and jurisprudential situations make this sensitive and current issue legally insecure.

Key words: confidentiality, protection, personal data, labor rights.

III. Metodología

De acuerdo con el plan y la propuesta de la investigación nos proponemos la pregunta de investigación " *Existe de forma efectiva Confidencialidad y Protección de datos personales en Derecho Laboral?"* con el objetivo primordial de evaluar el estado del arte en la actualidad, su evolución y adaptaciones legales y jurisprudenciales relacionadas con el desarrollo social y progresivo de las Tecnologías de Comunicación y Información: el diseño de este trabajo es retrospectivo, de pesquisa bibliográfica y de fuentes Jurisprudenciales, haciendo referencias a la evolución de derechos laborales de los trabajadores, a casos relevantes de la Jurisprudencia y a la evolución normativa Nacional, Europea y Mundial .

La garantías legales y sociales de los trabajadores deben permanecer aseguradas y previstas en el texto constitucional español: los trabajadores de todas las empresas publicas y privadas constituyen nuestra muestra y el momento del trabajo de investigación se reporta a la actualidad, con referencias a toda la evolución pasada y a la implementación progresiva en los medios laborales de la informática: la potestad de control y la situación de dependencia de los trabajadores ante el empleador aportan extrema sensibilidad y actualidad a esta cuestión.

IV. Evolución de la protección de los datos personales de los trabajadores

La OIT fue creada en 1919 como parte del Tratado de Versalles al final de la Primera Guerra Mundial[1] y reflejó la importancia de la adquisición de Derechos laborales, de encarar los trabajadores como personas, con trabajos dignos, en paz universal y con justicia social.

Una reunión de 24 expertos de la OIT en Ginebra[2] en 1996, representantes de una veintena de países, aprueba un proyecto de repertorio de recomendaciones prácticas, ante la creciente preocupación mundial de la protección de la vida privada y de datos personales de los trabajadores, en el ámbito laboral, agravada por el desarrollo meteórico de la Plataformas de Tecnologías de Información y Comunicación (TIC), trazando las líneas directrices de la Confidencialidad de los datos personales de los trabajadores y de su uso empresarial publico y privado.

Motivada fundamentalmente por hechos relacionados con la discriminación negativa al acceso al trabajo de pacientes con HIV/Sida, a finales de los años 80, esta reunión de expertos adoptó a 7 de octubre e 1996 este proyecto aún sin carácter obligatorio, es decir, que sus líneas directrices eran en ese momento voluntarias; constituyeron un primer esfuerzo de ámbito internacional en el sentido de trazar las orientaciones para la protección de datos personales. Este importante proyecto fue usado para elaborar leyes, reglamentos, convenios colectivos, directivas y políticas laborales en diferentes países que rigen el tratamiento de los datos personales de los trabajadores: la premisa fundamental es que los datos personales solo deberían utilizarse de modo "*ecuánime y lícito*" directamente relacionados con el empleo y "*con el fin para el cual hayan sido acopiados"*.

Los principios generales del Proyecto invitan a los trabajadores, empleadores y representantes de los dos grupos a participar activamente en la protección de los datos individuales sometiendo los mismos a una "*obligación de reserva*" y jamás deberían de servir para "*controlar la actuación de los trabajadores*" ya que estos no deberían poder renunciar a ejercer su derecho de protección de su vida privada.

La naturaleza de la información protegida abordaría temas de naturaleza sexual, convicciones político religiosas, que por texto, imágenes o audio permitan la identificación de una persona. Existen dos tipos de datos: datos de poco riesgo, como es el nombre o el correo electrónico y

2 Organización Internacional del Trabajo https://www.ilo.org/global/about-the-ilo/lang--es/index.htm

[2] (Trabajo O. I., 1996), op. cite

datos más sensibles, como aquellos relacionados con la salud personal, la religión, las orientaciones de género o políticas; los antecedentes penales de los trabajadores son igualmente de riesgo mayor, siempre que estos no guarden relación directa con el empleo, de conformidad con las leyes nacionales.

Los datos personales no deberían comunicarse a terceros sin el "consentimiento explícito" de los trabajadores exceptuando los casos en que exista riesgo para la salud o la vida de las personas o que sea obligatorio por ley, en cumplimiento de disposiciones penales.

Por ultimo, los trabajadores tendrían el derecho a ser informados con regularidad sobre los datos personales usados y su tratamiento electivo y deberían poder consultar, modificar o borrar sus datos.

V. Las fuentes jurídicas en materia de protección de datos personales

4.1 La Constitución Española de 1978

La protección de datos personales en la Constitución Española de 1978, en el artículo 18.4 establece que "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. Este es el "punto fulcro"[3] para averiguar si la protección efectivamente se cumple o no, en relación a la automatización de los datos personales y familiares y sobre el uso de los datos informatizados por los Poderes Públicos. Según algunos autores, la Constitución establece un derecho de protección frente al uso de la informática y, por su propia ubicación en el texto constitucional, constituye un derecho fundamental específicamente protegido (Aguilar del Castillo, M C. Universidad de Sevilla, 2016). El contenido de este derecho o libertad es concretado particularmente referido al derecho al honor y a la intimidad personal y familiar de los ciudadanos (no de las personas jurídicas), respecto al tratamiento informático de datos personales. Supone una garantía específica de tales derechos, que son reconocidos como tales en el mismo art. 18.4 de la CE, punto 1.

La insistencia constitucional para la protección de este derecho está igualmente presente en el enunciado del art. 20.3 de la CE, que pone límites a la libertad de expresión y de información, también derechos fundamentales, al establecer que *«estas libertades tienen su límite en el respeto a los derechos reconocidos en este título (Título 1 «De los derechos y deberes fundamentales», arts. 10 a 55 de la CE).* Es, pues, un derecho fundamental de libertad, para ejercer cualquier derecho, frente a los obstáculos o intrusiones que puedan producirse con la utilización de la información privada y confidencial (Sentencia del Tribunal Constitucional 254/1993 de 20 de julio)[4].

La integración de la tecnología en la organización de la empresa influencia directamente la relación laboral (contenido ex lege del derecho a la protección de datos del articulo 18. 4 de la

[3] Constitución Española de 1978, artículo 18, punto 1

[4] STC 254/1993 de 20 de julio

CE, STC 110/1984 (RTC 1984/110)[5] y STC 292/2000 (RTC 1000/292)[6]): la subordinación del trabajador al poder de la organización y dirección del empresario y sus facultades de vigilancia y control (Tascón López, 2016). Sobre libertad informática, Antonio -Henrique Pérez Luño (Luño, 2000) afirmó que "*se trata de uno de los principales sectores que integran el Derecho Informático. La libertad informática aparece como un nuevo derecho de auto tutela de la propia identidad informática: o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un programa electrónico".* Sin embargo este nuevo derecho no debe imponerse al derecho a la protección efectiva de los datos personales y a la confidencialidad de os mismos.

4.2 Leyes Orgánicas de Protección de los Datos

Este suporte constitucional de la protección y alcance de la misma, pasa a un segundo escalón, la Protección mediante Ley Orgánica[7]. En cumplimiento de lo que dispone el art. 18.1 de la CE se promulga la LO 5/1992, " Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos personales (LORTAD)[8]"; En 1994 se promulga el RD 1332/1994 de 20 de junio[9], normativa sobre protección de datos personales. La LO 5/1992 fue sustituida por la LO 15/1999 (LOPD)[10], de Protección de Datos de Carácter Personal, tanto en lo que se refiere a las Administraciones Publicas pero también a la protección de los derechos personales frente a los ficheros de titularidad titularidad privada, artículos 6, 7 y 11.

[5] STC 110/1984 de 21 de diciembre

[6] STC 292/2000 de 30 de noviembre

[7] Ley Orgánica: Norma emanada de las Cortes Generales, para cuya aprobación, modificación o derogación la Constitución Española (art. 81) exige mayoría absoluta del Congreso de los Diputados, en una votación final sobre el conjunto del proyecto. Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y otras previstas expresamente en la Constitución.

[8] Ley Orgánica 5/1992, " Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos personales"

[9] Real Decreto 1332/1994 de 20 de junio

[10] Ley Orgánica 15/1999 de 13 de diciembre (Ley Orgánica de Protección de Datos de Carácter Personal)[10],

Tanto en la LORTAD como en la LOPD se ve la aplicabilidad de este principio constitucional tal como en el Articulo 20.4 de la CE: "*en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección* (Trabajadores, 1996) *de la juventud y de la infancia"* (LO 1/1982, de 5 de mayo, de protección civil del honor, la intimidad la propia imagen, y su corrección por la LO 3/1985).

De hecho, el Estado, a través de las administraciones Públicas, necesita informaciones referentes a los ciudadanos para el desempeño de sus objetivos: urge por eso la limitación del poder estatal sobre esos datos y la existencia de normas de protección de datos personales. Es al Derecho que le asiste la protección de los derechos de los ciudadanos permitiendo así el pleno ejercicio de su derecho a la intimidad: una breve referencia a la evolución histórica nos remonta a Suecia en el año de 1973 (Sánchez Pérez & Rojas González) y en 1974 a EUA, con el "*Privacy Act*"[11], ley con propósito de la privacidad ciudadana. Fue con el Parlamento Sueco que se legisla la primera ley en este sentido y que despierta el Consejo de Europa que en el mismo año, dicta la resolución número R 22 sobre la protección de la vida privada de personas físicas referida a bancos de datos electrónicos en el sector privado, y del publico, la resolución R 29 en el año siguiente[12] (Garriga Domínguez).

La reciente modificación de la LOPD 15/1999 para la LOPDGDD 3/2018 de 25 de mayo de 2018 (Ley Orgánica de Protección de los datos de Carácter Personal y Garantía de Derechos Digitales) va al encuentro de las garantías constitucionales apuntadas: modifica las exigencias en el tratamiento de información personal de usuarios y de empresas. Esta ley sustituye la antigua LOPD y entró en vigor en 6 de diciembre de 2018: es la actual referencia normativa de la protección de datos y tiene como objetivo principal adaptar la legislación española a la normativa europea, más precisamente, al Reglamento Europeo de Protección de Datos (Reglamento de la UE 2016/679) vigente desde 25 de mayo de 2018. Establece los requisitos y obligaciones en materia de protección de datos en empresas, de como proceder con la información de los trabajadores, usuarios y consumidores: todas las sociedades mercantiles, los Autónomos, los Organismos Públicos, las Administraciones Publicas, Asociaciones, Entidades sin animo de lucro y Comunidades de Propietarios están obligados a cumplir con esta ley,

[11] Privacy Act, The United States of America, Department of Justice. https://www.justice.gov/opcl/privacy-act-1974

[12] Domínguez, A G, Revista VLex, Información Jurídica Inteligente, Pág. 149-159: https://vlex.es/vid/proteccion-datos-caracter-personal-642494413

señalando que "*cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero"* a todas las personas jurídicas o físicas, empresas y entidades publicas o privadas que utilicen cualquier dato personal en el desarrollo de sus actividades profesionales, en España.

La finalidad de la LOPDGDD es proteger la intimidad, la privacidad e la integridad del individuo, de acuerdo con el artículo 18.4 de la CE, siempre que se traten de datos personales y incluso aportando garantías de seguridad cuando es necesario el intercambio o transferencia de esos datos entre empresas.

Las principales modificaciones de la LOPDGDD en relación a la anterior LOPD residen en los cambios de tratamiento de datos de usuarios en internet, novedades incluidas en el Reglamento Europeo de Protección de Datos (RGPD) y que encuentra la adaptación del ordenamiento español a este Reglamento Comunitario por remisión.

4.3 Reglamento Europeo de Protección de Datos (R UE 2016/679)

De entre las novedades que encontramos en la nueva ley de protección de datos, la LOPDGDD, hay que citar los siguientes contenidos derivados del RGPD. Este Reglamento establece en su artículo primero las normas relativas a la protección de las personas físicas en materia de tratamiento de datos personales y las normas relativas a la libre circulación de tales datos, protegiendo los derechos y libertades fundamentales de las mismas y su derecho a la protección de los datos personales: en la Unión Europea, "*la libre circulación de los datos personales no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".*

El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Los datos de los trabajadores están por analogía sometidos a la misma protección de datos conferida por el RGPD.

El Reglamento no se aplica al tratamiento de datos personales si ocurren los siguientes hechos: en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la

Unión; por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de la Unión Europea ("Disposiciones especificas sobre Política Exterior y de Seguridad Común" (PESC)); efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

El Reglamento número 45/2001del Parlamento Europeo y del Consejo[13] es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión[14], con sus valores y principios de Imparcialidad, Integridad, Transparencia y Pragmatismo en el "trabajo del día a día "y con su Estrategia EDPS 2020-2024 (edps.europe.eu op. cit).

4.4 Novedades del RGPD

De acuerdo con este Reglamento, y en el ámbito material de su artículo segundo, presenta algunas novedades que fueron incluidas en la nueva ley y que pasamos a citar:

La Rendición de cuentas o Accountability que amplia la información que se debe de facilitar a los trabajadores en relación al tratamiento de sus datos personales y a sus derechos en esta materia y incorpora la llamada "*privacidad desde el diseño":* el conjunto de los procedimientos de la empresa a realizar en este ámbito y desde el principio de la relación laboral afirma que nadie podía ser obligado a revelar datos de estas categorías sobre su persona y solo se podrán tratar bajo consentimiento expreso y por escrito del afectado.

14 Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos: https://www.boe.es/doue/2001/008/L00001-00022.pdf

[14] https://edps.europa.eu/sites/default/files/publication/21-01-20_edps_brochures_en.pdf

Los datos de ideología, afiliación sindical, religión y creencias pueden ser revelados sin este consentimiento si los ficheros están mantenidos por partidos políticos, sindicatos, iglesias y comunidades religiosas y por asociaciones, fundaciones y otras entidades sin animo de lucro siempre que su finalidad sea política, filosófica, religiosa o sindical.

Los datos de salud, origen racial y vida sexual pueden ser tratados por razones de interés general, como la Salud Publica (caso de enfermedades de transmisión sexual o de enfermedades con peligro de diseminación comunitaria), pero debe estar legalmente previsto y con el consentimiento expreso del afectado: existe un "*Decálogo de Protección de datos para el personal sanitario y administrativo"*[15] que todos los profesionales sanitarios y administrativos deberían de tener presente, evitando que se produzcan posibles ilícitos vinculados a la protección de datos personales. Incluso recientemente el Comité Europeo de Protección de Datos sugirió que la Comisión debería prohibir el uso de los datos biométricos de reconocimiento facial en los medios laborales y incluso en la vía publica[16] (Aguiar, 2021)

4.5 El Análisis de Riesgo

El análisis de riesgo o notificación de brechas de seguridad informática se basa en el peligro de que puedan afectar a los datos personales y por eso estas deben ser reportadas en un plazo máximo de 72 horas a la Agencia Española de Protección de Datos[17]. En el caso que se vean afectados datos sensibles o especialmente protegidos (pertenecientes a las categorías especiales de datos, como son los de ideología, religión, creencias, origen racial, salud, vida sexual o relativos a infracciones penales o administrativas), los afectados deben igualmente ser notificados: los artículos 33 y 34 del RGPD evidencian el deber de notificación de las brechas

[15] https://www.aepd.es/sites/default/files/2019-10/infografia-decalogo-personal-sanitario.pdf

[17] Aguiar, A R," El Comité Europeo de Protección de Datos insta a la UE a prohibir los sistemas de reconocimiento biométricos en el espacio publico", junio 21

[17] Asociación Española de Protección de Datos, https://www.aepd.es/es

de seguridad y establecen el mismo un plazo máximo para informar la Autoridad de Control que ocurrió efectivamente una brecha de seguridad.

La LOPDGDD no recoge explícitamente el deber de notificación pero la establece como infracción muy grave en su articulo 72[18].

La Ley General de Telecomunicaciones análogamente establece en su articulo 41 la obligación de informar sobre posibles brechas de seguridad que puedan comprometer datos personales disponibles al publico.

Existen distintos tipos de brechas de seguridad: en un intento de establecer una clasificación, podemos citar las brechas de *confidencialidad,* si se produce un acceso no autorizado y no legitimo a la plataforma de TIC, de *integridad,* si hay indicios de manipulaciones o alteraciones de la información original almacenada en la TIC y las brechas de *disponibilidad,* con la perdida y acceso a los datos originales, temporal o definitivamente.

En 2020, la AEPD publica un modelo de informe que ayuda a las empresas publicas y privadas a realizar evaluaciones de impacto en protección de datos[19].

4.6 Viejos y Nuevos Derechos de los ciudadanos: la responsabilidad pro activa

Información confidencial es toda aquella que no puede ser divulgada a terceros sin consentimiento del propietario de la misma y que se reviste de una serie de medidas que garantizan su seguridad, por ser personal, sensible o privada. La aplicación de esta información confidencial puede variar en distintos ámbitos: si se trata de relaciones laborales entre trabajadores y empresarios, entre clientes y empresas o si se tratan de datos de salud, informáticos, religiosos, políticos o otros.

En el RGPD, articulo 5.f, apunta para la importancia del tratamiento seguro de los datos mediante la adopción de medidas técnicas y organizacionales que garanticen la integridad y confidencialidad de esos datos. Ya en el articulo 5 de la LOPDGDD tanto los encargados del tratamiento de toda la persona que intervenga en el intercambio de información protegida, y también al deber de secreto profesional que la complemente.

[18] https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[19] https://www.aepd.es/sites/default/files/2020-03/modelo-informe-EIPD-AAPP.rtf, versión marzo 2020.

El Registro de actividades de tratamiento de datos personales en una empresa con menos de 250 trabajadores no es obligatorio excepto si los datos tratados sean de naturaleza especial, como los de salud, étnicos, religiosos, o sean datos referentes a condenas o infracciones penales o otros que comporten riesgos para derechos y libertades de los trabajadores.

La responsabilidad pro activa o accountability en el RGPD[20] es un principio introducido en este Reglamento que simboliza la llamada Cultura Organizacional, la Gobernanza Institucional: garantiza y protege las Libertades Publicas y los Derechos Fundamentales de loa trabajadores, por la aplicación en la Organización de la normativa vigente, con el cumplimiento y demonstración de dicho cumplimiento *("la compliance* es *no solo lo que hay que cumplir, sino demonstrar que se cumple")* como sistema de prevención del delito y cumplimiento de la norma, otra forma de análisis de riesgo.

Este sistema de prevención del delito incluyó las personas jurídicas como sujetos responsables penalmente por actos delictivos cometidos por sus trabajadores, patente en la reforma del Código Penal de 2015: el termino *compliance* viene de os años de 1970 cuando los casos de corrupción del sistema financiero de EUA y en la cultura jurídica anglosajona (Redaccion, 2014,15 de ocubre): los casos de monopolio empresarial financiero, de soborno a funcionarios y de tráfico de influencias llevó a la actividad legislativa en diferentes países para condenar por corrupción a empresas. El principio de accountability en la protección de datos puede ser sintetizado en la llamada "*due diligence*"[21]: la aplicación de un código ético y organizacional con la aceptación de las responsabilidades sin excusas, la motivación de los equipos de trabajo, la transparencia en todas las actividades, el liderazgo, la creatividad y el sentimiento de pertenencia a la Institución (Tablado, 2020, 17 de marzo). Las obligaciones inherentes al responsable del tratamiento de datos, elemento indispensable previsto legalmente, debe demonstrar y garantizar que la normativa se cumple, está patente en la LOPDGDD en su articulo 28.

[20] https://www.dpoitlaw.com/el-principio-de-accountability-o-de-responsabilidad-proactiva/

[21] https://protecciondatos-lopd.com/empresas/due-diligence/

4.7 El consentimiento del Reglamento General de Protección de Datos

Las directrices de la UE 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679[22], adoptadas el 4 de mayo de 2020 versión 1.1[23] deroga la Directiva 95/46/CE relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos.

El articulo 4.11 del RGPD define el consentimiento como "*toda manifestación de voluntad libre, específica, informada y inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que conciernen"* no es más que una comunicación del interesado por la cual este acepta que se traten sus datos personales, para una finalidad concreta, bajo unas determinadas condiciones, de las cuales tiene de estar previamente informado; la única forma de consentimiento admitida en el RGPD es el consentimiento expreso: para el RGPD el consentimiento tácito ya no es válido. Este articulo del RGPD especifica que el consentimiento:

a) es una manifestación de *voluntad libre* , que implica elección y control reales por parte de las personas físicas: elección y control por parte de los interesados. El RGPD si el interesado no es realmente libre para elegir o se siente obligado a dar su consentimiento, este no es considerado valido. De igual forma, la información personal que pueda publicarse en el tablón de anuncios de la empresa debe contar con el consentimiento expreso de los trabajadores, mediante una clausula de información y de consentimiento en el contrato laboral que debe ser firmada por el trabajador.

   El desequilibrio de poder que se manifiesta en relación con Autoridades Públicas, cuando el trabajador no tiene alternativas realistas para aceptar o no el tratamiento de sus datos, por temor a alterar las perspectivas personales en términos laborales: el

[22] Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

[23] European Data Protection Board es un cuerpo independiente que contribuye a la aplicación consistente de la protección de datos promoviendo la cooperación de las Autoridades de los Estados Miembros. Se encuentra en el RGPD y esta situada en Bruselas, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are

CEPD[24] considera que hay otras bases jurídicas para aceptar el tratamiento de datos por Autoridades Públicas, previstas en el RGPD.

También la condicionalidad presente en el artículo 7, apartado 4, del RGPD, evidencia que vincular o supeditar el consentimiento al cumplimiento de un contrato a la prestación de un servicio, resulta bastante inapropiado: debe por eso disociarse el consentimiento de los fines del tratamiento de datos personales y los interesados tener la libertad para elegir que fines aceptan separadamente en vez de dar su consentimiento para todos ellos a la vez.

Por fin, como manifestación de consentimiento libre, el trabajador debe poder negar o retirar el mismo sin perjuicio o desventaja alguna.

b) es manifestación de *voluntad específica*: el consentimiento expreso del trabajador debe de ser obtenido siempre que esos datos personales no tengan ninguna finalidad dentro de la relación contractual y informarlo de cómo y cuando puede ejercer sus derechos. Los desequilibrios de poder no ocurren solo con Administraciones Públicas y los trabajadores: el consentimiento solo puede ser considerado válido si se puede elegir sin riesgo de perjuicio ni de engaño, intimidación o coerción o de cualquier consecuencia negativa, caso contrario no será libre. Este requisito refuerza la transparencia y control para el interesado: garante contra la desviación del uso, contra la disociación de las solicitudes de consentimiento y estableciendo una clara separación entre el consentimiento para los tratamientos de datos personales y aquel dado para otras cuestiones -"*limitación de la finalidad*" (articulo 5, apartado 1, letra a) del RGPD).

c) es una manifestación de *voluntad informada*: el consentimiento debe de ser informado (articulo 5 del RGPD), de acuerdo con el principio de transparencia, para asegurar la toma de decisiones informadas, comprendiendo el interesado lo que está autorizando y tener seguridad de poder retirarlo en un determinado momento. Para tal existen algunos requisitos que de forma abreviada se pueden sintetizar: saber la identidad del responsable del tratamiento de los datos, su finalidad, que datos se recogen y tratan, el derecho a poder retirar el consentimiento en un momento posterior, los riesgos de una posible transferencia de datos y si habrá decisiones

[24] Comité Europeo de Protección de Datos es el organismo responsable de la aplicación del RGPD, de forma coherente en toda la UE https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_pt

automatizadas (articulo 22, apartado 2, letra c) del RGPD). Para facilitar la información se pueden usar medios verbales, mensajes de audio, escritas o de video (artículo 7, apartado 2).

d) y una manifestación de *voluntad inequívoca*: el interesado acepta el tratamiento de sus datos personales, por una declaración o por una clara acción afirmativa, a una operación concreta de tratamiento de datos, bien identificada.

La obtención de un consentimiento explícito, en el articulo 9 el RGPD, enumera el tratamiento de categorías especiales de datos personales y en la transferencia automatizada de estos datos a terceros países o Organizaciones Internacionales: el consentimiento *normal* es expreso, escrito o no (caso de consentimientos emitidos en línea, en impresos electrónicos o vía telefónica) claro y afirmativo, que elimina cualquier *duda o falta de prueba en un futuro*.

La retirada del consentimiento del artículo 7, apartado 3 del RGPD, establece que el responsable del tratamiento debe garantizar que el interesado pueda retirar su consentimiento al tratamiento de sus datos personales a cualquier momento, y deberá ser tan fácil retirarlo como lo fue darlo al inicio de los tramites.

Toda esta información referente a datos personales y el consentimiento expreso del trabajador o interesado, debe quedar almacenado por el responsable de la gestión de los datos debe igualmente demonstrar que dicho consentimiento se ha obtenido de forma adecuada y de acorde con la ley, generando un justificante conservado por medios electrónicos o físicamente en ficheros.

El uso de datos personales sin consentimiento o solicitados de forma incorrecta puede conllevar a una serie de sanciones: de acorde con el RGPD, en su artículo 7, y paralelamente en la LOPDGDD 3/2018 en varios de sus artículos, prevén que la vulneración de todo lo relacionado con el recabo del consentimiento de datos personales sin el consentimiento expreso del interesado puede conllevar a multas administrativas de 20 millones de euros como máximo o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, en los casos de infracciones muy graves, y se optará siempre por la multa de mayor cuantía.

V. Protección de datos biométricos

Fue con la Declaración Universal de Derechos Humanos que se expresaron los derechos humanos básicos como se expresa en su articulo 12: *" Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias o ataques"*. Entre estos datos se cuentan los llamados biométricos que almacenados en sistemas digitales y en bases de datos son susceptibles de posibles de ataques cibernéticos: desde huellas dactilares, a análisis del iris o de la retina, rasgos faciales, timbre vocal, cadencia del paso, firma manuscrita entre otros, son apenas algunos datos biométricos usados para permitir la identificación y/o autentificación individual[25].

Estos datos legalmente previstos con la finalidad de proteger la honorabilidad del individuo aún cuando hubiera este fallecido: En Alemania, en 1970,con la *Datenschutz* que prohíbe expresamente la transmisión de cualquier dato personal sin el consentimiento del titular; el *Privacy Act* Estado Unidense de 1974; el primer Convenio de la UE o *Convenio 108* de Estrasburgo y la *Directiva 95/46/CE*, son algunos de los textos legales que evidencian la importancia del tratamiento de este tipo de datos en contexto laboral.

En España con la *Ley Orgánica 15/1999* y en diferentes países de América Latina a finales del siglo XX principio del XXI (Sánchez Pérez g, Rojas González Isai. Universidad Nacional Autónoma de México) se han promulgado textos legales equivalentes.

[25] https://revista.seguridad.unam.mx/numero-13/leyes-de-protección-de-datos-personales-en-el-mundo-y-la-protección-de-datos-biométricos-–

VI. Excepciones al tratamiento de datos personales

Las situaciones de desequilibrio de poder entre las partes implicadas derivadas de la situación de dependencia entre empleado y empleador (Paniagua Alario, 2021)-recuérdese las cuatro características del trabajo: voluntariedad, dependencia, ajenidad y retribución- plasmadas en las Directrices 5/2020 sobre el consentimiento en el sentido del reglamento UE 2016/679, constituye la base de legitimación que de forma excepcional se considera para acreditar que los mismos se han otorgado de forma libre, inequívoca e informada. Los datos aportados han de ser adecuados, pertinentes y limitados a los fines para los que son tratados: los que son derivados de las nominas, de identificación a través de tarjetas identificativas o el aporte de datos cuyo tratamiento revista un interés publico, sean en cumplimiento de una obligación legal o basados en intereses legítimos. Así analizaremos cada uno de estas variantes al tratamiento de datos personales:

6.1 Interés publico

El muy difundido "caso del canal de denuncias internas" en la actividad empresarial como instrumento de compliance, dio origen a 16 de abril de 2019 a la aprobación de una propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección frente a represalias de las personas que informen sobre infracciones del Derecho de la Unión, conocida como *Directiva Whistleblowing (el "denunciante o el que sopla, el silbato"),* elemento esencial en la protección del denunciante contra la corrupción y la investigación de irregularidades empresariales, incluso premiando económicamente a quien revela esa información que difícilmente se podría describir sin ese aporte interno (Rosa, Espín: Universitat Autònoma de Barcelona, 14/09/2017).

La Directiva Europea[26] prevé este tipo de cauces y procedimientos internos de tramitación de denuncias y la efectiva implementación de canales de denuncias internas, para la detección de irregularidades y infracciones legales en la empresa que afecten de forma significativa el funcionamiento de la misma, la seguridad alimentaria, la salud publica o la protección de consumidores: están obligados no solo Entidades Publicas pero también para empresas de más

[26] Directiva de la UE 2019/1937 do Parlamento Europeo y del Consejo de 23 de octubre de 2019: Protección de Whistleblower publicado en Jornal Oficial de la UE de 26/11/2019 https://www.boe.es/doue/2019/305/L00017-00056.pdf

de 50 trabajadores; se establece en esta Directiva la negociación con la representación de los trabajadores y de sus representantes si así lo establece la Normativa de cada Estado Miembro.

Este deber de información, se puede proporcionar por diferentes cauces: directamente en el contrato de trabajo y al alcance del denunciante y del denunciado, individual o colectivamente al modificar el sistema o mediante circulares informativas.

Los procedimientos de tramitación de denuncias permiten que de forma material y a través de los canales de *Whistleblowing* se formulen denuncias por escrito o de forma verbal, vía telefónica o por otras formas de mensajería de voz o incluso de forma presencial si así lo solicita el denunciante; existe una obligación de acuse de recibo de la denuncia en un plazo máximo de 7 días; la designación de una persona o servicio imparcial que tramite esas denuncias de forma efectiva y que lo haga de todas ellas, incluyendo las anónimas, y que la respuesta al denunciante se haga en un plazo máximo de 3 meses.

En España, ya se empezó a regular estos canales por la ley Orgánica 3/2018 (LPDPGDD) y la Directiva que con un plazo de transposición de 2 años desde su publicación en el DOUE, es directamente aplicable. Los planes de *compliance* ya recomiendan contar con estos canales. Entre los derechos del denunciado, están los de acceso, rectificación, supresión o oposición al denunciante sin que se revele su identidad y posibilitando que el denunciado pueda defender debidamente sus intereses.

6.2 Intereses legítimos

Con la publicación de datos de productividad, debe de ponderarse el interés legitimo y la posible lesión de derechos de los afectados: el abono de un complemento de productividad o la publicación de los datos de *performance* individual de forma transparente e imparcial y mediante códigos específicos conocidos por los interesados. Su finalidad primordial debe ser la motivación laboral de los trabajadores y su publicidad se debe de ajustar a la finalidad prevista, evitando así su difusión generalizada.

De igual modo, la cesión de datos a otras empresas del mismo grupo debe consistir en la centralización de carácter administrativo como procedimientos internos de cada entidad empresarial.

El acceso de datos y la información facultada de los candidatos que han obtenido mejor cualificación profesional, por otras personas candidatas a un puesto de trabajo en procesos de concurrencia competitiva, sólo debe permitirse en relación a datos relevantes para la tutela de derechos y intereses eventualmente vulnerados (*principio de minimización de datos)* y de forma disociada (no se podrá facultar currículum completos y nada más que la información relativa a la formación, experiencia profesional y datos estrictamente relevantes para formalizar la reclamación). No se permitirá el acceso como regla general al nombre, fotografía, dirección postal o de correo electrónico.

Como excepción en los casos de reclamaciones por vulneración de derechos fundamentales (discriminación por raza, genero, edad, etc.) la persona trabajadora podrá acceder a datos personales verdaderamente relevantes del candidato elegido para fundamentar su reclamación.

6.3 Cumplimiento de una obligación legal

Existen tres situaciones relevantes: el registro de jornada, el registro de salarios y la protección de la privacidad de las victimas de acoso en el trabajo y de las mujeres supervivientes a la violencia de género. El registro de jornada de conformidad legal en el articulo 34.9 del Estatuto de los Trabajadores tiene su base jurídica en la obligación de incluir en la jornada de trabajo el horario concreto, su inicio y final, de cada trabajador; estos trabajadores tienen derecho a ejercitar sus derechos de rectificación, supresión y oposición con independencia del tipo de registro: la Agencia Española de Protección de Datos (AEPD) ha reiterado que los sistemas de datos biométricos sean lo menos invasivos posibles, como por ejemplo por el uso de tarjetas personales y/ o códigos personales igualmente eficaces, en vez de impresiones digitales o por la iris del trabajador (ver apartado V de este documento) . Este registro de jornada no puede ser de acceso publico ni estar en un lugar visible, no se pueden usar para finalidades distintas al control de la jornada de trabajo, como por ejemplo, para comprobar la ubicación del trabajador y deben de estar incluidos en el registro de Actividades del Tratamiento del articulo 30 del RGPD.

Cuánto al registro de salarios, y teniendo en cuenta la igualdad retributiva entre mujeres y hombres (art. 28.2 del E.T y Real Decreto 902/2020 de 13 de octubre), el empleador está obligado a tener un registro de salarios de sus trabajadores lo que implica un tratamiento de datos personales: sin embargo, en ese registro no ha de constar el salario de cada trabajador sino "valores medios", complementos y percepciones extra salariales "*desagregados por sexo y*

distribuidos por grupos profesionales o puestos de trabajo iguales o de igual valor" o sea, no se contempla un derecho a la información derechos de acceso, supresión o modificación, rectificación o oposición, pues no existe un verdadero tratamiento de datos personales; el registro deberá contar con las medidas de seguridad y análisis de riesgo adecuadas previstas en el RGPD.

6.4 La protección de las víctimas de acoso laboral

Asienta también en una obligación legal prevista en el articulo 6.1 c) del RGPD; la puesta en marcha de los procedimientos sancionadores en la empresa frente al acosador no requiere el consentimiento del acosado y está ligada a la obligación de la empresa como garante de la salud, seguridad en el trabajo y procedimientos en equidad (artículos 4.2 d) del Estatuto de los Trabajadores y 14 de la Ley 31/1995 de 8 de noviembre de Prevención de Riesgos Laborales. Sin embargo, la empresa debe garantizar la confidencialidad relativa a la identidad de la víctima, que sólo será revelada a las personas con interés en el procedimiento, "*no siendo admisible una publicidad masiva y indiscriminada sin consentimiento de la victima".* Deberá atribuirse un código identificativo a la persona supuestamente acosada y al supuesto acosador, preservando sus identidades; la víctima deberá prestar su consentimiento para declarar o testificar en los procedimientos sancionadores frente al acosador, y la cesión o comunicación de los datos de la víctima requiere su consentimiento, salvo previsión legal en contra. Si la empresa decide sancionar al acosador en el cumplimiento de una obligación legal y denunciar el contrato de trabajo, la potestad sancionadora es la base jurídica del tratamiento y no propiamente el consentimiento.

Novedad relevante en el marco de las relaciones laborales son las "decisiones automatizadas" de carácter excepcional, aprobadas en el RD 9/2021 de 11 de mayo[27] que modifica el ET, refuerza la transparencia y la *compliance* como garantías adicionales a la normativa de protección de datos: estas decisiones automatizadas son admitidas cuando de la celebración o ejecución de un contrato de trabajo y pueden ser determinantes en el ascenso/extinción/ renovación de un contrato, siendo sin embargo inadmisible que estos datos puedan generar

[27] Real Decreto-ley 9/2021, de 11 de mayo, por el que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales.

alguna forma de discriminación: si se genera lesión de derechos fundamentales, el algoritmo deberá ser modificado.

6.5 Protección de datos de Salud

Los datos de salud son una categoría de datos especialmente sensibles recogidos en el Reglamento 679/2016 de 27 de abril, relativo a protección de datos personales de personas físicas, también presentes en el RGPD, en sus artículos 9 y 35: *"el estado de salud física o mental pasado, presente o futuro del trabajador o de cualquier paciente, la información de cualquier persona contenida en bases de datos de la asistencia sanitaria, todo el numero que posibilite su identificación, los resultados de pruebas genéticas o de muestras biológicas, una discapacidad, los datos de tratamientos o el estado fisiopatológico de cualquier persona son datos relativos a salud y por tanto, confidenciales y propiedad del interesado de los mismos"*.

Cuando un profesional sanitario acede a datos de una historia clínica debe de tener una justificación motivada y bien identificados los motivos por los cuales se torna indispensable hacerlo: el paciente tiene derecho de acceso, rectificación, supresión, y limitación de su tratamiento y debe ser informado si sus datos de salud van a ser objeto de tratamiento, automatizado o no, y de la lógica aplicada para que se le de la oportunidad de expresar su opinión y de poder impugnar ese tratamiento. Caso contrario, el acceso ilícito a datos de salud de una persona física o de un trabajador, puede conllevar a la imputación de un delito de descubrimiento y revelación de secretos previsto en el Código Penal.

El Decálogo de Protección de Datos para el Personal Sanitario y Administrativo (Administrativo, 2021) debe estar siempre presente durante las labores sanitarias y administrativas diarias, evitando posibles infracciones.

Como última cuestión relevante y sensible actual está la revelación de datos personales de salud para la emisión de los recientes certificados de vacunación: los derechos individuales relacionados con la comunicación de datos personales confidenciales están actualmente a ser manipulados por un número elevado de personas sin la formación sanitaria adecuada y sin que exista un delegado para el tratamiento de esos datos.

VII. Obligación del empresario de información de las medidas de vigilancia y control

Este tema ha sido debatido de forma exhaustiva por distintos Tribunales Nacionales y Europeos en relación a la instalación de cámaras de video vigilancia en lugares de trabajo y el control y monitorización del trabajo a través de nuevas tecnologías como son los correos electrónicos, la navegación por internet o los dispositivos de geolocalización de los trabajadores durante la jornada laboral.

La obligación del empresario al deber de información se contrapone al derecho a la intimidad del trabajador y a la protección de datos personales del mismo; sin embargo son varias las sentencias que declaran la licitud de las medidas de vigilancia y control: todos conocemos el carácter mutable del Derecho y en los últimos años constatamos que la influencia de contexto socio cultural cada vez mas se ve menos influenciada por los distintos ordenamientos jurídicos de los Estados Miembros y más adaptada a la jurisprudencia comunitaria: ejemplo es la sentencia del Tribunal Supremo numero 766/2020 de 15 de septiembre (Rec 528/2020, página 6)[28] que ha declarado procedente el despido disciplinario de una trabajadora, justificando "*esta decisión empresarial por la constatación de las señales de movimiento en tiempos no justificados"* por el uso del coche de la empresa fuera de la jornada laboral (lo tenía prohibido),basado en los datos del GPS, que no sólo implica problemas asociados a la seguridad del vehículo de la empresa como también el Tribunal no consideró que hubiese cualquier vulneración a la intimidad o a la protección de los datos personales de la trabajadora pues la empresa ha podido comprobar que esta había sido expresamente informada previamente cuanto a la instalación del dispositivo de geo localización (según el artículo 90 de la LOPDGDD). Los datos del GPS se referían únicamente al vehículo, al uso seguro del mismo, y no a la circunstancia personal de la trabajadora que tenia constancia que el uso del vehículo de haría

[28] STS 766/2020, Sala de lo Social de 25 de septiembre, Unificación Doctrina.

Número del procedimiento: 528/2018

Fecha de Votación y Fallo: 15/09/2020

Ponente: Excma. Sra. D.ª María Lourdes Arastey Sahún

Procedencia: Tribunal Superior de Justicia de Andalucía/Granada

Letrada de la Administración de Justicia: Ilma. Sra. Dña. María Jesús Escudero Cinca

exclusivamente durante la jornada laboral y uso profesional (VLex: Información Jurídica Inteligente, 30/11/2016).

Otra sentencia importante dentro del tema de la instalación de cámaras en los centros de trabajo y en sentido opuesto a la anterior, fue la del TSJ de Andalucía número 1146/2020 de 1 de junio y Recurso 3926/2019 de 28 de mayo de 2020 [29] : como las cámaras en los centros de trabajo no pueden ser ocultas conllevó a la nulidad del despido de un vigilante de seguridad que fue gravado dormido, descalzo y viendo películas en su centro de trabajo durante su jornada laboral. En este caso el TSJ consideró que la empresa había vulnerado el derecho a la intimidad del trabajador por no haber informado previamente de la instalación y localización de las cámaras de seguridad (no habían ni carteles ni se había informado individualmente el trabajador).

Sin embargo el Tribunal Europeo de Derechos Humanos con su STEDH de 17 de octubre de 2019, el caso "*López Ribalda y otros contra España*" Gran Sala[30], remota a junio de 2009 donde las trabajadoras estaban trabajando en la cadena de supermercados Mercadona: la empresa colocó una serie de cámaras ocultas para poder evidenciar sospechas de hurto, y como consecuencia de estos hechos se produjo el despido procedente de las trabajadoras. El TEDH ha dictaminado a favor del Estado Español en contra de su criterio anterior de 9 de enero de 2018 (en esta STEDH resultó favorable a las trabajadoras en base a la violación del artículo 8 –Derecho a la vida privada y familiar- del Convenio Europeo de Derechos humanos por no haberse cumplido por parte de la empresa los requisitos información de la instalación y señalización adecuados a los trabajadores en base al artículo 5 de la LOPD, actual LO3/2018 de la LOPDGDD) y consecuentemente no se tendría que indemnizar a las 5 cajeras de la cadena de supermercados citada por este Nuevo Dictamen de 2019: porque no hubo vulneración del articulo 8 del CEDH pues las trabajadoras sabían de la existencia de cámaras pero no de las ocultas y tampoco se había vulnerado el articulo 6.1 del CEDH (Derecho a un juicio justo) porque los Tribunales españoles no se habían excedido en su poder de discreción cuando dictaminaron que la vigilancia legitimada y proporcionada por parte de la empresa era lícita y

[29] Sentencia Contencioso-Administrativo STSJ Nº 1146/2020, de Andalucia, Rec 3926/2019 de 28/Mayo de 2020

30 https://www.mjusticia.gob.es/es/AreaInternacional/TribunalEuropeo/Documents/Sentencia%20López%20Ribalda%20c.%20España.pdf

justificada de acuerdo con los fines previstos. La sentencia no es recurrible y creó un nuevo precedente en la jurisprudencia de lo Social suscitando polémica por el uso de cámaras ocultas y la no preservación de los derechos de la intimidad y dignidad de los trabajadores.

El Tribunal Constitucional había dictaminado sentencias anteriores que habían creado lagunas al respecto: la STC 39/2016 del 3 de marzo, el caso "*Bershka"* [31]en la cual el TC dio razón a la empresa por el despido procedente de trabajadores basado en imágenes de cámaras instaladas sin previa información de los trabajadores ni de sus representantes;

La STC 29/2013 de 11 de febrero, caso "Universidad de Sevilla" (García Rubio, 2016) dio razón a los trabajadores por vulneración de los derechos de protección de datos por utilización de grabaciones de cámaras de video vigilancia para la supervisión laboral aunque las cámaras estaban debidamente localizadas y los trabajadores y representantes habían sido previamente informados.

También en Alemania la Sentencia del TEDH 420/2007 de 5 de octubre de 2010, el llamado caso "*Köpke contra Alemania"* que dicta lo contrario, pues en este caso no había legislación nacional y las grabaciones fueron de corta duración (apenas 2 semanas) y focalizadas en los trabajadores sospechosos (al contrario del caso "*López Ribalda"* en el cual las grabaciones habían sido prolongadas en el tiempo y a toda la plantilla) (López Cumbre, enero 2018).

Por ultimo, el caso de la STEDH del caso "*Bārbulescu contra Rumania"* número 61496/2008[32] dictaminando un fallo con 6 votos a favor y uno en contra y por lo que se admite la monitorización de las comunicaciones privadas por la entidad patronal en determinadas circunstancias dentro del principio de la proporcionalidad y respetando la dignidad del trabajador: en este caso el despido a 1 de agosto de 2007 del trabajador Bogdan Mihai

39.Sentencia 39/2016, de 3 de marzo de 2016. Recurso de amparo 7222-2013. Promovido por doña Mónica Rebeca Liberato Rodríguez en relación con las Sentencias del Tribunal Superior de Justicia de Castilla y León y de un Juzgado de lo Social de León en proceso por despido. Supuesta vulneración de los derechos a la intimidad y a la protección de datos: despido basado en las imágenes captadas por una cámara de video vigilancia instalada sin comunicación previa a la trabajadora. https://www.boe.es/boe/dias/2016/04/08/pdfs/BOE-A-2016-3405.pdf

[32] Tribunal Europeo de Derechos Humanos, Gran Sala, Sentencia de 5 Septiembre 2017, Rec. 61496/2008

Bārbulescu por el empleador se fundamentaba en el uso de Internet de la empresa (Yahoo Messenger) con fines personales y durante la jornada laboral violando las reglas internas de la misma: para el trabajador los datos interceptados entre los días 5 y 12 de julio de 2007 por la empresa eran datos personales (45 paginas de contenido sexual y de salud), sensibles y carentes de consentimiento previo (Directiva 95/46/CE) y violaban la ley de protección de datos de Rumania. Los Tribunales Nacionales Rumanos y el TEDH en 2016 no dieron razón a Bārbulescu: la conducta del empleador fue considerada lícita pues no violó el artículo 8 de la CEDH ("Derecho al respecto por la vida privada y familiar"). Sin embargo esta sentencia fue recurrida a la Gran Sala del TEDH en 2017 contra la cual no cabe recurso, y que dio amparo al trabajador rumano al entender que este desconocía que el contenido de sus comunicaciones podía ser vigilado, monitorizado o supervisado por la empresa: como tal no sucedió previamente al inicio de la vigilancia, la empresa no había respetado la privacidad del trabajador[33] (Reyes Bermejo Bosch & Botella Vivó, 43/2016)

El TEDH Gran Sala, declara finalmente que las Autoridades Rumanas no protegieron adecuadamente el derecho del trabajador al respeto de su vida privada y de sus comunicaciones, ya que estos Tribunales no determinaron en qué momento exacto del procedimiento disciplinario había accedido la empresa al contenido de las comunicaciones, lo que va en contra al principio de la transparencia; a pesar de todo, no dio lugar a compensación económica y reconoció apenas la violación del derecho: las STEDH tienen naturaleza vinculante aunque es una cuestión muy debatida- el TC afirmó en diferentes ocasiones que "*la jurisprudencia del TEDH ha de servir como criterio interpretativo en la aplicación de los preceptos constitucionales tuteladores de los Derechos Fundamentales*", según el artículo 10.2 de la CE (Legaltoday.com, 2017).

A modo de conclusión, la labor de notificación previa de los trabajadores por la empresa es crucial en lo que respeta a la colocación de cámaras de vigilancia en los centros de trabajo (según artículo 89 de la LOPDGDD), no pueden ser ocultas y deben de estar anunciadas en carteles visibles; la grabación de audio a nivel laboral en relación a conversaciones entre empleados y la licitud de los datos personales del geo localizador GPS demuestran que el tratamiento casuístico del TEDH con sus sentencias muchas veces de sentido opuesto, reflejan que la vigilancia por las empresas debe estar basada en la proporcionalidad, en el uso de la

[33] https://www.uria.com/documentos/publicaciones/5096/documento/foro02.pdf?id=6757

medida más adecuada y menos intrusiva. La necesidad de que las empresas poseen Protocolos de Uso y Medios que regulen la identificación, ubicación y finalidad así como el deber de información a los trabajadores: con estos Protocolos se consiguen informar los derechos y deberes de los empleados para con los medios que la empresa pone a su alcance destinados al desempeño laboral, y informar a priori, estos trabajadores de las acciones que en cualquier momento la empresa puede llevar a cabo en su labor de vigilancia y control, obteniendo así la cobertura legal.

Llevar a cabo un despido de un trabajador no respetando sus Derechos Fundamentales o haberlo hecho por hechos ilícitos realmente probados por un Tribunal que así dictamine la nulidad de ese despido y el pago de indemnizaciones, con la readmisión de los trabajadores, constituye una situación dañina para el benchmarking empresarial.

VIII. Uso de grabaciones de cámaras de seguridad por las Administraciones Públicas

A 1 de octubre de 2021 se confirma la sentencia en casación del Tribunal Supremo de 26/04/2021, Recurso número 4645/2019 y Resolución 557/2021[34]- que rebajó la sanción impuesta de 8 meses a 4 meses de suspensión del contrato laboral a una funcionaria de la Administración Tributaria del Estado (LO 7/2015): se discute si en el pleito, "*en el ámbito de la Administración Pública, el uso de sistemas de video vigilancia, instaladas en el edificio, con carácter permanente y con una finalidad general de vigilancia y seguridad",* exige informar a los funcionarios de manera previa, expresa e inequívoca, sobre la finalidad de control de la actividad laboral de dicho sistema y, en su consecuencia, su posible utilización para la imposición de sanciones disciplinarias.

Declara el Alto Tribunal que la instalación de las cámaras se anunciaba mediante los correspondientes carteles informativos situados en el edificio, colocación que el TC ha considerado suficiente para considerar cumplido la obligación de información, por lo que la trabajadora conocía que se había instalado un sistema de control por video vigilancia, no siendo necesario especificar, más allá de la mera vigilancia, la finalidad exacta que se hubiera asignado a ese control. Dicta el Alto Tribunal que "*Las acciones o omisiones del trabajador dirigidas a evadir los sistemas de control de horarios o a impedir que sean detectados los incumplimientos no justificados de la jornada de trabajo constituyen infracciones graves"*. Por eso, no existe injerencia de una Autoridad Publica sobre un Derecho Fundamental, como es el respeto a la vida privada y familiar, siempre que esté prevista en la Ley y constituir, en una sociedad democrática, una actuación necesaria y proporcional para la seguridad publica, para el bien estar de los ciudadanos, para la defensa del orden y la prevención de infracciones penales, para la protección de la salud publica, de la moral o de los derechos, libertades y garantías de terceros.

La instalación de cámaras de seguridad, que graben a los trabajadores en sus puestos de trabajo, está permitida dentro de la facultad de dirección del empresario pero siempre que su finalidad esté limitada a lo en el estatuto de los Trabajadores (Real Decreto 2/2015 de 23 de octubre, aprobado el texto refundido de la Ley del Estatuto de los Trabajadores)[35]: la cámara de

[34] STS 557/2021, de 26/04/2021, recurso número 4645/2019 y Resolución 557/2021

[35] BOE núm. 255 de 24/10/2015 de 13/11/2015

seguridad *"debe servir para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales"* y los trabajadores "*deben estar informados de la presencia de las cámaras"* y prestar su consentimiento expreso para que las grabaciones sean lícitas.

De acuerdo con la jurisprudencia del Tribunal Supremo[36] las Administraciones Publicas pueden utilizar las grabaciones de las cámaras de seguridad instaladas en sus edificios para vigilar controlar si los funcionarios cumplen su jornada de trabajo y se pueden usar en procedimientos disciplinarios aunque no se haya avisado (Tribunal Supremo, 2021). El uso de esta información confidencial del trabajador debe de tener un objetivo legítimo, haber necesidad y concurrir la proporcionalidad y buenas prácticas.

El empresario podrá instalar un sistema de localización de sus flotas y equipos por GPS sin necesitar el consentimiento expreso previo de sus trabajadores aunque debe informarles de ello y de cual será el tratamiento y la finalidad de los datos que se obtengan de dichos sistemas.

Los datos personales de salud, que son especialmente protegidos de acuerdo con el RGPD, requieren siempre el consentimiento inequívoco y voluntario previo del interesado; este consentimiento puede ser revocado en cualquier momento por el afectado debiendo estos datos poder ser cancelados, excepto si existiera una obligación legal de conservación por un tiempo determinado.

[36] STS 557/2021 de la sala tercera del Contencioso Administrativo en 26Abr. 2021, Rec. 4645/2019

IX. Uso de grabaciones de voz

Toda la persona tiene derecho a grabar una conversación en la cual interviene y con ello no se está realizando ninguna acción ilícita y así queda reflejado en la sentencia del TC[37] en la cual se dictamina que "…*si una persona al grabar, no está siendo parte de la conversación (grabación ajena), se vulnera el artículo 18.3 de la Constitución Española, pero que si una persona graba las palabras que un tercero le dirige, no realiza ningún hecho ilícito…".* El supuesto ilícito se podría producir en las acciones posteriores de uso y divulgación pública de los contenidos. Sin embargo, se deberá informar a la contraparte de la grabación y este debe aceptar la grabación en un proceso judicial poder solicitar un informe pericial de certificación de originalidad de la grabación, caso contrario se puede infringir derechos constitucionales como son el de la intimidad (art. 18.1 CE) o el de secreto de las comunicaciones (art. 18.3 CE) ambos recogidos y protegidos como derechos fundamentales; para que el trabajador no cometa ningún tipo de ilícito al usar aparatos de grabación debe de cumplir determinados requisitos conjuntamente (López Rivera, 2016, 11 de julio): existir una motivación (debe existir algún tipo de antecedente que la justifique: un conflicto laboral o clima laboral tenso, avisos, sanciones o llamadas de atención reincidentes previas) y que al trabajador el posible contenido de la grabación pudiera ser relevante para su situación personal; que el trabajador cuando grabe una conversación haga parte de la misma y sea en contexto laboral, aunque se pueda considerar que el uso de aparatos de escucha pueda vulnerar el art. 7.2.e) de la LO 1/1982 (Ley de protección civil del derecho al honor, a la intimidad personal y familiar y de la propia imagen); la no divulgación publica de la grabación es fundamental para que no se produzca ilícito aunque la aportación de la misma a los letrados para assessoramento o al perito para certificación de su autenticidad no se consideraría difusión ilegítima de la misma. Si concurren estos requisitos, el trabajador está legitimado para realizar la grabación sin informar a los otros participantes en la misma y sin tener que recibir autorización para ello: tiene derecho a conservar la grabación sin que nadie se la pueda retirar en caso de ser descubierta la acción de la grabación totalmente privada, suya y dentro de las instalaciones de la empresa.

El Tribunal Europeo de Derechos Humanos, Sentencia de la Gran Sala que declaró que hay intromisión en la privacidad del trabajador por monitorizar sus comunicaciones personales sin

[37] STS 5125/2014 de 20 de noviembre

aviso previo[38]: en la Sentencia de 2017 de 5 de septiembre "el TEDH se ha pronunciado en sentido contrario, al considerar que los tribunales rumanos no habían valorado adecuadamente el equilibrio entre los derechos e intereses en juego en atención a las circunstancias del caso: por un lado, el derecho a la privacidad del trabajador, y por otro lado, el derecho de la empresa a proteger el adecuado desarrollo de su negocio mediante el control de la actividad de sus empleados"

[38] https://blog.cuatrecasas.com/propiedad-intelectual/el-tedh-declara-que-existe-intromision-en-la-privacidad-de-un-trabajador-por-la-monitorizacion-de-sus-comunicaciones-personales-sin-aviso-previo/

X. La privacidad y el acceso al Correo Electrónico

En el desempeño laboral diario la comunicación a nivel empresarial publico y privado se efectúa a través de correos electrónicos, con finalidades administrativas, de gestión y coordinación de actividades y de comunicación entre los distintos colaboradores (Rafael, 2016). La empresa con sus atribuciones de control de actividades puede en determinado momento acceder al contenido del correo electrónico del trabajador lo que se de forma incorrecta ocurriera, plantear posible ilícito: el equilibrio entre los derechos fundamentales del trabajador y de la empresa como persona jurídica, teniendo como base legal el articulo 18.1 y 18.3 de la CE (Derecho al honor, la intimidad personal y familiar y al secreto de comunicaciones) y el articulo 20.3 del Estatuto de los Trabajadores (derecho de la empresa a la vigilancia y el control de actividades para verificar el cumplimiento de la obligaciones y deberes laborales del trabajador). Aunque el Tribunal Supremo[39] respalde el poder de control y vigilancia empresariales, las empresas no pueden a su libre albedrio hacer en cada momento lo que les parezca en relación a información personal de los trabajadores. El acceso a los correos electrónicos de los trabajadores debe estar sometida a determinadas condiciones como ser idóneo, necesario, excluyendo otra medida menos lesiva y proporcional a lo que se pretende[40]. La direcciones de correo electrónico grupales (usadas por diferentes personas) no son consideradas unipersonales; cada correo electrónico de salida de cada trabajador se hace en nombre de la empresa y es considerada una actividad laboral: su contenido adjunto, el redactado es siempre accesible por parte de la empresa; los correos entrantes, que se les ha nombrado " contenido de la taquilla" en medios laborales, no pueden ser investigados por las empresas a su libre albedrío y indiscriminadamente. Por esto, nunca debe la empresa consultar el buzón de entrada del trabajador al cometer un posible ilícito y que pone en duda la buena fe contractual: si es una medida necesaria, imprescindible para lograr algún objetivo, no se deben abrir indiscriminadamente todos los correos del trabajador y sólo aquellos relacionados con la actividad empresarial, como son laos correos de proveedores, clientes, administradores, etc. Un Protocolo de la Empresa que regule el destino de los correos de un trabajador que salga de la misma, impendiéndole de borrarlos y asegurando la continuidad de la labor empresarial.

[39] STS 6128/2007 de la Sala 4ª de lo Social de 26 de septiembre de 2007

[40] https://peritoit.com/2016/05/12/la-privacidad-en-el-correo-electronico-de-la-empresa/

XII. Conclusiones

La esencia del derecho de autodeterminación informativa consiste en el derecho de control sobre los datos personales por parte del titular de los mismos: este control se manifiesta por el poder de acceder, rectificar o anular los datos personales almacenados en bancos de datos electrónicos, ejerciendo el ciudadano una función preventiva al dar su consentimiento expreso para que estos datos puedan ser accedidos, rectificados, cedidos o anulados por terceros.

El sistema de protección de datos personales almacenados en bancos de datos electrónicos o no, debe de estar amparado por el derecho fundamental a la intimidad y protección de datos personales. En España este derecho fundamental se proyectó a la llamada "*era de la información"* para la protección de la intimidad frente a uso de las TIC y de la informática. Cuando este derecho a la intimidad informática esté consagrado como derecho fundamental, es decir, posea una previsión en una Norma Constitucional de forma material, mayores garantías se podrán ofrecer a los ciudadanos en relación a la protección de la intimidad frente al uso de las TIC. Mientras tanto, las Sentencias de los Tribunales pueden tener direcciones opuestas dependiendo de cada hecho lo que conduce a una inseguridad jurídica indeseable.

Hay un camino para recoger de forma a que la jurisprudencia se fundamente en normas constitucionales y ayude a aportar mayor previsibilidad de las sentencias de los Tribunales que son todavía muy variables dependientes de la gran variabilidad de situaciones socio laborales: en relación a la pregunta de investigación de este trabajo "*Existe de forma efectiva Confidencialidad y Protección de datos personales en Derecho Laboral?"* se piden políticas y medidas públicas que permitan asegurar la protección adecuada de los datos personales de las personas físicas, y así responder a retos planteados por la transformación digital del trabajo, rápida y inexorable, que contribuya para la promoción laboral, inclusiva, sostenible, en equidad, digna y segura para todos. La mejor manera de lograrlo es a través del diálogo social y de coordinación normativa entre cuatro partes interesadas: las plataformas digitales de trabajo, los trabajadores, los representantes de estos y los Gobiernos, creadores de políticas públicas.

XIII. Bibliografía

Administrativo, D. d. (2021). *Asociación Española de Protección de Datos.* Obtenido de https://www.aepd.es/sites/default/files/2019-10/infografia-decalogo-personal-sanitario.pdf

Aguiar, A. R. (2021). ” El Comité Europeo de Protección de Datos insta a la UE a prohibir los sistemas de reconocimiento biométricos en el espacio publico”, junio 21 . *Business Insider España*.

Aguilar del Castillo, M C. Universidad de Sevilla. (2016). La protección de datos entre su contenido constitucional y su contenido legal. *ISSN 2421-2695*, volume 2.

Aguilar del Castillo, M. (2018). El derecho de huelga y el uso de la tecnología: realidades en conflicto. *Labour and Law Issues*, vol.4, n.1.

Aguilar del Castillo, MC. Universidad de Sevilla. (2018). El uso de la tecnología y el Derecho de Huelga: realidades en conflito. *ISSN 2421-2695*, Vol.4 n.1 .

Benson, J. (s.f.). *British Coalminers Nineteenth Century: A Social History.* Longman Higher Education.

Cáceres, M. E. (2013). La Huelga “Grande” Del Carbón En Lota, Coronel Y Curanilahue De 1920. *Hao, Número 32 (Otoño, 2013), Issn 1696-2060*, 73-79.

Casas, B. C. (2017, 6 de septiembre).

Comisión Europea. (2021). *Digital Economy and Society Index (DESI).*

DHpedia. (2021). *La "wiki" de los derechos humanos.* Obtenido de https://dhpedia.wikis.cc/wiki/Portada

El Tedh Declara Que Hay Intromisión En La Privacidad Del Trabajador Por Monitorizar Sus Comunicaciones Personales Sin Aviso Previo. (2017). *Cuatre Casas*.

España, G. d. (2021). *Ministério de Derechos Sociales y Agenda 2030*. Obtenido de Agenda 2030: https://www.mdsocialesa2030.gob.es/agenda2030/index.htm

García Rubio, M. A. (2016). Nueva doctrina constitucional sobre videovigilancia laboral y protección de datos personales. *Elderecho.com*.

Garriga Domínguez, A. (s.f.). La protección de los datos de carácter personal en el ámbito europeo. Especial referencia al Convenio 108 del Consejo de Europa y a la Directiva 95/46/CE. *V Lex, Información Jurídica Inteligente*, 149-159.

Ilo.org. (2008). *OIT.* Obtenido de http://www.ilo.org/global/about-the-ilo/mission-and-objectives/WCMS_099768/lang--es/index.htm: http://www.ilo.org/global/about-the-ilo/mission-and-objectives/WCMS_099768/lang--es/index.htm

Legaltoday.com. (2017). *Legaltoday.com.* Obtenido de Thomson Reuters Aranzadi Fusión: https://www.legaltoday.com/files/File/pdfs/Sentencia-id190106.pdf

Luño, A. E. (2000). La tutela de la libertad informática en la sociedad globalizada, pg 59-68. *ISEGORfA/22* .

López Cumbre, L. (enero 2018). Vigilar ocultamente a los trabajadores en la empresa y la reciente doctrina del Tribunal Europeo de Derechos Humanos. *Gómez-Acebo y Pombo*, 2-4.

López Rivera, R. (2016, 11 de julio). Grabación de conversación por un empleado en la empresa. *Revista ACPJ*.

OIT. (1998). *ILO Declaration on Fundamental Principles and Rights at Work) fue aprobada en la 86ª reunión, Ginebra, junio de 1998.* Obtenido de ilo.org

Organización Internacional del Trabajo. (2021). *Perspectivas Sociales y del Empleo en el Mundo, Resumen ejecutivo.*

Paniagua Alario, A. M. (2021). Protección de Datos y Relaciones Laborales. *Prodata.es*, Parte II.

Rafael, L. R. (2016). La privacidad en el correo electrónico de la empresa. *Perito Informático y tecnológico*.

Redaccion . (2014, 15 de ocubre). ¿Qué sabemos del origen del Compliance Penal, el concepto de moda? *Diario Juridico.com*.

Reyes Bermejo Bosch, R., & Botella Vivó, S. (43/2016). La Sentencia Del Tedh Sobre El Control Por El Empleador Del Uso Del Correo Electrónico (Mensajería Instantánea) Por Sus Empleados (Caso Barbulescu V. Rumanía N.O 61496/08 De 12 De Enero De 2016). *Actualidad Jurídica Uría Menéndez* , 90-94.

Rosa, Espín: Universitat Autònoma de Barcelona. (14/09/2017). El canal de denuncias internas en la actividad empresarial como instrumento de compliance. *TDX 2001-2021, Tesis Doctorales en Xarxa. ISBN: 9788449077104*, 417.

Sánchez Pérez g, Rojas González Isai. Universidad Nacional Autónoma de México . (s.f.). Leyes de protección de datos personales en el mundo y la protección de datos biométricos- Parte 1. .*Seguridad Bimestral*, número 13.

Sánchez Pérez, G., & Rojas González, I. (s.f.). Revista . Seguridad ,Source URL: https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93, número 3. .*Seguridad*, 2.

Sierra Benítez, EM Universidad de Sevilla, Derecho del Trabajo. (s.f.). Seguridad Social sostenible y Sistemas de Protección Social en la era digital europea. *Revista do Conselho de Recursos da Previdência Social, CRPS: Previdência e JUstiça*.

Tablado, F. (2020, 17 de marzo). Due Diligence, Qué es y para que sirve? *Grupo Atico 34*.

Tascón López, R. (2016). El lento pero firme proceso de decantación de los límites del poder de control empresarial en la era tecnológioca. *Revista Doctrinal Arazadi Social número 17/207, vol. 2, no. 1, 2016 ISSN: 2421-2695*.

TRABAJADORES, R. D. (1996). *Organización Internacional del Trabajo.* Obtenido de Codigo del proyecto OIT/96/29.

Trabajo, L. R. (2019). *LAS REGLAS DEL JUEGO Una introducción a la actividad normativa de la Organización Internacional del Trabajo.* Ginebra: OIT.

Trabajo, O. I. (1996). *OIT.* Obtenido de OIT: https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_008427/lang--es/index.htm

Tribunal Supremo, S. T.-a. (2021). *Diario La Ley.* Obtenido de Diario la Ley: diariolaley.laleynext.es

Villalba Sanchez, A. (2018). El derecho fundamentala la protección de datos del trabajador frente a los riesgos de la contratación estandaddizada. *Revista Española de Derecho del Trabajo* , 207, ISSN 2444-3476.

VLex. (1993). *Información Jurídica Inteligente.* Obtenido de VLex: https://vlex.es/vid/on-via-144795

VLex: Información Jurídica Inteligente. (30/11/2016). STS 766/2020, 15 de Septiembre de 2020. *V Lex*.

Legislación, Normas y Jurisprudencia

España

Constitución Española de 1978

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del honor, la intimidad la propia imagen

Ley Orgánica 3/1985, de 29 de mayo (sobre modificación de la LO 1/1982)

Ley Orgánica 5/1992, " Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos personales" (LORTAD)

Ley Orgánica 15/1999 de 13 de diciembre "Ley Orgánica de Protección de Datos de Carácter Personal" (LOPD)

Real Decreto 1332/1994 de 20 de junio

Real Decreto Legislativo 2/2015, de 23 de octubre

Real Decreto-ley 9/2021, de 11 de mayo

STC 110/1984 de 21 de diciembre

STC 254/1993 de 20 de julio

STC 292/2000 de 30 de noviembre

STS 6128/2007 de la Sala 4ª de lo Social de 26 de septiembre

STS 5125/2014 de 20 de noviembre

Sentencia 39/2016, de 3 de marzo de 2016. Recurso de amparo 7222-2013

STS 766/2020, Sala de lo Social de 25 de septiembre, Unificación Doctrina

Sentencia Contencioso-Administrativo STSJ 1146/2020, Rec 3926/2019 de 28 de mayo

STS 557/2021 de la sala tercera del Contencioso Administrativo en 26Abr. 2021, Rec. 4645/2019

Unión Europea

Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril (RGPD)

Directiva de la UE 2019/1937 do Parlamento Europeo y del Consejo de 23 de octubre de 2019: Protección de Whistleblower publicado en Jornal Oficial de la UE de 26/11/2019

Tribunal Europeo de Derechos Humanos

Tribunal Europeo de Derechos Humanos, Gran Sala, Sentencia de 5 Septiembre 2017, Rec. 61496/2008

STS 557/2021, de 26/04/2021, recurso número 4645/2019 y Resolución 557/2021

Los derechos de los trabajadores han experimentado grandes modificaciones y han contribuido a asegurar en la actualidad, la protección de datos confidenciales legalmente protegidos en numerosos textos legales. La Organización Internacional del Trabajo creada en 1919, a través de su original estructura tripartita se han logrado acuerdos entre empleadores, trabajadores y Sindicatos, de forma a asegurar los derechos y garantías de los trabajadores y la mejoría de las condiciones laborales.

Aunque el tratamiento de los datos personales y su confidencialidad estén previstos en la Constitución Española y en Leyes Orgánicas, Directivas Comunitarias y por aplicación directa del Reglamento Europeo de Protección de Datos, la posición de subordinación y dependencia de los trabajadores en relación con el empleador público o privado y la variabilidad de situaciones socio laborales y jurisprudenciales revisten de inseguridad jurídica este tema tan sensible y actual.

9 791387 676193