DERECHO A LA INFORMACIÓN Y CONSENTIMIENTO DEL TRABAJADOR EN MATERIA DE PROTECCIÓN DE DATOS

EDUARDO GONZÁLEZ BIEDMA

Catedrático de Derecho del Trabajo y de la Seguridad Social
Universidad de Sevilla

EXTRACTO **Palabras clave: protección de datos, consentimiento, información, videochat, propia imagen, datos biométrico**

La privacidad real en materia de datos es un fin cada vez más difícil de mantener, y a ese fin se orienta el nuevo Reglamento de la UE en materia de protección de datos.

En el ámbito de las relaciones laborales, en materia de datos, la regla es la de "informar" a los trabajadores sobre el tratamiento de los mismos, y no su consentimiento. La jurisprudencia ha entendido que, en determinadas circunstancias, cabe omitir incluso el deber de información expreso. El Tribunal Constitucional –Sentencia 39/2016- ha corroborado esta tesis. En materia de comunicación por "videochat" entre un teleoperador y el cliente, no puede concluirse que esté implicado el derecho a la imagen del trabajador, ni implique en sí mismo un tratamiento de datos, a menos que los mismos sean almacenados o grabados. La Sentencia AN de 15 de junio de 2017 ha considerado que no es válido un consentimiento previo y genérico en materia de datos. Los datos biométricos de los trabajadores no se consideran especialmente protegidos a la hora de su tratamiento.

ABSTRACT **Key words: Protection of data, consent, videochat, self-image, biometric data**

Real privacy of data is an increasingly more difficult to maintain order, and to that end leads the new regulation of the EU in the field of data protection.

In the field of labour relations, in terms of data, the rule is the "report" to workers on the treatment of the same, and not consent. The jurisprudence has understood that, in certain circumstances, you can skip even the express duty of information. The constitutional court -Sentence 39/2016- underpinned this thesis. In terms of communication by "chat" between a sales representative and the customer, not you can concluded that is the right of the image of the worker involved, nor in itself involves a processing of data, unless the same be stored or recorded. AN judgment of 15 June 2017 has been considered a prior generic consent of data is not valid. The biometric data of the workers are not considered specially protected when it comes to your treatment.

 Recepción del original: 02.10.2017 Aceptación original: 09.10.2017

ÍNDICE:

1. PROTECCIÓN DE DATOS EN LA ÉPOCA DE LA "SUPERCONEXIÓN" ¿ES REALISTA ACTUALMENTE RECLAMAR LA "PRIVACIDAD" DE LOS DATOS PERSONALES?

El nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, que entrará en vigor el próximo 25 de mayo de 2018[1], justifica su implantación, entre otras distintas razones, en que "...*La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades"*.

Y, precisamente, nos recuerda, que "*La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"*[2]. Y añade que *"El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad"*[3].

Estamos, por lo tanto, no ante un cambio sustancial, cualitativamente esencial respecto de la realidad previa, sino sobre todo ante un cambio cuantitativo de la realidad que, como todos, tienen también una incidencia indirectamente cualitativa. En efecto, no se trata de que estemos ante la novedad de las bases de datos electrónicas, de internet o del comercio y administración electrónica. Se

[1] Vd., en concreto, su art. 99
[2] Vd. Exposición de Motivos del texto legal, apartado (1)
[3] Idem, apartado (4)

trata de cómo esos modelos y sistemas han progresado hasta hacerse presentes e invasivos en todos los ámbitos de la vida, a partir de su generalización. Ello, sin perjuicio de que otras tecnologías y aplicaciones de las mismas están suponiendo una novedad sustantiva. Las tecnologías "disruptivas" –genómica, robotización e inteligencia artificial, la nube, internet móvil de alta velocidad, internet de las cosas, vehículos autónomos, impresión 3D, materiales avanzados…[4]- se unen a usos específicos e intensivos de internet –como el manejo del "*big data*", *block-chain*…- y todo ello implica un manejo realmente masivo de datos personales con -¿inevitables?- invasiones de la privacidad[5].

Ahí es donde precisamente pretende irrumpir el Reglamento[6], que quiere de alguna manera reafirmar el juego del derecho personal a la intimidad y confidencialidad. El éxito de este loable deseo es una cuestión distinta.

En torno a este Reglamento, lo primero digno de destacarse es precisamente su propio carácter normativo: estamos ante un Reglamento Europeo. Significa un cambio cualitativo en relación a la regulación de la protección de datos, sustituyendo a otra norma que tenía rango de Directiva -la 95/46/CE- que quedará derogada a partir del 25 de mayo de 2018 (art. 94 del Reglamento). Significa por lo tanto el deseo de un mayor nivel de homogeneización y también de la propia ejecutividad, en la práctica, de la norma, ya que, como es sabido, un Reglamento tiene alcance general y es *"…obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro"*[7]. Lo que en términos prácticos significa que, alcanzado el momento de su entrada en vigor[8], va a ser la norma de referencia en la materia, por su directa aplicación por nuestros tribunales domésticos. Se limita así mucho más, mediante su aplicación directa, el margen regulatorio de los Estados miembros, que va a estar limitado, prácticamente, a aquellos ámbitos en los que el propio Reglamento Europeo les confía un espacio regulatorio propio.

[4] Vd. en especial MCKINSEY GLOBAL INSTITUTE, (J. Manyika, M. Chui, J. Bughin, R. Dobbs, Peter Bisson, A. Marrs) "Disruptive technologies: Advances that will transform life, business, and the global economy", Mayo 2013. En https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies.

[5] Vid. Las reflexiones al respecto de Desdentado Bonete, A. y Muñoz Ruiz, B., Control Informático, Videovigilancia y Protección de Datos en el Trabajo, ed. Lex Nova, Valladolid, 2012, pág. 18.

[6] Resulta de enorme interés al respecto contrastar el análisis al respecto de J.L. Goñi Sein, "Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores. Análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016", en Revista de Derecho Social,

[7] Art. 288 TFUE. Tras su mismo art. 99, el Reglamento sobre Protección de datos, nos recuerda que el mismo "será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro".

[8] El Reglamento será aplicable desde el 28 de mayo de 2018, si bien, técnicamente entró en vigor a partir de los veinte días de su publicación en el DOUE, lo que sucedió el 4 de mayo de 2016.

Así lo reconoce también la propia E. de M. del Reglamento, en su apartado 10º, cuando afirma que "*... el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros"* [9], aun reconociendo que los Estados deben estar facultados para regular a nivel nacional la aplicación de las normas del Reglamento, incluidas las que se refieren a las normas sectoriales.

El propósito del Reglamento Europeo es, sin duda, encomiable. Es justo ser hoy particularmente sensibles a la enorme fuerza de la tecnología para acceder a los datos personales, en el deseo de preservar la privacidad de las personas. Con ello, se salvaguarda nada menos que la intimidad personal y, a la postre, la más básica libertad individual.

Pero cuestión distinta es cuán factible resulta en las circunstancias actuales. Esto es, si ante la masiva presencia de internet y los motores de búsqueda –que hace una recolección constante de datos personales- teléfonos inteligentes, y todo tipo de registros públicos (seguridad social, AEAT, padrones, instituciones educativas, Registros oficiales como el RM, Registro de la Propiedad, expedición de DNI y pasaportes) centros de trabajo, tarjetas de crédito y medios de pago, bancos, compañías de teléfono y de servicios públicos, establecimientos comerciales, páginas de venta on-line, aerolíneas, compañías ferroviarias, agencias de viaje..., nuestros datos están, y casi diríamos que inevitablemente, en manos de decenas de instituciones y empresas de todo tipo. Y ello por no hablar de los datos que mostramos voluntariamente en las redes sociales: Linkedin, Whatsapp, Facebook, Youtube, Skype, Instagram, Google+ ... Son lugares donde de una manera voluntaria comunicamos no ya nuestros datos personales, sino aspectos concernientes a nuestra vida privada y familiar, e incluso de otras personas, no necesariamente con su autorización (p.ej., cada vez que se "etiqueta" a una persona en una fotografía de una entrada propia de Facebook, se indica ante terceros dónde estaba, qué hacía e incluso su imagen física). Si a ello sumamos nuestros accesos a internet, entrando en páginas cuyas "cookies" aceptamos repetidamente, dejando todo tipo de rastro informático a terceros, nuestra intimidad está cada vez más cuestionada. Hasta el punto de que, en la actualidad, con una pantalla de ordenador conectada a internet y algunas habilidades informáticas, incluso poco sofisticadas, un simple usuario puede acceder a datos increíbles sobre las más distintas personas. El desarrollo tan acusado de los "big data", por lo demás, no

[9] Y añade: "Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea".

hacen sino evidenciar hasta qué punto los datos de los ciudadanos circulan a muy distintos niveles y llegan a ser una mercancía.

Y es que, en efecto, como la propia E. de M. de este Reglamento admite, *"Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales*"[10].

Plantear por lo tanto la privacidad de los datos personales, su tratamiento, o restricción en el uso de los mismos puede ser, probablemente, una actividad realmente hercúlea, y de muy dudoso éxito. Nos debemos preguntar, de hecho, si esa etapa, la de la "privacidad controlada" –esto es, que los terceros sepan sobre nosotros sólo lo estrictamente permitido o aceptado por el interesado en cada caso- puede que sea ya, desafortunadamente, algo del pasado. Y es que, por si hubiese ya poca complejidad en la gestión y regulación de la privacidad de los datos personales, se suma la dimensión esencialmente supranacional y transfronteriza de internet. La misma permite sortear el cumplimiento de cualquier legislación nacional –o supranacional, como la de la UE- en materia de datos sólo con un poco de imaginación a la hora de ubicar servidores.

Sin embargo, el legislador, acertadamente, insiste en reivindicar esos bienes jurídicos –privacidad, intimidad, derecho a regir libremente los datos de nuestra vida, que pueden ser conocidos por terceros- de una manera activa y enérgica y con ese fin arranca ese nuevo Reglamento Europeo.

Facilitar información sobre qué datos van a ser almacenados o tratados, exigir –sólo a veces y con limitaciones, como se verá- el consentimiento del afectado, se parece, cada vez más, a una formalidad más, que se añade a la carga regulatoria y documental que tiene que soportar las empresas e instituciones.

Todas estas reflexiones tienen una clara proyección en el ámbito de las relaciones laborales, como no puede ser de otro modo. Los datos de los trabajadores deben manejarse con toda una serie de cautelas, pero el manejo de sus datos es inherente a la propia presencia en una organización como es una empresa: el devengo de sus salarios, control de jornada, de presencia, datos familiares, itinerario formativo, datos con relevancia fiscal y de seguridad social, datos de salud, habilidades, expediente de conducta y desempeño dentro de la propia empresa. Constituyen todos ellos datos de mucha entidad y que la empresa debe manejar de

[10] Vd. Exposición de Motivos, (6)

manera indeclinable ¿Cuál es el margen y las exigencias que la misma tiene para su tratamiento? ¿Con quién puede compartir esos ficheros? ¿Cuál es la capacidad de los propios representantes de los trabajadores a la hora de tener acceso a los datos de esos ficheros que les sean relevantes?

2. REGLAS BÁSICAS EN EL TRATAMIENTO DE DATOS PERSONALES DENTRO EN EL ÁMBITO DE LAS RELACIONES DE TRABAJO

Como es sabido, en materia de recogida y tratamiento de datos, la Ley distingue entre "información" al afectado y "consentimiento" del mismo.

La primera constituye un derecho más extendido, fácil de interpretar y fácil de cumplir. En síntesis, nos indica el art. 5 LOPD que siempre que se soliciten datos a un afectado éste deberá ser informado "de modo expreso, preciso e inequívoco", de una serie de extremos: en todo caso, de la existencia de un fichero o tratamiento de los datos, de la finalidad de su recogida y de los destinatarios de la información; la segunda de la identidad del responsable del tratamiento.

Además, existen otras obligaciones de información que sólo deberán ser cumplidas si del contenido de la solicitud de dato no queda ello claro: el carácter obligatorio o facultativo de las respuestas, las consecuencias de la obtención de los datos o la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

El deber información, por lo demás, deberá cumplirse incluso cuando los datos personales no hayan sido recabados del interesado directamente, debiendo informar el responsable del fichero a éste a los tres meses del registro de los datos, si bien existen excepciones para esta importante carga de suministro de información[11].

Para el "tratamiento" de los datos debe partir del consentimiento del afectado, o bien, alternativamente, que tal tratamiento se justifique por razones que evidencien la necesidad ineludible de ese tratamiento. Así nos lo indica el art.

[11] En efecto, no siempre deben informarse. El art. 5.5. LOPD establece que no será necesaria la información al interesado, "… cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten".

6.1 LOPD, cuando afirma que "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".

Sin embargo, no resulta totalmente claro cuándo deba "informarse" al afectado y cuándo éste deba prestar su "consentimiento". Si la distinción de partida es que lo primero procede cuando se recaben datos del interesado, y lo segundo cuando tales datos vayan a ser "tratados", no puede obviarse que la definición legal del "tratamiento" de los datos incluye también la actividad de la propia recogida de los mismos. Así, veamos el art. 3 LOPD cuando, a la hora de exponer las definiciones de los conceptos manejados por la Ley encontramos lo siguiente:

"c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"[12]

Superposición que también se encuentra, por cierto, en la lista de definiciones del propio Reglamento Europeo[13].

La AEPD es consciente de este solapamiento de conceptos y abordó brevemente la cuestión en su informe 60/2004, donde trata de salir al paso de esta cuestión, resolviéndolo de la siguiente manera[14]:

[12] En efecto, el Reglamento Europeo entiende que la propia "captación" del dato es ya parte del "tratamiento" (Art. 6 Rgto. Europeo). Para que sea lícita requiere las siguientes condiciones: a) Consentimiento expreso por del interesado para que sus datos sean tratados "para uno o varios fines específicos". b) Que el tratamiento sea en sí mismo necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. c) Que el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. d) Que el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física. e) Que el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. f) Que el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que concurran además otras circunstancias. Se admite, por último, que los Estados miembros puedan mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del reglamento en ciertos aspectos.

[13] Su art. 4 lo incorpora a su lista de definiciones: "… cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción

[14] Guía, La protección de datos en las relaciones laborales. Pág. 12. Obtenible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales2.pdf

"El artículo 5 de la Ley Orgánica 15/1999 viene a establecer un deber impuesto en general a los responsables de los tratamientos, de tal suerte que, en principio, será necesario informar al afectado del tratamiento de sus datos de carácter personal, tanto en los supuestos en que el mismo cuenta con el consentimiento del mismo como en los casos en que el tratamiento se encuentra habilitado por otras causas admitidas por el artículo 6 de la propia Ley".

Es decir, reconociendo la mencionada superposición, y admitiendo implícitamente que la recogida de datos es ya parte del "tratamiento" de los mismos, la salva concluyendo que mientras que el deber de información existe en todo caso (aunque existen también excepciones a ese deber) hay que tener en cuenta que no sucede lo mismo con el consentimiento, debido a que existen muy distintos supuestos en los que ese deber no existe. Así lo razona, además, la propia AEPD en un documento público[15], indicando que el deber de información forma parte del contenido esencial al derecho de protección de datos, y por lo tanto se aplica tanto en el caso de que requiera consentimiento como en los casos en los que no se requiera. Es decir, rige con carácter general –aun con algunas excepciones- mientras que el consentimiento no será siempre exigido, pues existen amplias importantes excepciones legales, como se expondrá más adelante.

De cualquier modo, el consentimiento del afectado es esencial para el tratamiento de datos consistente en su "grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."

Para ello, no basta la información, sino que se precisa el consentimiento del afectado… salvo las excepciones legalmente aceptadas, que no son pocas. Así, el art. 6.2. LOPD, en concreto, dispone que:

"No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción

[15] Guía, La protección de datos…. Cit.., pag 8. El deber de información del art. 5 LOPD forma parte del contenido esencial del derecho a la protección de datos. Este carácter esencial lo posee tanto en el caso de la recogida de los datos personales para un tratamiento que requiera consentimiento como en el supuesto de que no lo requiera.

del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".[16]

Podemos apreciar que se abre por lo tanto un amplio abanico de razones de difícil control, definición e incluso de averiguación por parte del interesado: ¿Cómo conocer cuando se protege el "interés vital"? ¿y cuándo los datos son accesibles al público? ¿cómo estar seguro de cuándo el tratamiento de un dato es necesario para cumplimiento de una relación negocial, laboral o administrativa? ¿cuándo el tratamiento es necesario para satisfacer el interés legítimo por el responsable del fichero o por el tercero al que se le comunican los datos? Como se puede apreciar, cada aserto del art. 6.2 es una fuente de preguntas y de posibles interpretaciones que somete cualquier deseo de certidumbre y de control por parte del interesado.

Y ¿en qué condiciones debe darse el consentimiento? Mientras que el art. 6 LOPD indica sucintamente que el consentimiento del afectado debe ser "inequívoco", el art. 7 del Reglamento Europeo lo especifica con mayor claridad: debe "dejar rastro", aunque no se establece un método específico para ello. Sabedora la norma europea de la rápida evolución de las tecnologías, se limita a decir que el responsable debe únicamente "demostrar" (se entiende que por cualquier medio razonable, sin exigir ninguno en concreto) que el afectado prestó su consentimiento para el tratamiento de sus datos personales[17].

Matiza también que "Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo". Es decir, previene expresamente de las cláusulas de consentimiento

[16] El Reglamento Europeo indica por su parte, en su art. 9.2, que son recabables los datos especialmente sensibles (los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física) en determinados casos. En concreto: a) Cuando el interesado hubiera dado su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuanddo realmente la exigencia inicial de consentimiento expreso pueda ser ignorada.

[17] Especifica este precepto lo siguiente: 1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

que son meras apostillas, en letra pequeña, incorporadas a un contrato principal. Exige, por lo tanto, "fácil acceso", lenguaje "claro y sencillo", y además debe presentarse con claridad respecto de los otros asuntos que se incorporen al documento en cuestión.

El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

También interesa destacar que se establece una prohibición específica de tratamiento respecto de ciertos datos personales: Así, los que muestren el origen étnico y racial, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Como hemos podido observar, no cabe apreciar una gran diferencia entre lo regulado a nivel nacional y a nivel europeo.

El consentimiento vuelve a jugar otro papel importante en materia de comunicación de los datos. Así, nos indica el art. 11. LOPD que la comunicación de datos a un tercero exige, junto al requisito de "legitimidad" –pues dispone que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario- el del "consentimiento" del afectado. Y, de nuevo, se prevé que este consentimiento pueda no ser requerido en una serie de circunstancias (autorización por ley, ser datos recogidos de fuentes accesibles al público…). Se prevé además que tal consentimiento será nulo "… cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar".

Sabido es también que existen determinados supuestos en los que es más restringida la posibilidad de tratamiento de datos. Es el caso de datos especialmente sensibles, y por ello particularmente protegidos, que se contemplan en el art. 7.2 LOPD. Se trata en concreto de los datos personales que revelen la "… ideología, afiliación sindical, religión y creencias". En tales casos, sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal, también necesario para la cesión.

3. ¿INFORMACIÓN O CONSENTIMIENTO?

Debemos en este momento, a la vista de los planteamientos anteriores, recapitular si en el marco de las relaciones laborales, con carácter general, debe "informarse" a los trabajadores del tratamiento de los datos de carácter personal o si debe haber consentimiento por parte de los trabajadores. Esto es, debemos preguntarnos si cabe acudir a alguna de las excepciones legalmente contempladas en el art. 6.2 para que sea necesario que el trabajador consienta el tratamiento de sus datos o si, por el contrario, tal consentimiento debe darse indefectiblemente.

Esta pregunta es muy pertinente, no sólo por lo polémico del asunto en sí, sino por el hecho, creciente, de las "cláusulas de datos" en los contratos laborales, las cuales también han sido sometidas al análisis de los Tribunales en ocasiones, y a ello precisamente se dedicará el siguiente apartado. ¿Son realmente necesarias? ¿Basta la información? ¿Cuáles podrían ser las respuestas del empresario ante una eventual negativa del trabajador?[18]

Para abordar este tema se hace indispensable partir de la Sentencia del TC 39/2016, de 26 de marzo. En la misma, a propósito precisamente de una captura de datos de imagen de un trabajador que acabó en su despido –tema este que más específicamente se tratará en un apartado posterior- afirmaba 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*".

Incide además en que la excepción a la exigencia de consentimiento consta igualmente en el art. 10.3 b) del Real Decreto 1720/2007, de 21 de diciembre (RLOPD), según el cual los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando "se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento".

Afirma con rotundidad el TC que:

> *"... un tratamiento de datos dirigido al control de la relación laboral debe entenderse amparado por la excepción citada, pues está dirigido al cumplimiento de la misma. Por el contrario, el consentimiento de los*

[18] Vd., E.M. Blázquez Aguado, "La implantación de un protocolo de videovigilancia en elcentro de trabajo", Revista Aranzadi de Derecho y Nuevas Tecnologías, núm.43/2017, p. 12.

trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato".

Así, para el Alto Tribunal, el deber que de verdad pesa sobre el empresario no es otro que el de información, en tanto que "este deber permite al afectado ejercer los derechos de acceso, rectificación, cancelación y oposición y conocer la dirección del responsable del tratamiento o, en su caso, del representante (art. 5 LOPD)"[19].

Añade el TC que "En todo caso, el incumplimiento del deber de requerir el consentimiento del afectado para el tratamiento de datos o del deber de información previa sólo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada", citando a su vez otra Sentencia anterior del propio Tribunal -la STC 292/2000, FJ 11- para recordar que el derecho a la protección de datos no es ilimitado, por lo que debe ser cohonestados con los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución.

Destaquemos en este punto que la no exigencia de consentimiento en determinados supuestos tiene también repercusión en otro de los principios de la protección de datos, el denominado por el art. 4 LOPD, calidad de los datos. El art. 4.1 LOPD establece que "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". Por lo tanto, sólo cuando la finalidad del tratamiento de datos no sea el mantenimiento, desarrollo y control de la relación contractual se es preciso el consentimiento del afectado.

Por ello, aunque no se requiere el consentimiento expreso de los trabajadores para adoptar esta medida de vigilancia que implica el tratamiento

[19] Se ha visto en ello contradicción con la tesis previa del propio Tribunal Constitucional. De hecho, esta Sentencia cuenta con un voto particular, más partidario de la doctrina representada por las SSTC 29/2013, de 11 de febrero de 2013 (STC 2013, 29), 98/2000 de 10 de abril (RTC 2000, 98) y 186/2000, de 10 de julio (RTC 2000, 186). Vd. al respecto, entre otros, H. MONZON PÉREZ, "El deber de protección de datos personales» de los trabajadores y su transgresión., en Revista de Información Laboral, n. 2/2017. Y también, considerando críticamente esta Sentencia, véase C. González González, «Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016» en Revista Aranzadi Doctrinal, núm. 5/2016. Imprescindible también resulta en este sentido, para determinar la trayectoria previa del TC, examinar la obra de Casas Baamonde, M.ª Emilia, «El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal Constitucional», en 20 años de protección de datos en España, Madrid (AEPD) 2015, pp. 91-126.

de datos, persiste el deber de información del art. 5 LOPD. Sin perjuicio de las eventuales sanciones legales que pudieran derivar, concluye el Tribunal que "para que el incumplimiento de este deber por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad".

Se requeriría por lo tanto, sólo, "información". Pero, es más, incluso la misma sería eludible en ciertos términos, a la vista de la excepción contemplada en el art. 5.3 LOPD.

Es oportuno citar, al respecto, la Sentencia del TS (Sala de lo CA) de 2 de julio de 2007 (RJ 2007/6598) y que recientemente ha sido sacada a la luz en un brillante artículo de los profesores GARCIA PERROTE Y MERCADER[20], a propósito de los requisitos en materia de protección de datos cuando se trata de datos biométricos de los trabajadores, cuestión sobre la que, por cierto, se volverá más adelante.

Se destaca en esa Sentencia que, aunque es cierto que el art. 5.1. LOPD determina que los interesados a los que se soliciten datos personales deben ser, al menos, informados con carácter "…expreso, preciso e inequívoco" de distintas cuestiones relativas al fichero que se va a generar, dispone el mismo art. 5, en su núm. 3 que sólo será necesario informar de la identidad y dirección de los responsables de tratamiento, así como de la propia existencia del fichero y de su fin "… si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban". En el caso contemplado por la Sentencia en cuestión, se aprecia que la información sí se dio al trabajador -aun verbalmente, se ha de entender- por el mero hecho de que, al tomársele con infrarrojos la huella digital se le debería haber indicado en buena lógica su fin. Y en cuanto al responsable del fichero, si bien no se entra en detalle, parece que es un dato que se pasa por alto ante su obviedad, o porque probablemente le constaba al trabajador. Lo cierto es que, a pesar de no haber habido una información documentada convenientemente, el Tribunal entiende que se actuó correctamente por parte de la empresa y concluye que no procede sanción contra la misma.

Lo cual, como ya se hizo notar, deja la puerta abierta a que incluso pueda omitirse en la gran mayoría de los casos el deber de información a los trabajadores del tratamiento que van a sufrir sus datos personales. No es que sea algo precisamente recomendable o una regla a seguir por los empresarios, pero lo que nos indica esta Sentencia es que ese camino está abierto y que no

[20] I. García-Perrote Escartín y J. R., Mercader Uguina, "El control biométrico de los trabajadores", Revista de Información Laboral num.3/2017 (BIB 2017\1102).

puede presumirse que la falta de información aludida sea directamente un hecho sancionable.

No parece, por lo demás que el Reglamento Europeo vaya a cambiar este estado de cosas, puesto que el mismo, en su art. 6, requiere que, para que el tratamiento de datos sea legal, que el interesado dé su consentimiento al mismo (art. 6.1.a), pero no es menos cierto que también admite que el tratamiento de datos sea "… necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales" (art. 6.1.b), entre otras excepciones[21].

Sea entendido todo lo demás, por supuesto, con excepción de los "datos especialmente protegidos" del art. 7 LOPD (ideología, creencias, origen…), para los que no hay que obviar el consentimiento en modo alguno[22].

4. ¿ES NECESARIO EL CONSENTIMIENTO PARA MOSTRAR LA IMAGEN EN "VIDEOLLAMADAS"?. ¿PUEDE ÉSTE DARSE AL INGRESO EN EL TRABAJO Y CON CARÁCTER GENERAL? LA SENTENCIA DE LA AN DE 15 DE JUNIO DE 2017 (REC. 137/2017) (CASO UNISONO)

En una reciente decisión, la AN ha tenido ocasión de pronunciarse sobre cuestiones críticas en la prestación del consentimiento en materia de protección

[21] Aunque algún autor pretende averiguar en este Reglamento un cambio a favor de exigir siempre el consentimiento expreso. Así, E. BLÁZQUEZ, op. cit., pág. 13, que no entiende que pueda justificarse la falta de consentimiento expreso en la necesidad de ejecución de un contrato en el que es parte el interesado.

[22] Vd. AEPD, Guía… pags. 12 y 13: "Se trata de datos que bien por su naturaleza religiosa o ideológica, bien por pertenecer al núcleo más íntimo de la persona resultan merecedores de una especial protección. Lo que obliga a disponer de procedimientos que garanticen: Una adecuada información en la recogida de los datos ya que aquí se acentúa la importancia del cumplimiento de este deber. «En consecuencia, la posibilidad de admitir un consentimiento expreso que no conste por escrito para el tratamiento de los datos de salud, se encuentra condicionada a que pueda acreditarse que es una manifestación de voluntad libre, inequívoca y específica, que se presta una vez que se ha tenido conocimiento de una concreta información entre la que, necesariamente, ha de constar la finalidad determinada, explícita y legítima del tratamiento que se va a realizar sobre los datos personales del afectado. Lógicamente, la concurrencia de los extremos expuestos deberá constatarse en cada caso concreto. (PS/00029/2004 PS/00525/2007)». Antes de recabar este tipo de datos es necesario analizar la proporcionalidad del tratamiento y la legitimación para el mismo. Ej. Como más adelante se examina, para la adaptación de un puesto de trabajo es posible que deban conocerse algunosdatos de salud, o que estos se deduzcan de la adaptación propuesta. Pero ello no legitima al empresario para incorporar y tratar los datos de salud en sus sistemas de información salvo que cuente con un servicio de prevención de riesgos laborales propio o un servicio médico de empresa. En estos últimos casos se gestionarán historias clínicas."

de datos de ámbito jurídico-laboral. Nos referimos concretamente a la Sentencia de la AN de 15/6/2017 (Rec. 137/2017, Caso Unisono). Por el interés del tema tratado, así como por ser reciente, es buen punto de reflexión y por ello debe ser tratada, a pesar de que a buen seguro tal Sentencia está siendo objeto de recurso, no habiéndose en todo caso pronunciado el Tribunal Supremo al respecto.

La cuestión planteada se centra en el consentimiento prestado por los trabajadores ante el eventual uso de la herramienta de videollamada dentro del sistema informático y de comunicación de la empresa con los usuarios. "Unisono" es una empresa que presta servicios telemáticos, y en concreto, el de venta y atención telefónica en interés de terceras empresas, que incluye trato directo por el público a través del teléfono principalmente.

Unisono, al incorporar a los trabajadores, les invitaba a firmar una cláusula en el contrato de trabajo de este tenor:

> *«El trabajador consiente expresamente, conforme a la LO 1/1982, de 5 de mayo, RD 1720/2007 de Protección de Datos de carácter personal y Ley Orgánica 3/1985 de 29 de mayo, a la cesión de su imagen, tomada mediante cámara web o cualquier otro medio, siempre con el fin de desarrollar una actividad propia de telemarketing y cumplir, por tanto, con el objeto del presente contrato y los requerimientos del contrato mercantil del cliente".*

La finalidad que perseguía dicha cláusula era precisamente la de amparar jurídicamente el hecho de que, eventualmente, los empleados tuviesen que prestar su imagen ante una webcam cuando la interlocución con el cliente así lo requiriese. Estaba claro –así se destaca también en la sentencia- que no se trataba de cubrir con esta cláusula la aparición de la imagen con fines promocionales (para lo que sí se solicitaría un consentimiento específico), sino únicamente cubrir esa posibilidad que en realidad afectaba a sólo unos 15 trabajadores frente a los aproximadamente 6.000 con los que contaba la empresa.

Advirtamos que, aunque la cláusula en cuestión alude tanto a la cesión de la imagen del trabajador (en tanto que menciona la Ley Orgánica 1/1982), como a los datos de carácter personal (en tanto que cita expresamente el R.D. 1720/2008 Reglamento de la Ley de protección de datos), la Sentencia que comentamo examina el caso, principalmente, desde la perspectiva del consentimiento y tratamiento de datos contenida en la normativa específica en materia de datos.

La Sentencia concluyó que esa cláusula debía considerarse nula. Razona al respecto que:

> *"A lo que exclusivamente nos oponemos es que en el contrato de trabajo se haga constar -como específica cláusula/tipo- que el trabajador presta su «voluntario» consentimiento a aportar los referidos datos personales y a*

que la empresa los utilice en los términos que el contrato relata, siendo así que el trabajador es la parte más débil del contrato y ha de excluirse la posibilidad de que esa debilidad contractual pueda viciar su consentimiento a una previsión negocial referida a un derecho fundamental".

Concluye esta Sentencia, así pues, que en un momento inicial del contrato de trabajo sobre todo, el consentimiento prestado por el trabajador no tiene, de hecho, una validez asegurada. Ese consentimiento puede no ser sincero –de hecho, en la Sentencia parece asegurarse que así fue- porque siendo el trabajador la parte débil del contrato, el mismo no tiene otra alternativa que dar ese consentimiento, mucho menos cuando se presta al inicio de su relación jurídica con la empresa.

Otra cuestión esencial y que así es valorada por la Sentencia es que se considera poco razonable que se pida de manera genérica a todos los trabajadores el consentimiento para atender videollamadas cuando sólo una pequeña parte de los trabajadores va a prestar efectivamente ese servicio que implica contacto visual con los clientes. Así, entiende que resultaría más adecuado y más acorde a la proporcionalidad que requiere la limitación del derecho fundamental, el hecho de que se pidiese ese consentimiento sólo a los trabajadores que fuesen destinados a ese minoritario servicio y precisamente cuando se aproximara ese momento. Desaprueba por lo tanto el Tribunal que sea factible manifestar tal consentimiento de manera indiferenciada por todos los trabajadores y justo además en el momento de inicio del contrato de trabajo.

Esta Sentencia, pues, con independencia de que sea confirmada o revocada por una decisión posterior del TS, nos plantea varios puntos de reflexión interesantes y que deben ser abordados:

-El primero es –de nuevo- el de la naturaleza realmente libre del consentimiento cuando éste es prestado por el trabajador. Apunta la AN que el consentimiento puede no ser jurídicamente aceptable, generándose así un incumplimiento de la normativa sobre protección de datos, por el mero hecho de la debilidad objetiva del trabajador como parte negociadora, sin necesidad por lo tanto de acreditar tan siquiera vicio de la voluntad en un caso concreto. Reproduzcamos por ello precisamente el texto específico de la Sentencia donde se formula tal observación:

"A lo que exclusivamente nos oponemos es que en el contrato de trabajo se haga constar -como específica cláusula/tipo- que el trabajador presta su «voluntario» consentimiento a aportar los referidos datos personales y a que la empresa los utilice en los términos que el contrato relata, *siendo así que el trabajador es la parte más débil del contrato y ha de excluirse la posibilidad de que esa debilidad contractual pueda viciar su consentimiento a una previsión negocial referida a un derecho fundamental, y que dadas las*

circunstancias -se trata del momento de acceso a un bien escaso como es el empleo- bien puede entenderse que el consentimiento sobre tal extremo no es por completo libre y voluntario*"*.

Invoca para ello distintas Sentencias del Tribunal Supremo si bien reconoce que las mismas están referidas a "cláusulas de temporalidad" insertas en contratos de trabajo.

Este razonamiento está en línea con el habitual recelo con el que es observada la autonomía individual en el ámbito laboral, particularmente desde las resoluciones judiciales. Y no hay que abundar mucho para cuestionar hasta qué punto la aceptación por un trabajador medio de las condiciones laborales que le vienen marcadas desde la empresa se aceptan de una manera genuina o si son realmente impuestos.

Sin embargo, ¿es realmente exportable esa desconfianza al ámbito de la protección de datos? Y aún más, ¿es en el ámbito jurídico-laboral donde únicamente se produce esa desventaja del individuo frente a la empresa/institución en materia de datos? Pensemos en que el consentimiento en materia de datos se pide, en la casi totalidad de las ocasiones, por instituciones o empresas en las cuales la alternativa a no prestar el consentimiento puede ser realmente frustrante para el usuario: en general, la alternativa será la denegación del servicio solicitado; sea una línea de teléfono móvil, una cuenta bancaria, una tarjeta de crédito o una compra on-line. Es decir, la alternativa a no prestar el consentimiento cuando éste sea necesario en materia de tratamiento de los datos personales no es otra que la de no recibir el servicio (el equivalente en el ámbito laboral sería: no obtener el trabajo ofertado). Por lo demás, las "cláusulas de datos" son redactadas siempre por el empresario o institución en cuestión, sin que el cliente o usuario tenga ninguna opción en relación a la modificación de su contenido.

Se hace esta reflexión únicamente para poner de relieve las consecuencias tan significativas y graves que tendría aceptar con carácter general este planteamiento de la AN en relación al consentimiento en materia de tratamiento de datos: si se entiende que la situación intrínseca de sumisión en la que se encuentra estructuralmente el trabajador (y no el engaño, el abuso o el dolo en una determinada ocasión) a la hora de acceder a un empleo es susceptible de viciar en términos materiales el consentimiento para el tratamiento de los datos, las consecuencias sobre la invalidez del consentimiento podrían extenderse de forma ilimitada.

-El segundo es que pedir un consentimiento demasiado amplio en materia de datos en relación a los datos que posiblemente vayan a ser objeto de tratamiento se debe tener como una práctica rayana al fraude, en tanto que supone un exceso respecto de los derechos personales en juego. Se indica que debe pedirse el

consentimiento según vaya a ser necesario el tratamiento de datos de acuerdo con la modificación del puesto de trabajo o con la posible modificación funcional del trabajador. En concreto, no se debe pedir un consentimiento para datos –como en este caso, los relativos a la imagen del trabajador- que no vaya a ser tratado. Debe pedirse ese consentimiento para cada contrato que exija desvelar el físico de cada trabajador. Así lo razona la Sentencia de la AN:

"Consiguientemente, cuando la empresa destine a sus trabajadores a la realización de servicios de video llamada, porque lo requiera así el contrato mercantil con el cliente, deberá solicitar, en ese momento, el consentimiento del trabajador, que deberá ajustarse de manera precisa y clara a los requerimientos de cada contrato, sin que sea admisible la utilización de cláusulas tipo de contenido genérico, que no vayan asociadas a servicios concretos, requeridos por contratos específicos, por cuanto dicha generalización deja sin contenido real el derecho a la propia imagen de los trabajadores, que queda anulado en la práctica, aunque se diera consentimiento genérico al formalizar el contrato".

Desde esa perspectiva, según ya se ha indicado, habría que ir pidiendo a los trabajadores consentimiento de tratamiento de datos no de un modo genérico y al inicio de la relación laboral, sino por etapas, ajustando la petición de consentimiento a las específicas necesidades de tratamiento. El Tribunal observa que en este caso, al tratarse de datos concernientes a la imagen, que sólo afectaba a una cantidad muy poco significativa de trabajadores, no era proporcionado pedir ese consentimiento indiscriminadamente a todos los teleoperadores, como al parecer así sucedía.

El propósito de esta tesis es desde luego muy cabal, pero la misma no está exenta de inconvenientes:

-El primero es que la Ley no exige tal requisito. La norma requiere que el consentimiento sea informado y libre y, sobre todo, inequívoco. Recordemos que el art. 12.2 RLOPD dispone que el interesado "…deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario" disponiendo que "en caso contrario, el consentimiento será nulo". Esto es, se reserva la declaración de nulidad a aquellos supuestos en los que falle la información previa al interesado -sin perjuicio, naturalmente, que sean aplicables al caso las causas de nulidad derivadas de la teoría general del Derecho de obligaciones- pero, sobre todo, no se impide que el consentimiento pueda ser dado para eventuales situaciones posteriores que surjan en la relación con la entidad o persona que precisa el consentimiento para su tratamiento. Siempre, claro está, que no se trate de eventualidades claramente inconexas del factor que promovió que prestara originariamente el consentimiento.

Por lo demás, el art. 3. H) LOPD, a la hora de especificar los requisitos de la manifestación de voluntad que exprese el consentimiento que hay que dar, la voluntad tiene que ser "libre, inequívoca, específica e informada". ¿Cuál es el elemento que faltaría en el asunto contemplado por la AN en esta Sentencia? ¿Por qué? No olvidemos que el procedimiento en el que se emite esta doctrina es un conflicto colectivo en el que el sindicato demandante argumenta el carácter ilícito en sí de la cláusula, de manera apriorística, pero no se llega a alegar de qué manera algún trabajador puede haber visto singularmente perturbada su libertad a la hora de suscribir su consentimiento.

Desde esta perspectiva, esta exigencia adicional que formula la AN consistente en que el consentimiento sea escalonado o adecuado a las distintas situaciones que puedan surgir, puede ser razonable, e incluso una atinada propuesta *de lege ferenda*. Pero resulta más que cuestionable que, con la vigente ley en la mano, pueda exigirse ello bajo sanción de nulidad.

-El segundo se refiere a si la alternativa que sugiere el Tribunal realmente es capaz de superar los inconvenientes que observa en ese consentimiento anticipado y más genérico. Y las dudas vienen porque, si el punto de partida es que el consentimiento del trabajador no es muy creíble, al estar en un lugar de debilidad en su relación contractual, esa situación va a persistir también al momento de ser pedido un nuevo consentimiento. Presumir que al principio de la relación el trabajador es más débil que en ese segundo momento es algo que puede ser verdad o puede no serlo, dependiendo de cada caso. Habrá, por ejemplo, algún trabajador que en las condiciones de negociación de su contrato se atreva a incluir una mayor restricción en el tratamiento de sus datos, dentro de las condiciones generales de incorporación a la empresa, y habrá quien lo prefiera hacer de otra manera y habrá a quien le sea indiferente. Pero presumir con carácter apriorístico que al principio de la relación laboral el trabajador firma "cualquier cosa" para no perturbar que le den su trabajo, y que después no lo haría, es algo que todo lo más podría ser cierto por aproximación, de manera intuitiva o estadística, pero que no se puede elevar a categoría jurídica. Pero, es más, si aceptamos ese razonamiento, cualquier consentimiento habría de darse por viciado, y por lo tanto por inútil, tanto si se refiere a eventos futuribles y de dudosa ocurrencia, como si se refiere a otros inmediatos.

El argumento que más sólidamente podría haber sido expuesto por la Sentencia, se habría de referir a valorar si concurren en este caso los elementos del consentimiento para desplegar sus efectos, pero eso no se ha hecho así ya que, como se ha recordado, se trata de una Sentencia de conflicto colectivo, en la que por tanto se ha prescindido de las peculiaridades de casos concretos.

-El tercero es que la ley prevé algo que, aunque la Sentencia recoge, parece haber quedado fuera de su razonamiento: El consentimiento puede ser revocado

en cualquier momento. Así nos lo recuerda el art. 6.3 LOPD cuando afirma que "El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos".

En muy buena medida, esa previsión legal permite que los abusos que se hubieran constatado a la hora de haber solicitado el consentimiento, puedan ser redimidos con una revocación. Poca mejor "justa causa" para la revocación puede ser la de entender que no se debe extender a aspectos que no quedaron suficientemente claros a la hora de dar el consentimiento, la falta de libertad subjetiva al suscribir el compromiso o bien la existencia de cualquier circunstancia sobrevenida que haga razonable tal revocación.

-Por último, destaquemos que un aspecto muy llamativo de esta Sentencia es que entra en el análisis de la demanda de conflicto colectivo, esto es, en la adecuación a Derecho de la cláusula de datos, obviando el tema de que podría haber supuesto enfocar el asunto de una manera muy distinta: ¿es preciso realmente prestar el consentimiento al tratamiento de datos en un supuesto como el presente?

A la vista de la Sentencia del TC mencionada en el epígrafe anterior, no lo parece. Pero ese es un tema que, quizás por no haberse planteado adecuadamente en el proceso, no fue considerado en la Sentencia, que siguió la pauta lógica de la petición formulada en el conflicto colectivo –la declaración de antijuridicidad de una cláusula determinada- sin entrar a considerar si ese consentimiento era en realidad necesario para el correspondiente tratamiento de los datos.

Tampoco puede obviarse que, en el caso, junto al consentimiento en materia de datos puede estar también implicado el derecho a la protección de la propia imagen, invocándose también el mismo en el proceso, por lo que podría estar también bajo consideración el art. 2.1.de la L.O. 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, precepto según el cual "La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia. Dos. No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por ley o cuando el titular del derecho hubiese otorgado al efecto su *consentimiento expreso*".

Este aspecto, curiosamente, no ha sido prácticamente tenido en cuenta por la Sentencia, si bien cita a esta Ley en algún momento, no la tiene en cuenta a la hora de emitir sus razonamientos. Así, se ha centrado de hecho, de forma exclusiva, en la aplicación de la normativa de datos. Esta perspectiva, de haberse considerado con mayor profundidad, nos hubiese llevado a otro escenario y a otra serie de

cuestiones incluso previas a la del tratamiento de datos: ¿Debe considerarse la aparición en pantalla ante un cliente como un hecho que atente, en sí mismo, a la propia imagen, y que por tanto deba ser requerido de consentimiento previo?

Cuestión ésta que se sale en cierto modo del objeto de este estudio pero en relación al que se pueden exponer ahora algunos planteamientos básicos:

No parece que fuese directamente aplicable a este supuesto la doctrina del TC construida a partir de su Sentencia 99/1994, de 11 de abril, sobre "el cortador de jamón", en tanto que la misma dirimía la legitimidad de incluir fotografías del empleado en un medio impreso con fin publicitario.

Por el contrario, en el caso presente, lo que se dirime es la aparición de un empleado a través de una conversación donde, eventualmente, mostrara su cara ("videochat" de cualquier tipo, aplicaciones estándar como Skype o Facetime…) no implica la apropiación ni divulgación de su imagen (pues divulgar una imagen es distinto que meramente ser observado, siquiera por vía telemática, por el único interlocutor que tiene el interesado en cada momento). Más propiamente son medios de comunicación instantánea, que no presuponen una grabación ni almacenamiento de las imágenes. Por lo tanto, ni siquiera constituye un almacenamiento de las mismas en una base de datos.

A lo sumo, es algo parecido a una conversación telefónica (sólo que con imagen, que a su vez no es almacenada en ninguna base de datos): en una videoconferencia estamos prestando la imagen, al igual que no estamos prestando la voz en una llamada de teléfono de voz.

Es cierto que esa imagen implica que el empleado sea visto por el cliente: ¿Pero no sucede lo mismo en cualquier trabajo que exige interacción con el público? En todos ellos el empleado muestra su cara –y presta su voz- a esa interacción; así como en relación a sus compañeros de trabajo, con los que se relaciona constantemente. ¿Exige ello un consentimiento especial en relación a la normativa de datos?

Es cierto también que sería susceptible de almacenamiento: Pero no por sí mismo. Esto es, las aplicaciones informáticas en cuestión utilizadas no están directamente orientadas a la grabación. Son comunicaciones instantáneas que, en sí mismas, no se orientan a la grabación. No se descarta que puede haber utilidades que las graben de alguna manera, pero eso es algo extraordinario y excepcional, sólo para el caso de que algún cliente haga algo indebido. En ese caso, la empresa no se lo facilitaría y sería sólo fruto de las "malas artes" del cliente en cuestión. Ante eso, baste oponer una cláusula contractual en el contrato a suscribir con el cliente, sobre la prohibición de estas grabaciones y, además, adecuar los elementos técnicos de la aplicación para evitar la grabación.

Si el cliente, burlando tales prohibiciones y obstáculos tecnológicos logra grabarlo, entonces no sería ya un problema de cesión o de consentimiento, sino un tema de mera ilegalidad y fraude del propio cliente. Algo parecido a que entrase en un establecimiento físico y grabase ilegalmente a los demás clientes y al personal.

Desde esta perspectiva, la carencia de esta Sentencia es confundir la mera visualización con la grabación y almacenamiento de datos, que son conceptos distintos. Error no solamente imputable a ella, dicho sea de paso, sino a las propias partes litigantes, en tanto que la propia empresa obligaba a una dudosa "cesión de la imagen" del trabajador que en realidad no lo era: ni se "cedía" la imagen en sentido real, ni tampoco se constituía sobre ella una base de datos, en tanto que no se realizaban registros de las mismas. O, acaso, sí (por motivos de control de calidad o para grabar el eventual compromiso contractual del cliente), pero no era sobre ello sobre lo que se pedía el consentimiento, sino que únicamente se orientaba a una "cesión de imagen" que no parece que fuese tal.

En resumen, debe entenderse que la mera aparición virtual "cara a cara", siempre al menos que no implique grabación y almacenamiento de esos encuentros, no debe considerarse ni como una cesión de imagen ni de datos cuyo almacenamiento requiera consentimiento (ni siquiera información).

Distinto sería el caso si esas charlas cara a cara virtuales fueran registradas y almacenadas. En tal caso, se trataría de elaborar una base de datos que contuviera, además de voz, imágenes, y entonces sí que habría que cumplir las obligaciones derivadas de la ley, pero ello, como se ha indicado, no es el objeto de debate en este litigio.

5. CONSENTIMIENTO Y DATOS BIOMÉTRICOS DE LOS TRABAJADORES

Unas últimas líneas para hacer referencia a las bases de datos constituidas por los datos biométricos de los trabajadores.

La adquisición de los mismos –básicamente, las huellas dactilares- se hace cada vez más frecuente no ya como registros de presencia ("picar"), si bien también puede tener ese uso, sino sobre todo como vía de superar controles de acceso: barreras, cerraduras, zonas restringidas…

Es obvio que el registro de los mismos constituye la creación de una base de datos.

La pregunta sería si para ello es necesario el consentimiento o por el contrario bastaría la mera "información", a la vista de los argumentos expresados páginas atrás.

Cuestión ésta que va ganando actualidad y que fue abordado extensamente en la ya mencionada Sentencia del TS (Sala de lo CA) de 2 de julio de 2007 (RJ 2007/6598) y que mereció brillantes reflexiones de GARCÍA PERROTE Y MERCADER[23]. Tras su examen, concluyen que las bases de datos basadas en datos biométricos como éste, no exige previo consentimiento según indica el Tribunal, en tesis por cierto, bastante seguida por otros Tribunales Superiores de Justicia, sin que quepa hallar ninguna sentencia discrepante.

Se considera no sólo que se trata de un sistema plenamente aceptable (de control de horario, para el caso, y –añadimos- sin duda extrapolable a la apertura de accesos). Así, indica el TS que no se trata de un sistema lesivo para la integridad, ni es una injerencia ilegítima, ni ocasiona un resultado perjudicial para el empleado. La finalidad apuntada por el empresario –el control horario, como se ha indicado- es legítima.

Por lo tanto, no hace falta consentimiento –art. 6.2 LOPD- y, por supuesto, está plenamente justificado y es proporcional, en atención al fin perseguido, además de no resultar incompatible con la dignidad del trabajador.

Debe subrayarse además que se concluye que tampoco hace falta ejercer una información específica y detallada de este hecho, dadas las características del caso.

En efecto, aunque es cierto que el art. 5.1. LOPD determina que los interesados a los que se soliciten datos personales deben ser informados con carácter "…expreso, preciso e inequívoco" de distintas cuestiones relativas al fichero que se va a generar, dispone el mismo art. 5, en su núm. 3 que sólo será necesario informar de la identidad y dirección de los responsables de tratamiento, así como de la propia existencia del fichero y de su fin "… si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban".

Obviamente, la información se le dio al trabajador (aun verbalmente) por el mero hecho de que, al tomársele con infrarrojos la huella digital se le indicó su fin, y en cuanto al responsable del fichero, si bien no se entra en detalle, parece que es un dato que se pasa por alto, también ante su obviedad.

Llegados a este punto, es pertinente verificar si existe alguna contradicción entre estas conclusiones y lo dispuesto en el Reglamento Europeo 2016/679.

Al respecto, e invocando también el estudio de GARCIA PERROTE Y MERCADER[24], hay que alcanzar una respuesta negativa. Es cierto que este Re-

[23] Vd. Nota 20.
[24] Ob. Cit., Pág 7

glamento ha incluido los datos dactiloscópicos entre los sujetos a una especial protección. Pero, igualmente, hay que reparar en que el art. 9.2.b) indica que tal regla no resulta aplicable en los supuestos de que el tratamiento del dato en cuestión sea necesario "…. Para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral 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…." Siempre dentro del necesario respeto a los derechos fundamentales.

6. REFLEXIONES FINALES

Estas líneas no han tenido otro propósito que el de revisar sólo algunas de las cuestiones clave del tratamiento de datos de los trabajadores en las circunstancias actuales, particularmente a la vista del nuevo Reglamento Europeo que muy pronto será ya de inexcusable vigencia.

En tal sentido, no se puede sino reconocer la enorme dificultad que tiene, en el mundo actual, preservar la privacidad, y con ella los datos personales. Lo que no exime –al contrario- del permanente esfuerzo de protegerlos, y no a otra cosa se endereza el nuevo Reglamento Europeo. No sabemos si con un empeño digno de mejor causa, pero lo cierto es que el legislador no puede abdicar de ese constante propósito, pues el mismo está en el propio núcleo de los derechos fundamentales.

Se ha querido igualmente destacar que en el ámbito de las relaciones laborales, la regla por defecto en materia de tratamiento de datos es la de "información", más que el consentimiento del afectado.

Obviamente, los datos especialmente sensibles o protegidos (ideología, afiliación sindical, creencias…) no pueden sino estar sujetos a la más alta protección al respecto, y por escrito según indica el art. 7.2 LOPD, y por lo tanto su tratamiento exige consentimiento previo y escrito del afectado.

La Sentencia del TC 39/2016, en concreto, viene a confirmar que, en el ámbito laboral, el consentimiento se entiende implícito en la relación contractual inherente a la misma, en tanto que el tratamiento de los datos personales sea necesario para el cumplimiento del contrato firmado por las partes. Matiza además que este carácter implícito del consentimiento también se debe entender dado al tratamiento de datos que se dirija al control de la relación laboral.

Merece ser reseñada la Sentencia de la AN de 15 de junio de 2017, en tanto que aborda el consentimiento dado de modo amplio, en relación al tratamiento

de datos relativos a "hechos futuros". Entiende que el consentimiento en tales casos se ha de considerar ineficaz, declarando nula la cláusula en el marco de un procedimiento de conflicto colectivo.

Sin embargo, se concluye en este estudio que no sería necesario el consentimiento en este caso, sino sólo información a los interesados. Y, además, que no puede considerarse el "videochat" o la videoconferencia con los clientes como un tratamiento de datos.

En cuanto al tratamiento de datos biométricos de los trabajadores, que es un tema de cada vez mayor uso, reactivado como medio de control de presencia en los lugares de trabajo, la jurisprudencia –en la que destacamos la Sentencia del TS (Sala CA) de 2 de julio de 2007- entiende que el tratamiento de los mismos no sólo no precisa consentimiento de parte de los trabajadores, sino que ni siquiera requerirían de información específica, al ser obvio, cuando se le toman esos datos el uso que se le va a dar.