CONTROL TECNÓLÓGICO Y CON INTELIGENCIA ARTIFICIAL DEL TRABAJADOR. GARANTÍAS DE PRIVACIDAD Y PROTECCIÓN DE DATOS

LORENZO COTINO HUESO

Catedrático de Derecho Constitucional, Universitat de Valencia, OdiseIA[1]

La inteligencia artificial y el internet de las cosas han llegado al trabajo

Las autoridades de protección de datos están atentas al fenómeno.

La aplicación del régimen general de protección de datos al control laboral con estos sistemas.

Dignidad, legitimación del control tecnológico por el empleador.

Empleador que avisa no es traidor: obligaciones del empresario para poder controlar.

No cabe un control "total" del trabajador, sino proporcional.

Garantías concretas en controles ocultos, fuera del trabajo, geolocalización, datos biométricos, decisiones automatizadas y captación de audio.

La inteligencia artificial y el internet de las cosas han llegado al (control del) trabajo

En el ámbito empresarial e industrial proliferan de natural los sistemas inteligentes de monitorización, control, optimización especialmente respecto de la producción. En el ecosistema de la *Smart Office*, cada vez es mayor la oferta de productos y servicios para el control y monitoreo del trabajador a partir de la extracción, comunicación y tratamiento de datos del trabajador; controles de accesos y de horarios, vigilancia y localización de los empleados, seguimiento de sus movimientos. Se dan cada vez más servicios de ubicación en tiempo real que se integran con funcionalidades de comunicaciones y actividad del trabajador, relaciones con clientes y otros trabajadores. Asimismo, también

[1] El presente estudio es resultado de investigación del proyecto "Derecho, Cambio Climático y Big Data", Grupo de Investigación en Derecho Público y TIC como investigador de la Universidad Católica de Colombia. De igual modo, en el marco del proyecto MICINN Retos "Derechos y garantías frente a las decisiones automatizadas... (RTI2018-097172-B-C21); también "La regulación de la transformación digital …" grupo de investigación de excelencia Generalitat Valenciana "Algoritmic law" (Prometeo/2021/009, 2021-24) y estancia (AEST/2021/012).

son crecientes los productos destinados al cumplimiento de la seguridad e higiene, también por el Covid, al confort del empleado, la eficiencia y uso de los recursos de la empresa, herramientas laborales con sensores, etc. De todos ellos se generan datos que, en su caso, pueden servir también al control de obligaciones, control de productividad, etc.

Todos estos datos que se generan alimentan tratamientos de datos de perfilados y sistemas automatizados especialmente relativos a la eficiencia y conducta del trabajador. Y ello deriva también de natural a sistemas que evalúan la actividad del trabajador misma, la evolución de trabajo, incluso señales de bienestar o malestar. Asimismo y como se verá, hay que prestar especial atención a la captación y tratamiento de datos biométricos del trabajador.

Obviamente se puede directamente captar y grabar toda la actuación del trabajador. La sensorización incluye elementos de medición de distancia y trazabilidad de personas, lectores biométricos para el control de acceso, medición de presencia y ocupación, temperatura y otras condiciones ambientales, contador de personas, posición/ distancia social. En muchos de estos casos es posible que se haga, además, un tratamiento de datos biométricos, tanto por las características físicas o fisiológicas, como sobre todo por las pautas conductuales del trabajador. Especialmente conflictivos son los tratamientos masivos de datos de trabajadores en ámbitos cada vez más importante en las economías de plataforma, donde ya se han producido importantes sentencias sobre discriminación laboral por el algoritmo (Castillo 2021). También se da el rastreo continuo a través de pulseras y dispositivos de seguimiento. Se controla no sólo la ubicación, sino la velocidad, trayectos, movilidad en el establecimiento, etc. Y a partir de ahí se extraen evaluaciones y se adoptan decisiones empresariales. Todos estos datos se captan y se comunican en la capa de *Gateway* (*Wifi, Bluetooth, Zigbee*) para la extracción de información y usos en la capa de *Backend* para su uso por el empresario.

Debe tenerse en cuenta que el control de la actividad puede implicar ascensos, despidos, determinación de carga y horario de la empresa, movilidad geográfica, pago de bonificaciones, etc. Además de la afectación de los derechos de la personalidad, en concreto de la privacidad y protección de datos así como el derecho frente a decisiones automatizadas y perfilados, puede quedar afectada de modo muy importante la igualdad y la no discriminación. El presente estudio es una aproximación a esta cuestión, respecto de la que aún se dan importantes cuestiones. Destacan sin duda en la materia trabajos de

Todolí[2]. Asimismo, sin duda habrá que estar atentos al desarrollo del futuro reglamento de inteligencia artificial (IA) de la UE, en virtud del cual muchos tratamientos con IA son de alto riesgo y quedarán sometidos a un intenso régimen (Cotino, et al, 2021).

Las autoridades de protección de datos están atentas al fenómeno

El marco jurídico al respecto no es en modo alguno sencillo y se trata, sin duda de una cuestión de gran importancia tanto para la seguridad jurídica empresarial cuanto para los trabajadores, materia a la que los sindicatos han sido sensibles (CCOO; UGT, 2018). La AEPD ha realizado importantes esfuerzos en la materia desde antiguo. En este sentido especialmente ha destacado la *Guía La protección de datos en las relaciones laborales* de 2009. Desde entonces ha habido muy relevantes cambios normativos tanto por el RGPD como por la propia LO 3/2018 y en la jurisprudencia europea y española. La AEPD fue actualizando algunos de sus materiales respecto de cámaras para el control empresarial y realizando actividades y documentos de interés[3]. Asimismo, aunque totalmente orientado a cuestiones de prevención de acoso o violencia sexual, cabe tener presente el Protocolo del Ministerio y la AEPD (MTAS-AEPD, 2019) También, son plenamente aplicables en cualquier situación las importantes *Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo* (AEPD 2020 a), inspiradas en las políticas al respecto del NIST de EEUU (Souppaya y Scarfone 2020).

Al respecto de este último documento, por cuanto a la relación con el tema que nos ocupa, baste ahora recordar la necesidad de que los empresarios que utilicen soluciones IOT han de elegir herramientas y prestadores de servicio confiables y con garantías y que "eviten la exposición de los datos personales del personal, interesados y servicios corporativos de la organización". Obviamente, el empresario como responsable del tratamiento de datos que se produzca por el uso de servicios y aplicaciones IOT para el trabajo a distancia, debe velar por el cumplimiento de todas las exigencias por el encargado, que deben figurar en el contrato en los del artículo 28.3 del RGPD (objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable). Y, en general, el cumplimiento de las exigencias de seguridad de protección de la información que se está manejando. También en interés de los derechos del propio trabajador se recuerda que

[2] Referenciados en la bibliografía final.

[3] Con el nuevo contexto normativo, destacan AEPD, 2018, (s.f.) y 2019.

una vez concluida la jornada de trabajo en situación de movilidad debe desconectarse la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo.

En todo caso, ha destacado que recientemente la AEPD ha actualizado su guía en mayo 2021 (AEPD, 2021 a). De igual modo, sigue siendo un referente esencial el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29[4]. Cabe tener en cuenta algunos lineamientos básicos aplicables en la materia, que cabe ahora recordar.

El Estatuto de los Trabajadores, artículo 20.3, atribuye facultades específicas a la empresa que posibilitan el control del desarrollo de la prestación laboral, por lo que: la legitimación para el tratamiento deriva de la existencia de la relación laboral, no del consentimiento del trabajador. La finalidad ha de ser la establecida por el art. 20.3 ET: «verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales».

Ello, en términos del RGPD se traduce en que la legitimación básica va de la mano de la necesidad para la ejecución de un contrato en el que el interesado es parte (art. 6.1 b) RGPD). Y tanto el RGPD como el mencionado art. 20.3 ET son las bases legales que legitiman en principio el tratamiento .En no pocas ocasiones, el tratamiento de datos es obligatorio para el empresario (Art. 6.1 c) RGPD (p. e. cotización de Seguridad Social, obligaciones tributarias, registro de jornada, información y consulta con representantes de las personas trabajadoras, etc.), ahí, la base legal se hará depender de la obligatoriedad al empresario por vía legal o por convenio colectivo (AEPD, 2021 a, p. 9) No hay que excluir en su caso el interés legítimo

Cuando los controles del empresario se basen en el uso de tecnologías de la información (controles biométricos, la videovigilancia, los controles sobre el ordenador, o los controles sobre la ubicación física del trabajador mediante geolocalización), deberá cumplirse lo establecido en la normativa de protección de datos.

Debe cumplirse con el deber de información: reglas o políticas de uso de los dispositivos y medios puestos a disposición del trabajador (art. 13 y 14 RGPD).

Los datos que se obtengan y almacenen deberán ser exactos y puestos al día y no podrán conservarse más tiempo del necesario.

Además el uso de tecnologías de la información multiplica las posibilidades de control empresarial y obliga a tener en cuenta el respeto a los derechos fundamentales de

[4] https://ec.europa.eu/newsroom/article29/items/610169

los trabajadores, a adoptar medidas de control que sean proporcionales y respeten su dignidad, su derecho a la protección de datos y su vida privada.

A la hora de decidir adoptar una medida de control que comporte un tratamiento de datos personales debe aplicarse el principio de proporcionalidad.

Como se verá, adquiere especial importancia este principio ante la captación masiva de datos laborales y la extracción intensiva de información del trabajador a través de sistemas IOT, luego muchas veces tratados con sistemas automatizados e incluso inteligentes.

La aplicación del régimen general de protección de datos al control laboral con estos sistemas

Las líneas maestras en la materia se han marcado en diversos documentos internacionales sin valor normativo y vinculante, pero de necesario seguimiento. Así, desde 1997 en el Código de buenas prácticas para la protección de los datos personales del trabajador de la OIT (1997). Pese a elaborarse para el anterior marco jurídico, destaca especialmente la Opinión 8/2001 del Grupo de Trabajo del artículo 29 sobre el tratamiento de datos en el contexto del empleo (GT 29 2002. Más reciente y actualizada es la Recomendación CM/Rec 2015 del Comité de Ministros del Consejo de Europa, sobre el tratamiento de datos personales en el ámbito de la relación laboral[5].

El RGPD establece un marco que han de seguir los Estados en la materia. Así, en esencia, las leyes y convenios colectivos nacionales han de regular los tratamientos y además han de incluir garantías adecuadas, especialmente en materia de información y transparencia y en particular por cuanto "a los sistemas de supervisión en el lugar de trabajo"[6].

---

[5] Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies) acceso en https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

[6] Del artículo 88 RGPD cabe destacar que remite a las leyes y convenios colectivos que los Estados "podrán" adoptar respecto de tratamientos de datos en el ámbito laboral "incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo […] gestión, planificación y organización del trabajo […] salud y seguridad en el trabajo, protección de los bienes de empleados o clientes (art. 88. 1º).

Se impone que las "normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando

Debe señalarse que es especialmente importante la jurisprudencia europea en la materia, a la que necesariamente debe ajustarse la acción del legislador y la jurisprudencia nacional. Y debe también apuntarse que la jurisprudencia en la materia no deja de evolucionar y fijar criterios, si bien, con carácter bastante oscilante y dejando abiertas no pocas cuestiones.

La LO 3/2018 contiene una mayor de las posibilidades del control tecnológico. Así, ha modificado el Estatuto de los Trabajadores, Real Decreto Legislativo 2/2015, de 23 de octubre (ET) y ha regulado la intimidad laboral y algunos requisitos y garantías del control laboral y uso de medios tecnológicos (art. 87), con particularidades para la captación de audio y vídeo (art. 89) y la geolocalización de los trabajadores (art. 90). La normativa ha recogido en buena medida los criterios jurisprudenciales básicos en la materia, aunque sigue dejando espacio a la incertidumbre.

El papel de los Convenios Colectivos laborales es importante. Es más, hay que partir de que estas normas pueden ser suficientes como base legal para efectuar tratamientos de control laboral, a partir del artículo 88 RGPD así como en razón del artículo 91 LO 3/2018[7]. Asimismo, las decisiones, políticas o normativas internas que fije el empresario son decisivas. Respecto de las mismas cabe adelantar que "deberán participar los representantes de los trabajadores" en los "criterios de utilización de los dispositivos digitales" que debe establecer el empleador (art. 87.2º). Ello debe ponerse en relación con los apartados 5 y 6 del art. 64 del ET. Alguna sentencia ya ha señalado que la falta de participación de los trabajadores en estas decisiones es un elemento más para la nulidad del control laboral efectuado[8].

En cualquier caso, debe reiterarse que esta regulación converge con todas las exigencias del régimen general de protección de datos en tanto en cuanto el empleador que controla tecnológicamente a sus trabajadores efectúa un tratamiento de datos. Ello impone, como siempre, proyectar para el ámbito concreto los principios relativos al

especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo" (art. 88. 2º).

[7] Artículo 91. Derechos digitales en la negociación colectiva. Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

[8] Audiencia Nacional, Sala de lo Social, Sentencia 13/2019 de 6 Feb. 2019, Proc. 318/2018, http://bit.ly/2SOTMGM%20 Ver FJ 4º

tratamiento, en particular la minimización y privacidad en el diseño tecnológico y de especial incidencia, el principio de proporcionalidad.

Por cuanto a la licitud del tratamiento, como se ha adelantado, que supone el control laboral tecnológico se da en razón de los mencionados preceptos del ET y LO 3/2018 y muy excepcionalmente en el consentimiento, al tratarse de una relación laboral naturalmente asimétrica. Frente al consentimiento, adquiere una esencial importancia en la materia la transparencia y la información a facilitar a la persona interesada. Como se verá, la información del control laboral hace que no se dé una expectativa razonable de confidencialidad respecto de los derechos de intimidad y secreto de las comunicaciones.

Se han de dar especiales cautelas respecto del tratamiento de categorías especiales de datos personales, y en particular por cuanto al tratamiento de datos biométricos.

Obviamente, el esquema de análisis de estos tratamientos de control del empleador obliga a seguir los derechos de la persona interesada y pueden adquirir especial importancia las condiciones para las transferencias internacionales de datos, en tanto en cuanto las plataformas y servicios que use el empleador impliquen tales transferencias. De igual modo es muy relevante el cumplimiento del registro de actividades de tratamiento, la adopción de medidas proactivas se seguridad y garantías específicas a los trabajadores.

Para el ámbito del reconocimiento facial y tratamiento de datos biométricos, recientemente la AEPD ha señalado que es plenamente aplicable el "principio de responsabilidad proactiva y de protección de datos desde el diseño por defecto, para lo que resulta esencial la realización del correspondiente análisis de riesgos, conforme al artículo 24 del RGPD. Por otro lado, hay que tener en cuenta que nos encontramos ante tratamientos de categorías especiales de datos, sujetos a una especial protección, cuyo tratamiento en el presente caso va a implicar un alto riesgo que haría necesario la realización de una evaluación de impacto en la protección de datos". (AEPD, 2021 a pp. 25 y ss. y AEPD, 2020 b).

Dignidad, legitimación del control tecnológico por el empleador

El punto de partida es la dignidad del trabajador reconocida obviamente también en el ámbito laboral. La importante STS de 26 de septiembre de 2007 de unificación de doctrina en la materia, recordó que la exigencia de respetar en el control la dignidad humana del trabajador es general para todas las formas de control empresarial (FFJJ 3º y 4º). A partir de la dignidad se reconoce el "derecho a la intimidad en el uso de los

dispositivos digitales puestos a su disposición por el empleador […] y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización" (art. 20 bis ET). Debe señalarse que la garantía de la intimidad también se extiende a los archivos personales del trabajador que se encuentran en el ordenador, incluso a los archivos temporales y los rastros o huellas de la "navegación" (STS de 26 de septiembre de 2007).

El trabajador tiene también "la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración" todo ello bajo "las exigencias de la buena fe." (Art. 20. 2º ET).

Y hay que tener en cuenta que el consentimiento del trabajador no es libre y no legitima el control laboral. Debe recordarse que el consentimiento no es la base de legitimación que pueda permitir el tratamiento de datos de los trabajadores y su control tecnológico. Y ello es así porque no se dará esencialmente el requisito de voluntad libre (art. 7. 1º RGPD). El considerando 43 del RGPD establece que no es posible aceptar la licitud para el tratamiento y procesamiento de datos basadas en el consentimiento en una relación donde exista un fuerte desequilibrio de poder entre las partes. El Grupo de Trabajo del artículo 29, en su Guía sobre el consentimiento entiende que el consentimiento de un trabajador difícilmente será "libre" y, como regla general, no se deberá entender válido el otorgamiento de consentimiento por parte del trabajador, teniendo que ser solamente aceptado como válido de forma excepcional. Para su admisibilidad, se deberá demostrar que el trabajador sabía que no había consecuencias adversas con independencia de si otorgaba consentimiento o no.

La STC 39/2016 de 3 de marzo, recuerda que la existencia de la relación laboral entre las partes hace innecesario el consentimiento individual de los trabajadores para la adopción de medidas de control de la actividad laboral. En la misma línea, la AEPD (Procedimiento Nº: PS/00401/2018) recuerda que

"para la instalación de un sistema de videovigilancia con finalidad de control del cumplimiento de las obligaciones laborales no es necesario el consentimiento de los empleados ni constituye per se una base jurídica legitima para el mismo. La base jurídica para la monitorización del cumplimiento de las obligaciones encomendadas a los empleados a través de dicho sistema no es la del consentimiento, toda vez que este no se obtiene ni se presta libremente, ni se puede retirar libremente sin consecuencia negativa alguna, dado el ámbito de sujeción y vinculación de los empleados.

Los trabajadores casi nunca están en condiciones de dar, denegar o revocar el consentimiento libremente, habida cuenta de la dependencia que resulta de la relación

empresario/trabajador. Dado el desequilibrio de poder, los trabajadores solo pueden dar su libre consentimiento en circunstancias excepcionales, cuando la aceptación o el rechazo de una oferta no tiene consecuencias."

No son válidas cláusulas contractuales o en otros instrumentos jurídicos que impliquen el consentimiento del trabajador para tratamientos de datos ajenos objeto del contrato y la propia prestación laboral. En esta línea, por ejemplo, la STS 21 de septiembre de 2015 declaró nula la cláusula tipo del contrato de trabajo en la que se hace constar la posibilidad de que la empresa pueda efectuar comunicaciones al trabajador vía SMS o vía correo electrónico, según los datos facilitados por el trabajador a efectos de contrato, con la obligación, además, de comunicar a la empresa de forma inmediata cualquier cambio o incidencia en el teléfono o en el correo electrónico.

Y de modo más concreto para el ámbito que nos interesa, la SAN de 6 de febrero 2019, Social, 13/2019, Proc. 318/2018[9] anula, asimismo, cláusulas introducidas en los nuevos contratos que condicionaban la relación laboral de repartidores de pizza a la aportación del móvil personal y la descarga y uso de una aplicación o App para hacer un seguimiento del trabajador seguimiento.

Empleador que avisa no es traidor: obligaciones del empresario para poder controlar

Cabe centrarse ahora en el control empresarial, políticas de uso de medios y transparencia sobre el control tecnológico del empleador. Y es que al mismo tiempo y por su parte, el empleador tiene reconocida la facultad de dirección y control de la actividad laboral. Para ello "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" (art. 20. 2º ET). En uso de su poder de dirección, el empleador "podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos." (art. 87. 2º). Y para ello, el empleador también está sometido a las exigencias de buena fe y asimismo se concretan diversos requisitos y garantías. Esencialmente, esta buena fe se traduce en la previa advertencia sobre el uso y el control del ordenador, información sobre el mismo y el establecimiento de las reglas de uso de esos medios.

[9] http://bit.ly/2SOTMGM%20

En esta dirección, la legislación impone que se "deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad" y, como se ha adelantado "En su elaboración deberán participar los representantes de los trabajadores." (art. 87. 3º). Y como parece señalar la jurisprudencia, la falta de participación de los trabajadores puede ser un elemento que conlleve la ilicitud del control.

Las garantías de transparencia se concretan de algún modo en el artículo 89 para el ámbito de "videovigilancia y de grabación de sonidos" y el artículo 90 respecto de la geolocalización.

-Se exige la información "con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida." (art. 89. 1º y en términos similares en el artículo 90. 2º).

-Habrá de informar del ejercicio de los derechos (art. 90. 1º, con referencia a la geolocalización).

Por cuanto al deber de transparencia debe recordarse el control empresarial es un tratamiento de datos, por lo que rigen los deberes de transparencia y el derecho de acceso del afectado fijados por la normativa. El deber de transparencia también obligará a informar al afectado de las evaluaciones y perfilados que se realicen legítimamente a partir de los datos extraídos.

Recientemente, la Carta de derechos digitales en su artículo XIX. 2. B) señala que "se informará a la representación legal de las personas trabajadoras. Esta información alcanzará los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de IA que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles."(Gobierno de España 2021). De igual modo deben ser informados de "la política de uso tales dispositivos digitales, incluidos los criterios para una eventual utilización para fines privados." (art. XIX. 2 f).

La STC 29/2013, de 11 de febrero consideró insuficiente y nula por vulneración de protección de datos que se informara de que existía videovigilancia por motivos de seguridad, sino que era preciso que la finalidad fuera la del control laboral. Se entendió que la finalidad del tratamiento de datos era la seguridad y se consideró que era incompatible con la finalidad del control laboral. No obstante, estas exigencias se han atemperado con la STC 39/2016 de 3 de marzo de 2016. Se admite la videovigilancia porque el trabajador conocía que en la empresa se había instalado un sistema de control

por videovigilancia, sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control. Lo importante para el será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato.

En España, la STSJ Navarra de 18 de febrero de 2019 (Nº de Recurso: 875/2018)[10] ya en aplicación de la LO 3/2018 ha sido especialmente exigente con la obligación de informar sobre el control tecnológico, conllevando la nulidad de los datos obtenidos del trabajador.

Resulta un elemento jurídico básico, la expectativa razonable de confidencialidad, transparencia y uso particular de los medios informáticos. Así, las SSTC 241/2012, de 17 de diciembre y 170/2013 de 7 de octubre reconocieron el poder empresarial de control y que no hay vulneración de la intimidad cuando no hay una expectativa de confidencialidad o intimidad. Y esta expectativa está directamente relacionada con la transparencia y conocimiento del tratamiento de datos y las políticas de uso de medios informáticos.

El trabajador no tiene esta expectativa s cuando se utilizan los medios informáticos de la empresa contra las normas, convenios colectivos e instrucciones fijadas por el empresario[11].

Sin embargo, sí que se da esta expectativa cuando trabajador no estaba advertido de la posibilidad de que sus comunicaciones o el uso de los medios de la empresa pudieran ser objeto de seguimiento por el empleador (SSTEDH de 25 de junio de 1997, caso *Halford c. Reino Unido*, § 45; de 3 de abril de 2007, caso *Copland c. Reino Unido*, § 42 y 47).

Debe recordarse al respecto que si no hay tolerancia de uso personal de los dispositivos, no hay expectativa razonable de la intimidad y el empresario sí que puede controlar el uso (Tribunal Supremo de 6 de octubre de 2011)

No cabe un control "total" del trabajador, sino proporcional

Es muy importante señalar que la STS de 26 de septiembre de 2007 de unificación de doctrina pareció permitir que las normas e instrucciones empresariales pudieran establecer "prohibiciones *absolutas* o parciales" respecto del uso de los medios de la

[10] http://www.poderjudicial.es/search/openDocument/e9e15eb131e642c9

[11] FJ 5, STC 170/2013 de 7 de octubre.

empresa. Ello llevó en cierto modo considerar permitido que el empresario pudiera llegar a efectuar un control total del uso de medios informáticos, siempre que fuera conocido por el trabajador y por tanto no tuviera expectativa de confidencialidad.

No obstante, en este punto hay que subrayar el punto de inflexión que implica la STEDH -Gran Sala- 5.9.2017, Caso Barbulescu II. El TEDH tiene en cuenta también la proporcionalidad para dar por bueno el control (en especial ap. 121). Frente a la doctrina asumida por el TS y el TC, ya no es suficiente que trabajador conozca el control por el empresario, no cabe un control absoluto, "las instrucciones de un empleador no pueden reducir la vida social privada en el lugar de trabajo a cero. El respeto por la vida privada y por el secreto de la correspondencia continúa existiendo" (ap. 80). La sola información al trabajador no basta.

La STS Sala de lo Social, de 8 de febrero de 2018[12] ha interiorizado de algún modo esta doctrina[13] subrayando no sólo la necesidad de que las medidas de vigilancia avisadas con carácter previo con claridad y concreción y recordando que la vigilancia del contenido exige siempre una justificación, así como que no haya otras alternativas para alcanzar el mismo fin. De igual modo se recuerda que no se puede divulgar el contenido de las comunicaciones y que la empresa está obligada a establecer garantías de privacidad para el trabajador en las comunicaciones.

Además de los requisitos de legitimación y base legal, minimización y esencialmente de transparencia e información del control laboral, cada vez cobra más importancia la ponderación de la proporcionalidad del tratamiento y control tecnológico del trabajador. Como es sabido, este control de proporcionalidad implica analizar si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad, 1º). Si la no hay otra alternativa que impacte menos en los derechos del trabajador, una medida

[12] STS de 8 de febrero de 2018,Nº de Resolución: 119/2018 http://www.poderjudicial.es/search/openDocument/caec97ebe1e1545f/20180305

[13] Y lo hace afirmando que ciertamente no hay especial novedad: "tales consideraciones del Tribunal Europeo nada sustancial añaden a la doctrina tradicional de esta propia Sala (las ya citadas SSTS 26/09/07 -rcud 966/06 - ; 08/03/11 -rcud 1826/10 -; y SG 06/10/11 -rco 4053/10 -) y a la expuesta por el Tribunal Constitucional en la sentencia de contraste [STC 170/2013], así como a las varias suyas que el Alto Tribunal cita [así, SSTC 96/2012, de 7/Mayo, FJ 10 ; 14/2003, de 28/Enero, FJ 9 ; y 89/2006, de 27/Marzo , FJ 3], pues sin lugar a dudas los factores que acabamos de relatar y que para el TEDH deben tenerse en cuenta en la obligada ponderación de intereses, creemos que se reconducen básicamente a los tres sucesivos juicios de «idoneidad», «necesidad» y «proporcionalidad» requeridos por el TC y a los que nos hemos referido en el FD Quinto [5.b)] (…)".

más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad, 2º) y si la medida en sí es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto, 3º). Este análisis en el marco de la protección de datos debe articularse en general bajo los principios de privacidad por defecto y en el diseño, bajo el principio de responsabilidad proactiva, la adopción del registro de actividades de tratamiento y de garantías y medidas de seguridad adecuadas. Asimismo, en muchos casos, bajo la obligatoriedad del análisis de impacto (tratamientos automatizados masivos, biométricos, geolocalización, etc.).

Serán elementos de juicio importante los datos que se captan, su número, naturaleza e impacto, la adopción de políticas negociadas con los trabajadores y posibles compensaciones establecidas al efecto, la capacidad real de ejercer los derechos por los afectados.

Cada caso debe ser analizado de modo particular. No obstante, la percepción inicial de la que partir es que el control tecnológico de la actividad del trabajador no habrá de implicar una captación masiva de datos y especialmente si lo que se pretende es la maximización de la eficiencia del trabajador. Habrá de analizarse toda alternativa posible.

La AEPD ha tenido en cuenta el principio de proporcionalidad en diversos informes y resoluciones para el ámbito laboral (por ejemplo, AEPD 2015 o AEPD 2018 b). Y lo ha recordado recientemente en su Guía (AEPD 2021 a, p 8 y p. 26)[14], especialmente con relación a la implantación de medidas de control laboral, que exige realizar el test de proporcionalidad (AEPD 2021 a, pp. 50 y ss.). El control de la proporcionalidad será más exigente y mayores las garantías exigibles en ámbitos particulares, como decisiones y perfilado automatizados, la grabación de sonidos, geolocalización o datos biométricos y reconocimiento facial.

Por ejemplo, la SAN 136/2019 de 6 de febrero, Sala de lo Social, determina que un sistema de geolocalización que había implementado la empresa no supera el juicio de proporcionalidad[15].

[14] Ver, p. 8 vinculada a la base de legitimación del tratamiento o respecto del desarrollo de la relación laboral p. 26.

[15] https://www.poderjudicial.es/search/contenidos.action?action=accessToPDF&publicinterface=true&tab=AN&reference=8ed60e51766c4e3e&encode=true&optimize=20190219&databasematch=AN

Garantías concretas en controles ocultos, fuera del trabajo, geolocalización, datos biométricos, decisiones automatizadas y captación de audio

Los controles tecnológicos ocultos al trabajador sólo caben excepcionalmente. Los controles ocultos y no informados por el empresario al trabajador son en principio contrarios a las exigencias de la buena fe y a los deberes de información y transparencia. No hay en la legislación expresamente una excepción del derecho de información del control laboral. El TEDH ha sido especialmente riguroso. En STEDH Köpke v. Alemania 5 de octubre de 2010, se admitió una medida de vigilancia porque había indicios para emprenderla y fue limitada en el tiempo (dos semanas) y la medida solo había apuntado a dos empleados. La STEDH 17 de octubre de 2019 de Gran Sala en el caso español de López Ribalda la grabación y control oculto de unos de cajas de un supermercado se trataba de una zona abierta al público y de libre acceso y no podía considerarse naturaleza privada la actividad en una caja. El tema, en todo caso es bien conflictivo y con jurisprudencia oscilante.

Tolerancia del uso de instrumentos tecnológicos fuera del trabajo y la prohibición de su control laboral. El empleador habrá de fijar concretamente e informar a los trabajadores de los periodos en los que los dispositivos, en su caso, pueden usarse con fines privados a los efectos de no acceder a la información de los mismos (art. 87.3º). como se ha adelantado, si no hay tolerancia en el uso privado de los medios del empresario, éste sí que puede controlar su uso (STS 6 de octubre de 2011). La STSJ de Asturias de 27 de Diciembre de 2017 (FJ 5º) [16] establece la obligación de la empresa de contar con un procedimiento que le permita desactivar el sistema de posicionamiento global instalado de forma que no capte datos una vez finalizada la relación laboral.

Especiales garantías cuando el control tecnológico también implique la geolocalización. La sensorización y control del trabajador en muchas ocasiones integra datos de geolocalización. Además de las reglas y pautas generales indicadas, la geolocalización cuenta con algunas especificaciones y regulación particular a tener en cuenta. En el ámbito de la geolocalización el Dictamen 13/2011 del Grupo de Trabajo del artículo 29, del Grupo del artículo 29 sobre interés legítimo (G29 2011), señala algunos requisitos para la geolocalización:

16 http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8283089&links=%222241%2F2017%22&optimize=20180208&publicinterface=true

-“deben investigar si es una necesidad demostrable controlar la localización exacta de los empleados con un fin legítimo y sopesar dicha necesidad con los derechos y libertades fundamentales de los trabajadores.”

-“El empresario debe siempre buscar los medios menos intrusivos, evitar un seguimiento continuo y, por ejemplo, elegir un sistema que envíe una alerta cuando un empleado cruce una frontera virtual preestablecida.”

-“El empleado deberá poder desactivar cualquier dispositivo de vigilancia fuera de las horas de trabajo y deberá instruírsele sobre cómo hacerlo. “

-“Los dispositivos de seguimiento de vehículos no son dispositivos para la localización de empleados ya que su función es hacer un seguimiento o vigilar la ubicación de los vehículos en que estén instalados. Los empresarios no deben considerarlos como dispositivos para seguir o supervisar el comportamiento o el paradero de los conductores o de otro tipo de personal, por ejemplo, mediante el envío de alertas relacionadas con la velocidad del vehículo”.

La AEPD ha señalado que “el tratamiento de los datos de localización fuera del tiempo de la prestación laboral, resulta excesivo en relación a la finalidad perseguida, por lo que vulneraría el principio de proporcionalidad y resultaría contrario a la LOPD” (AEPD 2009). Cabe recordar que la Agencia ha sancionado por no haber cumplido con el deber de informar sobre la instalación de geolocalizadores en vehículos (procedimientos AP/00032/2013 y AP/00040/2012) al no haber informado previamente a los agentes que utilizan estos vehículos de la instalación de estos dispositivos. En su Guía de 2021 deja relativamente claro que si la finalidad de la geolocalización es el registro horario los datos no podrán utilizarse para verificar la ubicación. También como ejemplo, señala que la geolocalización puede justificarse en el transporte de mercancías para conocer el vehículo dónde esta, pero sólo si la prestación del trabajador lo hace necesario. Y se subraya el criterio de que “La geolocalización puede no tener como objeto a la persona trabajadora, sino el de ser herramientas propiedad del empleador, como vehículos o dispositivos móviles.”[17] De este modo sí que es lícita la geolocalización. Se advierte, no obstante, que no cabrá monitorear u observar continuamente al trabajador. Y se señala que si la geolocalización implica el control del trabajador, hay que realizar una evaluación de impacto, debe tener un fin específico y no el general del control al trabajador. También

[17] AEPD, 2021 a, p. 53 y ss. Apartado 5. Cita de la p. 54.

se recuerda (AEPD, 2021 a p. 56) que no es lícito imponer al trabjador que facilite su propio teléfono móvil para facilitar datos de geolocalización.

Por cuanto a la información a facilitar, la STSJ Cataluña 5 de marzo de 2012[18] admitió una mera información general, esencialmente las advertencias expresas de adoptar medidas de control después de conocer incumplimientos del trabajador, asimismo analiza de modo concreto la proporcionalidad del control establecido. Sin embargo, la STSJ Madrid, Sección nº 1 de lo Social, de 21 de Marzo de 2014[19] consideró la nulidad por falta de información y de proporcionalidad. El trabajador sí que fue informado de la implantación de "GPS avalado por el Cuerpo Nacional de Policía", vinculado al uso exclusivo laboral del vehículo. Se atacó especialmente la falta de proporcionalidad del seguimiento continuo del trabajador, también en la línea de la STSJ País Vasco de 10 de mayo de 2011 (recurso nº 644/11). Y la ya referida STSJ de Asturias de 27 de diciembre de 2017 (FJ 5º) establece la obligación de la empresa de contar con un procedimiento que le permita desactivar el sistema de posicionamiento global instalado de forma que no capte datos una vez finalizada la relación laboral.

Prohibición general del control laboral a partir de datos biométricos. La sensorización empresarial fácilmente puede suponer el tratamiento de datos biométricos y en su caso de salud. Especialmente los lectores biométricos para el control de acceso y la captación de datos y telemetrías bien pueden suponer una captación de características físicas o fisiológicas, como sobre todo por las pautas conductuales del trabajador. Ello también sucede en muy buena medida cuando se introduzcan sistemas de reconocimiento facial.

Pues bien, en principio, hay que excluir el tratamiento de datos biométricos por los empleadores y menos de modo masivo, continuado y con carácter ordinario.

Como punto de partida, cuando la finalidad de estos tratamientos es la identificación única de la persona se considerarán datos biométricos y debe aplicarse el régimen más riguroso del artículo 9 RGPD por cuanto se trata de datos especialmente protegidos[20]. No

[18] http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=6365192&links=&optimize=20120516&publicinterface=true

[19] http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7018675&links=%221952%2F2013%22&optimize=20140410&publicinterface=true

[20] *"Artículo 4.14 del RGPD: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que*

obstante, también parece que la captación y tratamiento masivo de datos del trabajador para el control y evaluación de la actividad a partir de elementos físicos, fisiológicos y pautas conductuales debe someterse a este régimen más riguroso.

No se trata de una cuestión preclara, pero es de especial interés al respecto el extenso Informe AEPD (2020 b). El mismo es relativo a mecanismos de reconocimiento biométrico de alumnos en el control de exámenes. Lo que interesa para el contexto laboral es que la AEPD aplica el régimen del artículo 9 RGPD siendo que la finalidad no sólo -o no lo es claramente- la identificación. Además tiene en cuenta elementos que bien pueden darse en el control laboral tecnológico con IOT como eran las pulsaciones en el teclado, así como otros elementos de impacto como el acceso al micrófono para la grabación de sonidos, grabación del sonido y el hecho de que se trataba de un tratamiento no sólo en un momento determinado sino que se realiza de manera continuada. Se puede considerar que habrá que aplicar el artículo 9 RGPD para el contexto laboral. Y no hay una regulación que expresamente permita el tratamiento de datos biométricos en el contexto laboral.

Como excepción, y no como regla general, puede decirse que sólo ha habido cierta tolerancia de la AEPD por cuanto el tratamiento de datos biométricos se conecte al control horario obligatorio que tienen que efectuar los empresarios[21]. La obligación se establece por el Real Decreto-ley 8/2019, de 8 de marzo, pero no se expresa que ello habilite a un tratamiento de datos biométricos. Pues bien, en todo caso, esta tolerancia de la AEPD frente a la falta de regulación, no puede pensarse que se extiende a otros ámbitos de control empresarial y la regulación actual no contempla expresamente estos controles.

Es más, la Autoridad Catalana de Protección de Datos (2018) señala que no es suficiente el artículo 20.3º ET como base legitimadora para el tratamiento de datos biométricos, dado que la norma no expresa la posibilidad de utilizar categorías especiales de datos o, en concreto, de datos biométricos, con esta finalidad.

---

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

[21] Así, la AEPD se pronunció al respecto en la sesión abierta celebrada en 2018, al indicar que el tratamiento de la huella dactilar para el control de acceso por los trabajadores podría considerarse una medida de control amparada en el artículo 20 del Estatuto de los Trabajadores, por lo que no resultaría necesario recabar el consentimiento del interesado. En su encuentro sobre registro horario del 23 de Abril, en la sede de la Confederación Española de Organizaciones Empresariales vino a admitir la posibilidad de uso de identificadores biométricos.

La más reciente Guía de 2021 insiste en la importancia de distinguir el uso de datos biométricos como categoría especial de datos sólo cuando se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física. Es decir, hay que insistir que no son datos especialmente protegidos en el caso de verificación/autenticación biométrica (uno-a-uno). (AEPD 2021 a) p. 30 y 31). Y sobre estas bases señala una serie de recomendaciones más técnicas: uso de datos almacenados como plantilles cifradas bajo control del propio trabajador (tarjetas en la lectura de la huella, supresión automática de datos brutos una vez calculada la plantilla o cifrado).

De igual modo, para todo tipo de tratamiento biométrico, sensible o no recuerda los deberes de información, que los sistemas estén fabricados desde el diseño, también que se almacenen como plantillas biométricas, dispositivos personales y no almacenamientos centralizados, cifrado, diseño que se pueda revocar el vínculo de identidad, no formatos que interconecten bases de datos, supresión determinada, etc. (AEPD 2021 a) p. 32). Asímismo se recuerda que es precisa la evaluación de impacto.

Garantías especiales respecto del control y decisiones automatizadas laborales. En muy buena medida, en el ecosistema IOT de control laboral y en su caso con IA, se emplean tecnologías de perfilado y decisiones automatizadas que, además, afectarán significativamente al trabajador . Asimismo, hay que tener presente que pese a la apariencia humana de las decisiones, en muchos ecosistemas tecnológicos y empresariales las decisiones adoptadas a partir de la captación y tratamiento masivo de datos del trabajador serán esencialmente automatizadas (especialmente G29, 2018)[22]. Es por ello que en muchos casos serán aplicables las singulares garantías del artículo 22 RGPD, como es el derecho a la explicación así como a la impugnación de la decisión y su revisión humana (Palma 2021). Y ya contamos con un importante acervo con relación al tratamiento de datos con IA gracias a la AEPD (2020 c) y 2021 b).

En razón de este precepto esencialmente habrá que informar al trabajador que queda bajo un proceso automatizado de toma de decisiones, facilitarle la lógica del algoritmo, lo cual incluirá informarle sobre los parámetros evaluados por el algoritmo y la

[22] Cabe recordar su p. 21, la empresa (o responsable de datos) no puede evitar las restricciones del art. 22 fabricando artificialmente una intervención humana. Para que se entienda que existe intervención humana es necesario que el responsable analice toda la información relevante y lo haga un sujeto con autoridad y competencia para modificar la decisión. El Grupo del artículo 29 hace especial hincapié en que la revisión de la decisión por parte de un humano debe ser significativa, de lo contrario, la intervención humana no podrá entenderse excluyente de la protección del art. 22 RGPD.

ponderación de dichos parámetros. Asimismo habrá de informar al trabajador de las consecuencias concretas de la decisión. La AEPD recuerda la necesidad de facilitar cauces para la intervención humana en la decisión sobre el trabajador, y que esta intervención en modo alguno sea un "gesto simbólico" (AEPD 2021 a p. 24).

Garantías respecto de la captación de audio del trabajador y su posible extensión. La regulación contempla otras garantías del control laboral. Así:

-Se da la prohibición de grabaciones de vídeo o audio "en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos." (art. 89. 2º).

-La grabación de sonidos sólo se puede realizar cuando "resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad" (art. 89. 2º). Y se fijan garantías de supresión (art. 22.3º).

De estas garantías fácilmente se deriva que será más difícil para el empresario integrar en sus sistemas de control y seguimiento de la actividad empresarial el tratamiento de datos de audio. Y cuando se traten datos e información más próxima a la intimidad del trabajador, como la evaluación de pautas de trabajo, historial de navegación, etc. bien puede pensarse que se requerirá una justificación más específica de dicha necesidad, además de la inexistencia de otros mecanismos para lograr la finalidad de control perseguida.

Bibliografía empleada

AEPD:

- 2009. *Informe 0090/2009*, https://www.aepd.es/informes/historicos/2009-0090.pdf

- (s.f.). *Preguntas frecuentes "Tratamiento de datos en el ámbito laboral"*, https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/listadoFAQ.jsf?categoria=13

- 2018 a. Ficha *Prácticas de videovigilancia: VI. Cámaras para el control empresarial*, https://www.aepd.es/sites/default/files/2019-09/ficha-videovigilancia-control-empresarial.pdf

- 2018 b, *Resolución R/00900/2018*, https://www.aepd.es/resoluciones/PS-00002-2018_ORI.pdf

AEPD, 2015. *Informe 0065/2015*, https://www.aepd.es/media/informes-historicos/2015-0065_Control-de-acceso-al-comedor-por-huella-digital.pdf

- 2019. *Jornada sobre protección de datos y relaciones laborales el 23 de abril de 2019,* https://www.aepd.es/es/la-agencia/agenda/jornada-sobre-proteccion-de-datos-y-relaciones-laborales acceso a la sesión en https://www.youtube.com/watch?v=tZUayrmKzr0&feature=youtu.be

- 2020 b. *Informe Gabinete Jurídico 36/2020*, https://www.aepd.es/es/documento/2020-0036.pdf

- 2020 c. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción.*

- 2021 a. *La protección de datos en las relaciones laborales*, 18 de mayo, https://www.aepd.es/es/node/46369

- 2021 b. *Requisitos para Auditorías de Tratamientos que incluyan IA*, 2021.

- 2020 c. *Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo,* https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteger-datos-teletrabajo.pdf

Autoridad Catalana de Protección de Datos, 2018. *CNS 63/2018 Dictamen en relación con la consulta formulada por un colegio profesional sobre la utilización de sistemas de control basados en la huella dactilar*, https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2018/Documents/es_cns_2018_063.pdf

CASTILLO PARRILLA, José Antonio, 2020. "Sentencia del Tribunal Ordinario de Bolonia de 31 de diciembre de 2020 (Caso Deliveroo) ¿Discriminación algorítmica o discriminación a través de un algoritmo?", en *Derecho Digital e Innovación. Digital Law and Innovation Review,* , Nº. 7 (octubre-diciembre).

COMISIONES OBRERAS (s.f). *Límites al control empresarial y capacidad de intervención de la RLT ante el tratamiento de datos personales de los trabajadores y trabajadoras*. Acceso en http://industria.ccoo.es/ba4d560b5a9fef3ca26cee3d6f6063ce000060.pdf

COMISIONES OBRERAS (s.f). Sobre registro de jornada, http://www.ccoo.es/e5c4be55ac54bccf9eea9dbfa7f49901000001.pdf

COTINO HUESO, Lorenzo y otros, 2021. "Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (Artificial Intelligence Act)", en *Diario La Ley*, 2 de julio , Wolters Kluwer. Acceso completo en https://links.uv.es/2FK3xc4

GOBIERNO DE ESPAÑA, 2021. *Carta de Derechos digitales*, julio de 2021. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29:

-2002. *Opinion on the processing of personal data in the employment context* 5062/01/EN/Final, WP 48, 13 de septiembre. Acceso en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

- 2011. *Dictamen 13/2011 del Grupo de Trabajo del artículo 29*, sobre interés legítimo, https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf

- 2018 *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, 3 de octubre de 2017, versión final 6 de febrero de 2018, Doc WP251rev.01

MINISTERIO DE TRABAJO, MIGRACIONES Y SEGURIDAD SOCIAL y AEPD (2019), *Protocolo general de actuación para la atención a personas cuyos datos se hayan difundido ilegítimamente, en el entorno laboral, especialmente en caso de imágenes, vídeos, o audios con datos sensibles* , de 24 de septiembre de 2019, https://www.aepd.es/media/protocolos/protocolo-aepd-mitramiss.pdf

OIT, 1997. *Código de buenas prácticas para la protección de los datos personales del trabajador de la OIT*, https://www.dropbox.com/s/v1h8koxd3qhlj5p/guiaAEPDlaboral.pdf?dl=0

PALMA ORTIGOSA, Adrián, 2021. *Régimen jurídico de la toma de decisiones automatizadas y el uso de sistemas de inteligencia artificial en el marco del derecho a la protección de datos personales*, Tesis doctoral Universidad de Valencia.

SOUPPAYA Murugiah y SCARFONE Karen, 2020. *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, NIST Special Publication 800-46, Revision 2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf y http://dx.doi.org/10.6028/NIST.SP.800-46r2

TODOLÍ SIGNES, Adrián:

-2021. "Nuevos derechos digitales incorporados al estatuto de los trabajadores y Estatuto Básico del Empleado Público: más dudas que novedades", en *Comentario al rgpd y a la LOPDGDD*, Antonio TRONCOSO REIGADA (dir.), Civitas, Vol. 2, págs. 4107-4125

-2021. “Derecho a la intimidad y a la desconexión digital en el trabajo”, en RODRÍGUEZ-PIÑERO, Miguel y TODOLÍ, Adrián (coords.).*Trabajo a distancia y teletrabajo : análisis del marco normativo vigente*, págs. 229-245.

-2022.“La reputación digital de los trabajadores: perfiles y decisiones automatizadas”, en COTINO HUESO, Lorenzo (editor), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Thompson-Reuters Aranzadi, FIADI (Federación Iberoamericana de Asociaciones de Derecho e Informática), Cizur,.

-2022. “Derechos en el ámbito laboral”, en COTINO HUESO, Lorenzo (editor), *La Carta de Derechos Digitales*, Tirant Lo Blanch, Valencia,.

UGT, 2018. *Nuevas tecnologías en el control de los trabajadores y el derecho a la intimidad del trabajador*, diciembre http://www.ugt.cat/nuevas-tecnologias-en-el-control-de-los-trabajadores-y-el-derecho-a-la-intimidad-del-trabajador/