LAS FACULTADES DE CONTROL DE DATOS BIOMÉTRICOS DEL TRABAJADOR

MIGUEL RODRÍGUEZ-PIÑERO ROYO
Catedrático de Derecho del Trabajo y de la Seguridad Social
Universidad de Sevilla*

EXTRACTO **Palabras Clave:** Derecho del Trabajo digital, controles biométricos, privacidad, poderes empresariales, relaciones laborales

Los controles biométricos son un elemento común en los centros de trabajo del siglo XXI. Esta tecnología es fiable, eficiente y económica; por ello se han hecho ubicuos en las entidades empleadoras públicas y privadas.
Sin embargo, su utilización plantea la preocupación por la posibilidad de violaciones de los derechos de los trabajadores, como la privacidad y la intimidad. Este trabajo analizará el marco normativo en vigor para la utilización de estos controles. Su objetivo es poner de manifiesto las principales características de esta regulación, con especial atención en los derechos y obligaciones de trabajadores y empresarios.
En particular se prestará atención al papel de la negociación colectiva en la construcción de una regulación adecuada de los controles biométricos.
El presente trabajo parte de dos hipótesis. La primera es que, a pesar de su uso generalizado en los centros de trabajo contemporáneos, se conocen poco sus implicaciones legales. La segunda es que estos controles expresan las contradicciones esenciales que está creando la construcción de un Derecho del Trabajo digital, debido a la interacción de dos áreas del ordenamiento jurídico que muestran profundas diferencias entre ellas.

ABSTRACT **Key Words:** Digital Labour Law, biometric controls, privacy, employers' prerogatives, labour relations

Biometric controls are common in the XXI Century working places. This technology has become reliable, efficient and cheap; consequently, these controls have become ubiquitous in both private and public employers.
Nevertheless, this use raises concerns about potential violations of employees' rights, such as privacy and human dignity. This paper will analyze the normative framework in force regulating the use of these controls. Its purpose is to highlight the main features of this regulation, focusing on both employers' and employees' rights and obligations.
In particular, some attention will be paid to the role of collective bargaining in the construction of an adequate regulation of biometric controls.
There are two main hypothesis. The first one is that, notwithstanding its widespread use in contemporary working places, there is little knowledge about its legal implication. The second is that these controls expresses the essential contradictions that the construction of a Digital Labour Law is creating, due to the interaction of two areas of the legal system, which show profound differences among them.

* Senior Counsellor, PwC, mrodriguez7@us.es. ORCID 0000-0001-7926-6175. Grupo de Investigación PAIDI SEJ-322; Es un resultado científico de los proyectos de investigación "Nuevas dinámicas y riesgos sociales en el mercado de trabajo del siglo XXI: desigualdad, precariedad y exclusión social", de la convocatoria 2018 de "Proyectos de I+D Retos Investigación", con referencia RTI2018-098794-B-C31; y FEDER18-1264479 "Nuevas Causas y Perfiles de Discriminación e Instrumentos para la Tutela Antidiscriminatoria en el Nuevo Contexto Tecnológico Social".

 Recepción de original: 21.10.2019. Aceptación: 01.11.2019

ÍNDICE

1. PRESENTACIÓN

Utilizar partes del propio cuerpo para identificarse es, en realidad, muy antiguo. Seguramente el primer control biométrico de la historia fue el guarda de la fábrica que identificaba a los trabajadores en la puerta simplemente mirándolos y reconociéndolos. Hoy los mecanismos de verificación automatizada a través de la identificación de rasgos biométricos se han generalizado en las empresas, y son varias, a mi juicio, las razones que lo explican.

Se ha producido, en primer lugar, un progreso técnico, en tres direcciones paralelas: mejora de los instrumentos de verificación; abaratamiento de éstos[1]; y mayor velocidad en la transmisión y gestión de la información. Es lo mismo que ha ocurrido con otros sistemas de control[2].

La tendencia hacia el control en las sociedades contemporáneas explica igualmente su extensión. En las empresas se quiere tener conocimiento completo de cuanto ocurre en la organización, de cómo se utilizan sus recursos y de lo que sus empleados hacen. Se requieren mecanismos que lo hagan posible, sin suponer interferencias en su funcionamiento ordinario. En algunas ocasiones el control empresarial responde no a objetivos de supervisión, sino de verificación del cumplimiento de la normativa aplicable, en beneficio de otros sujetos; tal es el caso del registro de jornada, del que también me ocuparé en este trabajo.

[1] Como ha señalado el GT-29 en su Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, "*en la actualidad, pueden aplicarse tecnologías que permiten el tratamiento de datos en el trabajo con un coste muy inferior al de hace varios años, mientras que la capacidad de tratamiento de datos personales de estas tecnologías ha aumentado exponencialmente*". Ya en el año 2012, en su Opinión 3/2012, señalaba que "*in the past the use of this technology was expensive and as a result of this economic constraint the impact on individuals' data protection rights was limited. In recent years, this has changed dramatically. DNA analysis has become faster and affordable for almost everyone. The technological progress has made storage space and computing power cheaper; this made online picture albums and social networks with billions of photographs possible. Fingerprint readers and video surveillance devices have become an inexpensive gadget. The development of these technologies has contributed to make many operations more convenient, has contributed to solve many crimes and made access control systems more reliable, but it has also introduced new threats to fundamental rights*".

[2] No podemos olvidar factores como el precio, la disponibilidad, el tamaño de los aparatos y su manejabilidad, a veces olvidados por centrarnos exclusivamente en la aparición de nueva tecnología. Mucha de la que vamos a analizar aquí no es, en rigor, nueva. Sí lo es su ubicuidad, consecuencia de estos otros elementos.

La obsesión por la seguridad en las primeras décadas del siglo XXI es también un elemento a considerar, especialmente cuando se ve acompañada de la masificación de los lugares que se quieren vigilar. Estos controles son una forma rápida de gestionar el paso de grandes volúmenes de personas, de una manera rápida y segura, en lugares con mucha presencia de personas como aeropuertos, estaciones, centros educativos y, en lo que a nosotros interesa, centros de trabajo[3].

Seguramente el factor más significativo es la eficacia a la que se ha llegado con **éstos**, algunos de los cuales acreditan rapidez y acierto a precios accesibles, lo que explica su ubicuidad en los centros de trabajo y en otros lugares. Sorprende, por ello, la escasa atención que sus usuarios están prestando a la derivada legal en su implantación, particularmente cuando, como veremos, pueden generar consecuencias serias para las empresas.

En este estudio intentaré presentar y explicar la situación normativa en nuestro país, a partir de los materiales regulatorios que resultan de aplicación. Mientras lo hago, realizaré alguna reflexión sobre el Derecho del Trabajo digital en general, que engloba a ésta y otras figuras dentro de las empresas. Se trabajará fundamentalmente con los materiales normativos disponibles, en sentido amplio, aunque en algún momento se estudie algún aspecto de la realidad sobre la que la norma debe operar.

La hipótesis de partida es que existe en España un marcado contraste entre el conocimiento técnico de estos mecanismos de control y de sus implicaciones, de un lado, y el marco normativo que hemos sido capaz de articular para ordenarlo, por otro. Este desfase es común a otras facetas de ese fenómeno, como se puede comprobar en las distintas contribuciones a este monográfico; en ésta en particular resulta especialmente marcado, por lo que se verá. Hace falta, pues, desarrollar esta normativa, y en esta tarea tiene un papel fundamental la negociación colectiva.

Mi segunda hipótesis es que ésta es una de las áreas en las que más se notan las contradicciones internas del Derecho digital del trabajo, en la forma en que se está construyendo en nuestro país. Este Derecho es la confluencia de dos ramas preexistentes, el Derecho de la Protección de Datos y el Derecho del Trabajo, cada una con sus propios principios y objetivos, sin que hasta el momento haya podido lograrse un equilibrio adecuado entre los de cada una.

2. DELIMITACIÓN DE LOS CONTROLES BIOMÉTRICOS

Una temprana definición de controles biométricos la proporcionó el Grupo de Trabajo del artículo 29 en su Working Document 80, de 2003: "*los sistemas biométricos son aplicaciones de tecnologías biométricas que permiten la iden-*

[3] Llegando al extremo, son varios los Estados que se están planteado generalizar sistemas de reconocimiento facial en sus ciudades, justificadas por razones de seguridad pero generando grandes riesgos de hipercontrol sobre la ciudadanía.

tificación y/o la autenticación/verificación automática de una persona". En su Opinión 4/2007 consideraba como tales a las "*las propiedades biol*ógicas, l*os aspectos conductuales, las características fisiológicas, rasgos vitales o acciones repetibles en las que estos caracteres y/o conductas son a la vez únicas para ese individuo y medibles, incluso si los patrones usados en la práctica para medirlos técnicamente tienen cierto grado de probabilidad*".

El RGPD define los datos biométricos como los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos (artículo 4.14 RGPD).

Por su parte, la AEPD utiliza una fórmula en sus documentos para delimitarlos, como aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión.

Los datos biométricos tienen unas características comunes, que son los que los hacen útiles a efectos de autenticación o identificación: son universales (todas las personas los tienen); son únicos (deben ser capaces de distinguir a una persona de otra); y son permanentes (el dato tiene una presencia continua en el tiempo para cada persona).

Se dirigen principalmente a verificar la identidad de una persona física, pero pueden servir también a identificarla de manera unívoca. Las técnicas de control biométrico son muy variadas, pues pueden utilizar distintas características de la persona[4]. Aunque suelen identificarse con el control de sus rasgos físicos, la realidad es muy amplia, y en la práctica vamos a encontrar un amplio abanico de sistemas de vigilancia, clasificados en dos grandes grupos.

Por un lado, están los datos llamados "fisiológicos", que se refieren a características físicas y fisiológicas de la persona. Los datos fisiológicos más frecuentemente utilizados son la huella dactilar, el iris, la geometría de la mano, la retina, los vasos sanguíneos en determinadas partes del cuerpo, la voz, el sudor, las orejas y el ADN. Por otro, tenemos los datos relacionados con el comportamiento de la persona, con actuaciones o con la forma en que realizan ciertas conductas. Entre éstos destacan la escritura, el ritmo cardiaco, el ritmo respiratorio, la firma, la utilización de un teclado, la forma de conducir, la forma de andar o de moverse, y la marcha. El GT-29 identifica un tercer tipo de controles biométricos, al que califica como "emergente", que serían los psicológicos, la forma de reaccionar de la persona ciertas situaciones o pruebas, que pueden dar lugar a un perfil psicológico de ésta.

Es fundamental distinguir, cuando se trata de biometría, entre "controles" y

[4] Una descripción muy útil de estas técnicas en el ya citado GT-29, "*Working document on biometrics*", 2003 (WP 80), pg.3.

"datos", porque nos vamos a encontrar con ambos en el ámbito laboral. Control es el artilugio que permite realizar autenticaciones o identificaciones a partir de una característica biométrica de la persona, de las muchas posibles; sería el lector de huellas dactilares que encontramos en cada vez más empresas. Dato es la información que se obtiene a partir de estos controles, y que permite a su vez conseguir otras de la persona; sería la propia huella[5].

El RGPD los considera también como un identificador, una información a través de la cual puede determinarse la identidad de una persona. Según el artículo 4.1 RGPD, "*se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo uno o varios elementos propios de la identidad física (…) de dicha persona*". El mismo RGPD afirma en su considerando 51 que *"únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física"*.

3. LOS CONTROLES BIOMÉTRICOS EN LAS RELACIONES LABORALES

Nos encontramos ante un control particularmente intrusivo, tanto en los datos que recoge como en la forma de obtenerlos. En muchos casos va a exigir contacto físico; puede dar acceso a datos especialmente sensibles. Este dato es fundamental, porque es uno que se tiene en cuenta a la hora de valorar la legitimidad de su uso. Así lo ha indicado entre nosotros la Agencia Española de Protección de Datos (en adelante AEPD), que en muchos casos no ha aceptado su validez por entender que existen alternativas menos lesivas de la intimidad para lograr unos mismos fines. El grado de intrusión varía según el mecanismo de control y el dato tomado como referencia: no es lo mismo verificar el rostro de una persona (algo que se hace a distancia) que su huella digital (que exige un contacto físico con el aparato)[6], o que su ADN o grupo sanguíneo (que imponen la extracción de muestras biológicas). También depende de los datos concretos que se tomen como referencia: no es igual verificar el rostro, público y notorio, que el ADN o el ritmo cardiaco, ocultos y que pueden decirnos cosas sobre la salud o el origen genético de la persona[7].

[5] Recordemos que el artículo 4.1 RGPD define los datos personales como "*toda información sobre una persona física identificada o identificable*".

[6] Aunque para algunos este tipo de control resulta bastante intrusivo. Así, en la sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Andalucía de Sevilla, Sala de lo Social de 11 de febrero de 2016 leemos que un Comité de Empresa mostró su "*disconformidad con el sistema de control a través de un huella digital por entender que implica un sacrificio para el trabajador desprenderse de su huella digital*".

[7] El Tribunal Constitucional, en su Auto 57/2007, de 26 de febrero, se base en este impacto variable para concluir la legitimidad del sistema de control empresarial: en sus palabras, "*en el sistema de*

Se suelen utilizar para autenticar la identidad del trabajador, aunque resulta igualmente posible su uso para identificarlo. Este es su papel principal en las empresas, como mecanismo de vigilancia de la actividad de estos empleados. El problema es que no sólo cumplen esta función en las organizaciones productivas, sino que también son instrumentales a otros fines legítimos: seguridad en las sedes físicas, impidiendo el acceso de personas no autorizadas; prevención de riesgos laborales; detección del consumo de productos que puedan generar peligro en el centro de trabajo; o el cumplimiento de los derechos de los trabajadores, como el respeto a la jornada pactada. Su polivalencia supone también una fuente de contradicciones que dificulta una respuesta jurídica adecuada.

En cuanto mecanismo de control suele ser explícito, visible y controlable. Pero cabe también que se articule de manera oculta, como puede ocurrir cuando se combina con cámaras de vigilancia, cuando se controla el uso de un teclado, cuando se instala una aplicación en un ordenador o teléfono, cuando se vincula con un aparato ponible ("wearable")[8]… El nivel de riesgo de vulneración del derecho a la intimidad que genera puede también variar por ello[9].

Se trata de una forma de control en la que es frecuente una coincidencia con otros mecanismos de vigilancia, lo que provoca una interacción con los problemas particulares de cada uno de éstos[10]. Pensemos, por ejemplo, en los controles biométricos a través de wearables, que pueden operar fuera de la jornada de trabajo[11]; en los que se insertan en terminales telefónicos, con el mismo efecto y suponiendo además un control de dispositivos electrónicos; en los supuestos de reconocimiento

control que el recurrente impugna los datos biométricos de su mano no están protegidos por el derecho a la intimidad corporal, pues no existe colisión con la noción socialmente arraigada de recato en lo que respecta a esa parte del cuerpo, ni por el más extenso derecho a la intimidad personal, puesto que aquéllos no desvelan un ámbito reservado del recurrente".

[8] Utilizo la expresión "ponible" como traducción al castellano de "wearable". No es la única que se maneja, y en algunos casos se habla de "vestible". Ni siquiera es una expresión adecuada, porque el Diccionario de la Real Academia de la Lengua le da un significado distinto: "*Dicho de una prenda de vestir: Que se puede poner en distintas ocasiones o que combina bien con otras prendas*". Lo que me ha llevado a recurrir a ella, aparte de motivos sentimentales por ser una palabra muy de madre, es que el GT-29 la utiliza en la versión en castellano de sus documentos.

[9] El GT-29 ha indicado también en su Dictamen 2/2017 que "*las nuevas formas de tratamiento, como las relativas a los datos personales sobre el uso de servicios en línea y/o los datos de localización de un dispositivo inteligente, son mucho menos visibles para los trabajadores que otros tipos más tradicionales, como las evidentes cámaras de televisión de circuito cerrado. Esto plantea interrogantes sobre hasta qué punto los trabajadores son conscientes de estas tecnologías, ya que los empresarios podrían llevar a cabo ilegalmente este tratamiento sin informarles previamente*".

[10] INSTITUTO NACIONAL DE CIBERSEGURIDAD, "*Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario*"; accesible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf; visitada el 1 de septiembre de 2019; pg.13.

[11] También el GT-29 se ha hecho eco de este riesgo, indicando en su informa antes citado que "*los límites entre el hogar y el lugar de trabajo se han ido difuminando cada vez más. Por ejemplo, cuando los trabajadores trabajan a distancia (desde su domicilio) o mientras viajan por motivos profesionales, puede llevarse a cabo un seguimiento de las actividades realizadas fuera del entorno físico de trabajo, que puede incluir el control del individuo en un contexto privado*".

facial o conductual por medio de cámaras de vídeo… La complicación que se produce en estos casos es evidente.

De la misma manera, estos controles pueden implantarse mediante la utilización de aparatos propiedad del trabajador (como su teléfono móvil). Nos encontraríamos entonces ante un supuesto de "uso del propio equipo", lo que se conoce como "BYOD"[12], que también genera sus propias dudas, no sólo por cuestiones relacionadas con la propiedad del medio, el reparto de costes o la responsabilidad por su uso, sino también con la intromisión en la intimidad del trabajador, o la extensión del control fuera de la jornada o lugar de trabajo. Aunque pueda existir un interés legítimo del empleador en verificar los datos obtenidos mediante estos equipos, la posibilidad de acceder a datos personales no relacionados con el trabajo supone un importante riesgo para la privacidad de los trabajadores[13].

Las ventajas que suponen para las empresas son evidentes: seguridad, fiabilidad, celeridad en el control, comodidad (al hacer innecesarias tarjetas…). También lo son los riesgos. Para los trabajadores, la posibilidad de un control total por las empresas; la intrusión en sus espacios de privacidad; la disolución de fronteras entre lo laboral y lo personal; la posibilidad de construir perfiles con los datos obtenidos; el acceso a información personal sensible, directa o indirectamente; la pérdida de anonimato… Para las empresas, el mayor riesgo es la disponibilidad de una enorme cantidad de datos personales de sus trabajadores, datos sensibles además, que les imponen obligaciones estrictas en cuanto a su manejo, utilización, almacenamiento y comunicación. Obligaciones y sanciones muy elevadas en caso de incumplimiento, lo que debe llevar estos instrumentos al primer nivel de atención en las políticas de protección de datos y de cumplimiento normativo.

Su implantación obliga a las empresas a tomar decisiones arriesgadas: qué información se obtiene; cómo se obtiene; qué se hace con la información obtenida; qué papel se le a la persona cuyos datos se obtienen; y si existen medidas alternativas de control que supongan un menor nivel de intrusión.

[12] "BYOD" son las siglas de la expresión inglesa "bring your own device", algo así como "trae tu propio aparato".

[13] Según el GT-29, "*se puede considerar que el control de la localización y el tráfico de dichos dispositivos sirve al interés legítimo de proteger los datos personales de los que el empresario está a cargo como responsable del tratamiento; sin embargo, esto puede ser ilegal en lo que respecta al dispositivo personal de un trabajador, si dicho control también captura datos relativos a su vida privada y familiar. Con el fin de evitar la observación de información privada, deben adoptarse medidas adecuadas para distinguir entre el uso privado y profesional del dispositivo*".

4. LOS CONTROLES BIOMÉTRICOS Y EL DERECHO DEL TRABAJO DIGITAL

El Derecho del Trabajo digital, aún en construcción, presenta en España una estructura diferenciada por niveles de tratamiento. Esto es así porque la Ley Orgánica para la Protección de Datos Personales y Derechos Digitales ha recogido regulaciones especiales para ciertos aspectos de éste, pero ha dejado otros sin tratamiento. De este modo, en algunas materias, como pueden ser la geolocalización o el control de dispositivos electrónicos, se han introducido preceptos monográficos; este tratamiento ha creado la categoría general de "derechos digitales"; mientras que en otros, por el contrario, no se ha hecho así, no resultándole de aplicación sino la normativa general contenida en la Ley y el RGPD. Desde este punto de vista, los controles biométricos se ubican dentro de este segundo sector, al no haber sido tratados en el Título X de la LOPDGDD. Tampoco el artículo 20 bis ET, que se ocupa de los "*derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión*", lo incluye en su enumeración de estos derechos.

En esto se diferencia el Derecho del Trabajo digital del Derecho común de la protección de datos, que se organiza por niveles de tutela. Esta diferencia en la protección se articula mediante la utilización de la categoría de "datos especialmente sensibles", que se considera requieren un mayor grado de tutela jurídica.

Ocurre entonces que los datos biométricos se incluyen en el grupo de los que merecen mayor nivel de protección, pero a la vez el legislador laboral, cuando ha tenido que dar un tratamiento específico a algunos aspectos del control tecnológico de los trabajadores, no ha considerado necesario hacerlo[14]. Esto supone una primera paradoja en la regulación de esta figura, especialmente cuando el propio RGPD preveía la posibilidad de que los legisladores nacionales desarrollaran su regulación en este punto[15], aunque en modo alguno supone un problema de desprotección porque la normativa común ofrece un marco adecuado. Lo que ocurre es que en su ordenación prevalece la perspectiva de la protección de datos sobre la digital, lo que será clave para determinar su régimen jurídico[16].

[14] Un estudio del régimen jurídico de este control en E.M. Blázquez Agudo "Otros controles emergentes", en su libro "*Aplicación práctica de la protección de datos en las relaciones laborales*", Wolters Kluwer, Madrid, 2018. También R. Rojas Rosco & D. López Carballo, "El impacto del RGPD en el ámbito del control laboral y la era de la innovación", *Diario La Ley*, nº 4471, 2018

[15] Como se sabe, el artículo 9.4 del RGPD prevé que "*los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud"*.

[16] Un dato anecdótico para demostrar esta prevalencia de la perspectiva de protección de datos sobre la laboral: en la LOPDDGDD se utiliza la expresión tradicional en el Derecho del Trabajo español para referirse a las personas que trabajan, "trabajador". Sin embargo, en las leyes laborales del período en que se aprobó, incluyendo las últimas reformas del Estatuto de los Trabajadores, se usa la de "persona trabajadora", más correcta desde un punto de vista de lenguaje inclusivo. Esto pone de manifiesto, a mi juicio, que es un texto en el que el papel del Ministerio de Trabajo y de los expertos laborales ha sido reducido.

Junto a esta legislación existen otros materiales regulatorios que resultan muy útiles[17]. El conocido como "Grupo de Trabajo del Artículo 29" (GT-29), ha elaborado diversos documentos que se ocupan de cuestiones relacionadas con los controles biométricos. El más importante es el Working document on biometrics, de agosto de 2003 (WP 80). Junto a éstos, ha producido otros sobre la protección de datos en las relaciones de trabajo que también los tratan. Así, el Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral (WP48); el Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo (WP55) de 2002; y el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, de agosto de 2017 (WP 249)[18].

Aunque la Agencia Española de Protección de Datos ha elaborado una Guía de la protección de datos en las relaciones laborales, en ésta no se incluye expresamente esta cuestión[19]. Sí la ha afrontado en varios de sus informes, entre los que destacan el informe de 7 de septiembre de 2007, y sobre todo el Informe 0065/2015. En el ámbito autonómico son particularmente interesantes el Dictamen nº D17-005 de la Agencia Vasca de Protección de Datos, relativo a la implantación de un sistema de control de acceso por huella biometrica a instalaciones municipales; y los Dictámenes CNS 9/2009, CNS 22/2009, CNS 22/2011 y CNS 63/2018 de la Autoridad Catalana de Protección de Datos. Este último es particularmente útil, porque se dictó estando ya vigente el RGPD y la LOPDPGDD respecto de un supuesto laboral muy frecuente, la utilización del control de huellas en un lugar de trabajo. Por ello ha tenido bastante impacto en los medios jurídicos[20].

Mientras tanto, la principal fuente de tutela de los trabajadores, la autonomía colectiva, no está teniendo, al menos hasta ahora, un papel relevante. Son muy pocos los convenios colectivos que han incluido un tratamiento de estos sistemas en su articulado. Ni siquiera el artículo 91 LOPDPGDD, que como es sabido se ocupa de los "derechos digitales en la negociación colectiva" prevé expresamente su regulación en este tipo de acuerdos. En efecto, al señalar que "*los convenios colectivos podrán establecer garantías adicionales"*, específica que esto podrá

[17] Se me perdonará la expresión "materiales regulatorios", imprecisa y poco técnica. No pretendo ser original. Con ella quiero hacer referencia al conjunto de elementos con los que se construye la regulación de esta figura en España. Elementos que tienen distinto origen, naturaleza y grados de vinculabilidad; y que no siempre se corresponden con el concepto tradicional de fuente del Derecho, ni con el de norma jurídica.

[18] También se ha ocupado de esta cuestión en el "Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas)", de febrero de 2009 (WP 160).

[19] El Instituto Nacional de Ciberseguridad (INCIBE) ha elaborado también una guía sobre esta cuestión, "*Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario*"; accesible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf; visitada el 1 de septiembre de 2019.

[20] Un estudio monográfico en D. Gracia García, "El impacto de la privacidad en los sistemas biométricos de control de acceso y horario laboral tras el Dictamen 63/2018 de la Autoridad Catalana de Protección de Datos", *Diario La Ley*, nº 7492, 2018.

hacerse respecto "*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*". Esto es, para los que la ley llama "derechos digitales" en su vertiente laboral, y que son los que aparecen en los artículos 87 a 90. Derechos entre los que no se encuentran los afectados por la tecnología que nos ocupa.

Esto no quiere decir, es claro, que no puedan ser negociados. El RGPD así lo prevé, cuando en su Considerando 155 reconoce que los convenios colectivos podrán establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral[21]. Y en el artículo 88 RGPD se prevé que los convenios colectivos podrán establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral.

Desde la perspectiva del Derecho nacional, los controles biométricos encajan dentro de la delimitación del ámbito material de los convenios que hace el artículo 85 ET, al poder encajarse dentro de las "materias de índole laboral" propias de esta fuente del Derecho. El mismo artículo 34.9 ET, en su nueva redacción, señala que el registro de jornada obligatorio que establece se organizará y documentará "*mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores"*; y es este registro una de las utilidades principales de los procedimientos de verificación biométrica.

La realidad negocial española demuestra que los controles empresariales son un contenido típico, presente en múltiples de sus resultados. Aunque los últimos acuerdos nacionales de ordenación de la negociación colectiva no los hayan tratado, el Acuerdo Interprofesional de Cataluña contiene un Capítulo VII dedicado al "uso de tecnologías de la información y la comunicación", en el que se señala que "*se considera conveniente que los Convenios Colectivos regulen determinados aspectos sobre esta materia a efectos de clarificar el uso de los medios electrónicos, otorgar seguridad jurídica a las partes y evitar conflictos*". En particular se señala que "*en los procesos de implantación de nuevas tecnologías que supongan cambios en la organización del trabajo, la empresa deberá informar previamente a los representantes de los trabajadores*".

Como casi siempre que en España se señala el retraso de la negociación colectiva en ocuparse de una materia concreto, podemos encontrar algún convenio que **sí** lo hace, y muy bien. Este es el caso del XIX Convenio colectivo general

[21] Esta capacidad de ordenación negociada podrá efectuarse "*en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral*."

de la industria química que señala que "*la implantación por parte de la empresa de tecnologías de la información para el control de la prestación laboral, tales como controles biométricos como la huella digital, la video vigilancia, los controles sobre el ordenador (monitorización remota, indexación de la navegación por internet, o la revisión o monitorización del correo electrónico y/o del uso de ordenadores) o los controles sobre la ubicación física del trabajador mediante geolocalización",* se realizará respetando en todo momento las previsiones de la legislación vigente en materia de protección de datos.

Este convenio impone a los empleadores obligaciones concretas, señalando que deberán ser proporcionales a la finalidad de verificar el cumplimiento por parte del trabajador de sus obligaciones y deberes laborales; y deberán respetar su dignidad y su derecho a la protección de datos y a su vida privada.

Es interesante señalar que este convenio reconoce que la legitimación para el tratamiento deriva de la existencia de la relación laboral; en consecuencia, "*de acuerdo con la normativa aplicable, no se requiere del consentimiento del trabajador*". No es necesario este consentimiento, pues, pero sí la información: "*deberá en todo caso cumplirse con los deberes de información previa a los trabajadores afectados que se establecen en la legislación vigente*". Esta solución es técnicamente correcta, como veremos.

El convenio distingue también entre la dimensión individual y colectiva de estos controles, al afirmar que "*cuando este tipo de medidas tengan el carácter de colectivas o plurales deberá informarse previamente a su implantación a los representantes de los trabajadores, indicando la finalidad que se persigue*". Aparece, pues, un segundo deber de información, esta vez a los representantes de los trabajadores, que como se verá resulta coherente con la legislación laboral en vigor[22].

Se trata de un deber de informar en sentido estricto. Pero el artículo 64 ET impone un verdadero derecho de consulta en esta materia al reconocérsele el derecho a "*emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por este, sobre (...) control del trabajo*". Para el Estatuto, pues, el empresario no cumple con su obligación con la mera información, que es unilateral, sino que deberá también esperar un informe.

No es la única duda que se nos plantea. Así, parece que quedan excluidas de este deber de información las medidas que se establezcan a nivel individual, para un único trabajador. Con independencia de que resulte difícil imaginar en qué circunstancias puede procederse así, lo cierto es que las competencias que el Estatuto de los Trabajadores reconoce a la representación unitaria en la empresa

[22] Es interesante que se deba informar tanto de la propia medida como de la finalidad perseguida con ella, pues este último aspecto resulta fundamental para que estos representantes puedan valorar la legitimidad de su establecimiento en un primer momento (aplicando el test de la proporcionalidad y comprobando si existen alternativas más respetuosas con la intimidad de los trabajadores) y de su aplicación en un segundo (comprobando qué utilidad se le da a los datos así obtenidos).

no distinguen según el alcance de los sistemas de control que se implanten, por lo que la solución que recoge el convenio no me parece adecuada en este punto.

Este convenio colectivo, aprobado en una de las unidades de negociación de vanguardia en nuestro país, demuestra tanto una especial sensibilidad por estas cuestiones como una evidente experticia técnica en su redacción. Ofrece un tratamiento completo de los derechos digitales de los trabajadores, tanto individuales como colectivos, con un espacio de regulación muy amplio al incluir todos los medios de monitorización usuales en las empresas. Y pone en evidencia a otras unidades negociales, que a pesar de la generalización de este tipo de controles no han sido capaces de incluirlos

Esta ausencia es coherente con la situación de nuestra negociación colectiva, muy poco sensible a las cuestiones relacionadas con la tecnología. Los convenios que se ocupan de ésta lo hacen por lo general sólo en su parte disciplinaria, disponiendo sanciones por el uso indebido de los medios de trabajo electrónicos por los trabajadores. Es cierto, por otra parte, que son muchos los convenios que consideran sancionables las conductas dirigidas a sortear los medios de control puestos en práctica por la empresa, especialmente los de verificación de la entrada y permanencia en la empresa. Estas prácticas, como la fichar por otro, o la de acceder al ordenador con claves ajenas para este mismo fin, resultan sin embargo difíciles cuando estos mecanismos son biométricos, puesto que en estos casos la suplantación, contra la voluntad del trabajador o con su consentimiento, resulta imposible. Su utilidad a efectos de ordenarlos resulta por ello reducida.

5. RÉGIMEN JURÍDICO DE SU UTILIZACIÓN EN LAS EMPRESAS

Como se ha señalado, el régimen jurídico del uso de los controles biométricos es el resultado del entrecruzamiento de dos grandes conjuntos de materiales normativos, el laboral y el digital.

El artículo 9 RGPD los incluye dentro de las categorías especiales de datos personales, cuando señala en su apartado 1º que "*quedan prohibidos el tratamiento de (...) datos biométricos dirigidos a identificar de manera unívoca a una persona física*". Se integran así en la categoría de los datos merecedores de la mayor tutela, al mismo nivel que aquellos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los datos genéticos, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales[23]. Esta inclusión supone que disfrutan de un nivel de garantía

[23] Llamo la atención a que el artículo 9.1 RGPD utiliza la expresión "orientaciones sexuales", a diferencia de las normas unioneuropeas preexistentes, que hablan de "orientación sexual", en singular. Debe dar respuesta esta modificación a las demandas de los distintos colectivos que abogan por un reconocimiento expreso de las distintas manifestaciones sexuales y de identidad de género. Se trata de una tendencia a la inclusión que sin embargo, está empezando a crear motivos de protección antidis-

superior en todos los aspectos, quedando sometidos a una regulación más estricta. Una regulación que puede ser incluso más restrictiva, ya que este artículo habilita a los Estados miembros a mantener o introducir condiciones adicionales, inclusive limitaciones, al tratamiento de estos datos (artículo 9.4 RGPD).

Desde la perspectiva laboral, la posibilidad de establecerlos se encuentra en el artículo 20.3 ET, que como es sabido habilita al empresario a adoptar las medidas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Estas medidas serán las que "estime más oportunas", lo que le concede un amplio margen de actuación; al no tener una regulación digital propia, no se le imponen restricciones o exigencias más allá de la general de guardar "*en su adopción y aplicación la consideración debida a su dignidad*".

Pero esta afirmación, cierta desde el punto de vista laboral, resulta falsa desde el punto de vista del Derecho de la protección de datos, que se les aplica igualmente. Ya lo indica el GT-29 en varios de sus documentos, cuando señala que los empresarios deben tener siempre presentes los principios fundamentales de protección de datos, independientemente de la tecnología utilizada[24].

La base para la licitud del tratamiento de los datos biométricos del trabajador se encuentra en el artículo 6 RGPD, que dispone que será lícito por cumplir una de las condiciones exigidas en este precepto. En este caso nos encontraríamos ante el supuesto previsto en la letra b), a saber "*el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte*". El contrato cuya ejecución legitima el tratamiento es, obviamente, el contrato de trabajo que vincula al empleador que impone el mecanismo y el trabajador que lo sufre.

Sin embargo, no basta con esta habilitación. Teniendo en cuenta que nos movemos dentro del ámbito de aplicación del artículo 9 RGPD, que como se ha visto prohíbe como regla general el tratamiento de los datos biométricos, será necesario acreditar la concurrencia de alguna de las excepciones previstas en el apartado 2 del mismo precepto. En concreto cabe utilizar aquí la excepción de la letra b) de este apartado, según la cual "*el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión, de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado*".

criminatoria que, precisamente por su particularidad, pueden obviar todo aquello que no se encuentre expresamente incluido y definido. Por este efecto paradójico, parece una mejor opción la de la inclusión de un concepto antidiscriminatorio más amplio incluso que el de orientaciones sexuales, como puede ser el de diversidad sexual, puesto que, una vez claro que se trata de proteger manifestaciones de orientación sexual e identidad de género diversas a las culturalmente dominantes, permite mayor grado de protección de los colectivos más minoritarios.

[24] Últimamente en su Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, de agosto de 2017 (WP 249), pg.3.

Dos son los requisitos a cumplir para asegurar esta legitimidad: que sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos de trabajadores y empresarios, de un lado; y que esté autorizado por una norma, legal o convencional. El segundo se cumple con lo previsto en el artículo 20.3 ET; el primero resulta mucho más difícil de determinar, puesto que sólo podrá determinarse caso por caso, y utilizando el test de legitimidad construido por los tribunales nacionales e internacionales cuando se trata de valorar el impacto de una conducta empresarial sobre los derechos fundamentales de los trabajadores.

Esto supone que el empresario deberá acreditar que existe una finalidad legítima, superando el test de justificación. Que debe ser necesario, considerando la finalidad perseguida con el mecanismo de control. Y que debe ser proporcional, garantizando un equilibrio entre la finalidad legítima perseguida y el impacto sobre los derechos fundamentales de los trabajadores[25].

La aplicación de este test, común a los sistemas de control tecnológico de la actividad de los trabajadores, puede resultar compleja, y no siempre se llega a soluciones claras. Esto puede generar inseguridad jurídica en su utilización, algo que puede tener consecuencias serias para las empresas. Especialmente cuando, como ocurre en este caso, las opiniones sobre la legitimidad de los controles biométricos en las empresas no son unánimes.

Para la AEPD, los controles biométricos no superan, como regla general, el test de proporcionalidad, por su carácter intrusivo, lo que obliga a las empresas y entidades que los establezcan a demostrar que no existe un sistema que tenga un impacto menor en los derechos de las personas afectadas.

Por su parte, la Autoridad Catalana de Protección de Datos afirma que "*no parece que se pueda concluir la proporcionalidad de la utilización de la huella dactilar para establecer un sistema de control horario*". Según este organismo, "*la inclusión de los datos biométricos, entre ellos los de la huella dactilar, entre las categorías especiales de datos previstas por el RGPD no permite concluir de manera automática que la implantación de un sistema de control horario basado en la recogida de este tipo de datos pueda considerarse proporcionada y, por lo tanto, conforme con el principio de minimización"*. Esto no significa excluir este tipo de controles de las relaciones laborales, sino que hay que gestionar su introducción de otra manera: *"hay que hacer una evaluación del impacto sobre la protección de datos a la vista de las circunstancias concretas en las que se lleve a cabo el tratamiento para determinar su legitimidad y proporcionalidad, incluido el análisis de la existencia de alternativas menos intrusivas, y establecer las garantías adecuadas*"[26].

[25] Un caso práctico de aplicación de este test en A. Selma Penalva, "El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores", *Aranzadi Social*, nº9, 2010.

[26] Dictamen CNS 63/2018 de la Autoridad Catalana de Protección de Datos; pg.9 de la versión castellana del documento.

El GT-29 también expresa sus dudas sobre el cumplimiento de este test, y aporta algunas indicaciones sobre como comprobar que se aprueba[27].

Por el contrario, el Tribunal Supremo español, en sentencia de 2 de julio de 2007, ha encontrado que existe una finalidad en los controles biométricos que, en sus propias palabras, "*es plenamente legítima: el control del cumplimiento del horario de trabajo al que viene obligados los empleados público*s". En su opinión, tomar una imagen de la mano de un trabajador para velar por el respeto al horario laboral, puede considerarse una medida "*adecuada, pertinente y no excesiva*". Para el Tribunal Constitucional, "*que los datos sobre la biometría de la mano del recurrente sean datos personales no convierte su exigencia y posterior tratamiento automatizado en ilegítimos*" (Auto 57/2007, de 26 de febrero).

En cuanto a la forma de implantarlos, y de manera coherente con su visión restrictiva sobre esta tecnología, los organismos especializados en materia de protección de datos, como la AEPD o el GT-29, han señalado que es importante para la legitimidad del sistema que éste no almacene el dato biométrico; y que no se utilice para todas las instalaciones de la entidad que los imponga, sino sólo respecto de aquellas consideradas especialmente vulnerables o sensibles[28].

Estas limitaciones han hecho surgir dudas sobre su utilidad como mecanismo de registro de jornada, su uso más común en la práctica laboral. La obligación de registrar la jornada de trabajo ha sido sin duda una de las novedades del Derecho del Trabajo del año 2019, aunque el surgimiento y la consolidación de esta idea tengan un origen anterior. No es éste lugar para recordar este proceso; baste señalar el cambio de papel que ha tenido este registro, que ha pasado de ser un instrumento destinado a proteger el interés del empleador a actuar como medio de tutela del trabajador, asegurando el cumplimiento de la legalidad y de lo contractualmente acordado. Sin embargo, desde la perspectiva del Derecho del Trabajo digital el debate se vuelve a plantear en los términos tradicionales, en los que se consideran los riesgos que genera para los derechos del trabajador, más que como un instrumento para su protección.

[27] "*Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar1. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado*". La traducción al castellano la he tomado del Dictamen CNS 63/2018 de la Agencia Catalana de Protección de Datos.

[28] En palabras de la AEPD, en su Dictamen de 2015, *"esta Agencia considera que sólo sería ajustado al principio de proporcionalidad un sistema de reconocimiento dactilar que, por una parte, y como en el supuesto planteado, quede reducido a determinadas dependencias del centro, particularmente el comedor y, por otra permita que los medios de verificación, en este caso el algoritmo de la huella dactilar del alumno, permanezcan en su poder y no sean incorporados al sistema, que sólo incluiría los datos referentes a la identificación del alumno que accede al comedor, al producirse una verificación positiva del mismo*".

La nueva redacción del artículo 34.9 ET impone a las empresas la obligación de garantizar este registro diario, y al establecer sus requisitos mínimos señala que éstas deberán conservar los registros durante cuatro años, permaneciendo a disposición de los trabajadores, sus representantes colectivos y la Inspección de Trabajo. La Guía sobre el registro de jornada elaborada por el Ministerio de Trabajo, Migraciones y Seguridad Social desarrolla esta idea, señalando que los registros deben "*estar y permanecer físicamente en el centro de trabajo, o ser accesibles desde el mismo de forma inmediata*"[29]. El Criterio Técnico de la Inspección de Trabajo 101/2019 incide en la necesidad de esta presencia o accesibilidad en los centros de trabajo[30]. Esta obligación hace surgir, una vez más, la duda sobre la compatibilidad de ambas regulaciones, generando inseguridad para las empresas[31].

Un uso indebido nos coloca dentro del ámbito de las infracciones laborales muy graves, pues el artículo 8.11 LISOS tipifica como tales "*los actos del empresario que fueren contrarios al respeto de la intimidad y consideración debida a la dignidad de los trabajadores*". En la práctica judicial puede suponer también la nulidad de las pruebas obtenidas mediante sistemas implementados irregularmente, afectando a la validez de las decisiones empresariales adoptadas de acuerdo con la información suministrada por ellas.

Existe acuerdo entre tribunales y órganos administrativos sobre la necesidad de informar a los trabajadores afectados[32]. Por el alcance de la medida, pero también por aplicación de un principio general en la protección de datos de los trabajadores que ha acuñado el GT-29, para el que éstos "*deben recibir información efectiva sobre el control que se lleva a cabo*".

Sin embargo, no parece necesario obtener el consentimiento[33], algo en lo que coinciden también tribunales y órganos administrativos. Esto por movernos dentro de la ejecución de un contrato de trabajo, y por la propia legitimidad de la medida de control. La antes citada sentencia del Tribunal Supremo de 2 de julio de 2007, opina que dado que el control del cumplimiento del horario de trabajo es una finalidad legítima; y en tanto esa obligación es inherente a la relación que une a los trabajadores con la entidad que los emplea, no es necesario obtener previamente su

[29] MINISTERIO DE TRABAJO, MIGRACIONES Y SEGURIDAD SOCIAL, "*Guía sobre el registro de jornada*", accesible en http://www.mitramiss.gob.es/ficheros/ministerio/GuiaRegistroJornada.pdf. Visitada el 1 de septiembre de 2019.

[30] INSPECCIÓN DE TRABAJO Y SEGURIDAD SOCIAL, "*Criterio Técnico 191/2019 sobre actuación de la Inspección de Trabajo y Seguridad Social en materia de registro de jornada*". Accesible en http://www.mitramiss.gob.es/itss/ITSS/ITSS_Descargas/Atencion_ciudadano/Criterios_tecnicos/CT_101_2019.pdf, visitado el 15 de septiembre de 2019.

[31] En extenso Gracia García, *ibídem*.

[32] Así lo declara la sentencia de la Sala de lo Contencioso-administrativo de la Audiencia Nacional de 21 de 2013.

[33] Entendiendo por consentimiento, de acuerdo con el RGPD y la LOPDPGDD, toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

consentimiento[34]. De todas maneras, esta innecesariedad del consentimiento debe relativizarse, en la medida en que en este ámbito su utilidad como garantía de los derechos de los trabajadores es limitada. Así, en el Dictamen del G-29 de 2017 tantas veces citado en este trabajo se afirma que 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 tienen consecuencias[35].

Al no estar previstos en el Título X de la LOPDPGDD tampoco se recogen especialidades en cuanto al papel de los representantes de los trabajadores, que sí aparecen en la regulación de otros supuestos de control tratados en esta ley. Rige por tanto lo previsto en el artículo 64 ET, que reconoce al comité de empresa el derecho a emitir informe sobre "*la implantación y revisión de sistemas de control del trabajo";* informe que deberá ser previo a su implementación, y en los términos previstos en el apartado 1º de este mismo artículo. El artículo 34.9 ET también reconoce su competencia cuando el mecanismo de vigilancia se utiliza para registrar la jornada. Este papel lo corrobora la sentencia de la Sala de lo Social del Tribunal Supremo de 19 de diciembre de 2005: "*cuando el artículo 64 del ET ordena oír al Comité de Empresa para la implantación de determinados sistemas de control de trabajo está imponiendo una obligación laboral, cuyo incumplimiento debe ser objeto de análisis por la Jurisdicción Social*".

El incumplimiento de la obligación de información supone la comisión de una infracción laboral grave, según el artículo 7.7 de la Ley de Infracciones y Sanciones en el Orden Social[36]. También puede afectar a la validez de las pruebas obtenidas, y en consecuencia de las decisiones empresariales apoyadas sobre éstas.

Teniendo en cuenta el carácter intrusivo de los mecanismos utilizados, y la naturaleza de los datos obtenidos, parece claro que el recurso a esta tecnología debe venir precedido de una evaluación de impacto, en el sentido del art. 35 RGPD[37].

[34] Entre otras muchas, véase la sentencia de la Sala de lo Social del Tribunal Superior de Justicia de la Comunidad Valenciana, de 8 de febrero de 2017. Véase también la sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Andalucía de Sevilla de 27 de septiembre de 2007.

[35] En la ya citada sentencia de la Sala de lo Social del Tribunal Superior de Justicia de la Comunidad Valenciana, de 8 de febrero de 2017 se afirma que "*en el ámbito laboral el consentimiento del trabajador pasa, por tanto, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes*".

[36] Que, como es sabido, califica como infracción laboral grave "*la transgresión de los derechos de información, audiencia y consulta de los representantes de los trabajadores y de los delegados sindicales, en los términos en que legal o convencionalmente estuvieren establecidos*".

[37] Así lo entiende el Dictamen CNS 63/2018 de la Agencia Catalana de Protección de Datos, en el que se afirma lo siguiente: "*en cualquier caso, con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo, teniendo en cuenta las implicaciones tecnológicas de la tecnología utilizada, la observación sistemática de los hábitos de los trabajadores y el tratamiento de*

Como es sabido, el apartado 1º de este artículo dispone que cuando sea probable que un tipo de tratamiento, por la tecnología utilizada, por su naturaleza, alcance, contexto o fines, pueda suponer un alto riesgo para los derechos y libertades de las personas físicas, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Esta evaluación deberá realizarla el responsable del tratamiento, que podrá contar con la colaboración en su caso del Delegado de Protección de Datos; y deberá efectuarse previamente al inicio del tratamiento de los datos.

De la misma manera, aplica el principio general de minimización, que exige, de acuerdo con el artículo 5 RGPD, que los datos personales sean "*limitados a lo necesario en relación con los fines para los que son tratados*". Según el artículo 25.2 de esta misma norma unioneuropea, el responsable del tratamiento deberá aplicar las medidas técnicas y organizativas apropiadas para garantizar que, "*por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento*". En particular esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. El objetivo de minimización se tendrá en cuenta, además, tanto en el momento de determinar los medios de tratamiento como en el del propio tratamiento

En la práctica judicial española su generalización ha llevado a que sean considerados por los tribunales como un indicio de laboralidad. Como quiera que se implementan para controlar a los propios trabajadores, el que se apliquen también a otras personas no empleadas de la empresa apunta fuertemente hacia la calificación de éstos como personal de ésta, tanto en supuestos de cesión de trabajadores[38] como de falsos autónomos. Esto es una complicación, porque los controles biométricos se utilizan no sólo para verificar el cumplimiento de las obligaciones laborales, sino también para regular el acceso a las instalaciones empresariales[39].

La introducción de un sistema de control de acceso mediante datos biométricos no supone una modificación sustancial de condiciones de trabajo ni requiere el acuerdo del comité de empresa, como señala la sentencia de la Sala de lo Social del Tribunal Superior de Justicia de la Región de Murcia, de 25 de enero de 2010. En caso de desacuerdo de éste sobre la implantación de tal mecanismo resulta válido acudir a la vía del conflicto colectivo, según sentencia de este mismo órgano de 15 de julio de 2009.

datos de una categoría especial (biométricos), sería preciso llevar a cabo una evaluación del impacto relativa a la protección de datos de carácter personal para evaluar tanto la legitimidad del tratamiento y su proporcionalidad como la determinación de los riesgos existentes y las medidas para mitigarlos".

[38] Así ocurría en el supuesto de hecho contemplado por la sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Cantabria de 25 de mayo de 2010.

[39] No es raro encontrar, por ello, situaciones en las que las empresas combinan dos sistemas de regulación de acceso: el biométrico para los propios empleados; y otro alternativo, más tradicional, para personal ajeno, tanto clientes como proveedores y empleados de empresas contratistas.