PROTECCIÓN DE DATOS EN EL ÁMBITO LABORAL

Presentado por:
Eduardo José Lagarón Martín

14 de Febrero de 2011

Abreviaturas

LOPD: Ley Orgánica de Protección de Datos.

LSSI: Ley de Servicios de la Sociedad de Información.

ET: Estatuto de los Trabajadores.

PS: Procedimiento Sancionador.

S.L: Sociedad Limitada.

GME: Gabinete Médico Evaluador.

Índice

1. Introducción

La protección de datos en las relaciones laborales constituye actualmente uno de los pilares básicos de la investigación en materia de protección de datos. La importancia del tratamiento de los datos de carácter personal por parte del empresario sobre sus trabajadores, adoptando las medidas de seguridad necesarias para la confidencialidad de estos, resulta algo totalmente obligatorio para el empresario. El presente trabajo tratará de analizar las medidas y procedimientos que ha de utilizar aquel, así como los límites que se le imponen a la hora de ceder los datos de carácter personal de sus empleados, donde como bien indica la Ley Orgánica 15/1999 el principio fundamental es el consentimiento de este. El tratamiento de los datos por parte del empresario ha de ejercerse para una finalidad concreta, y son numerosos los casos por los que el descontento por parte de un empresario hacia sus subordinados, ha originado que aquél ceda los datos a otras empresas del sector con el fin de desacreditar su aptitud profesional, entrando en colisión con derechos del tan fundamentales como pueden ser el derecho al honor o el derecho a la intimidad del empleador.

Más controvertido y de mayor interés sin duda, por su alarma social, son aquellas en las que el empresario ejerce un poder de control y vigilancia sobre el empleado. Este aspecto era totalmente impensable en décadas anteriores pero debido a las apariciones tecnológicas actuales, y sobre todo por aquellas que están aún por crearse, el empresario deja de ser aquella persona que controlaba los datos personales para garantizar su confidencialidad frente a terceros, para poder utilizar esos datos como instrumento de control y vigilancia de sus empleados tanto en el ámbito laboral como fuera de él. Es por ello necesario, analizar cada uno de los aspectos donde el responsable de los datos puede ejercer un poder de control y vigilancia sobre los trabajadores, tratando este informe de investigación, entre otras cosas, delimitar el derecho del empresario y el derecho de las personas a su cargo, y así marcar los límites legales donde ambos derechos entran en colisión.

En definitiva, este trabajo de investigación pretende dar una visión general de aquellos mecanismos que ha de utilizar el empresario o empresa, para garantizar la privacidad de los datos, pero sobre todo pretende profundizar en aquellos temas donde actualmente existe mayor discrepancia en la doctrina y en la jurisprudencia a la hora de delimitar los derechos del propietario de los datos y los trabajadores. La resolución de estos temas de actualidad asentarán las bases futuras sobre como deben utilizarse los últimos avances tecnológicos, si por un lado se utilizarán de manera restrictiva lo que garantizará el derecho a la intimidad del trabajador, o por el contrario dichos avances carecerán de mecanismos legales de control, lo que dará lugar al fin de la privacidad individual a largo plazo.

2. Ámbito de Aplicación

El presente trabajo de investigación analizará las relaciones existentes entre la protección de datos y el ámbito laboral, analizando los problemas donde ambos ámbitos del Derecho convergen.

La compatibilidad existente entre las leyes de un ámbito y de otro son más que notables pero ello no impide la aparentemente existencia de incompatibilidades entre unas leyes y otras. Será entonces el análisis y las interpretaciones de la ley, los que nos aporte la solución a como han de combinarse, para que exista así una cohesión lo suficientemente estable como para poder afirmar que existe una seguridad jurídica evidente donde ambos Derechos se encuentran.

Por un lado, en cuanto al ámbito laboral, se utilizará primordialmente el Estatuto de los Trabajadores 8/1980, pues en el se recoge la mayor parte de la normativa, principios generales, y sobre todos los derechos de los trabajadores en el Derecho Laboral. Aunque también será de análisis la Ley de Prevención de Riesgos Laborales 31/1995. Asimismo, ello no impide que a lo largo del trabajo de investigación se cite normativa complementaria para el esclarecimiento de algún tema en concreto o el análisis de algún caso en particular.

Por otro lado, en cuanto al ámbito de protección de datos, se utilizará en mayor medida la Ley Orgánica de Protección de Datos 15/1999, ya que como es bien sabido, en ella se recoge los principios y derechos fundamentales en cuanto a los datos personales se refiere. Y se hará referencia también al Reglamento 1720/2007 por el cual se desarrolla la LOPD, haciendo hincapié en los aspectos procedimentales y de medidas de seguridad, los cuales, el empresario ha de cumplir. Del mismo modo, también se hará referencia a informes de la Agencia de Protección de datos con el fin de delimitar ciertos temas de diversa controversia.

2.1 Supuestos de no aplicación de la LOPD en el ámbito laboral

El Reglamento 1720/2007 plantea algunos supuestos de exclusión para la aplicación de la ley de protección de datos. Dichas exclusiones pueden afectar a la aplicación de la ley de protección de datos en el ámbito laboral. En concreto no se aplicará la ley de protección de datos a los datos definidos como "personas de contacto", y así lo indica el Reglamento en su artículo 2.2 que señala:

«Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales."

Evidentemente el concepto de "personas de contacto" es muy distinto del de fichero de personal, es decir, aquel fichero sobre los datos de los empleados, el cual si le es de aplicación la LOPD. De este modo, el concepto "personas de contacto" ha de interpretarse de modo restrictivo y

sentido estricto.

Para ello la Agencia de Protección de datos en su informe 78/2008 ha declarado tres requisitos:

a) Los datos tratados se han de delimitar a los meramente necesarios para identificar al sujeto en la persona jurídica a la que presta los servicios. Al tratarse de un concepto restrictivo y estricto, cualquier tratamiento que contenga datos adicionales a los citados se encontrará plenamente sometido a la LOPD. Y así hace constar este criterio restrictivo en el informe: "*Por ello, no se encontrarían excluidos de la Ley los ficheros en los que, por ejemplo, se incluyera el dato del documento nacional de identidad del sujeto, al no ser el mismo necesario para e mantenimiento del contacto empresarial. Igualmente, y por razones obvias, nunca podrá considerarse que se encuentran excluidos de la Ley Orgánica los ficheros del empresario respecto de su propio personal, en que la finalidad no será el mero contacto, sino el ejercicio de las potestades de organización y dirección que a aquél atribuyen las leyes"*.

b) La finalidad del tratamiento ha de ser una relación directa entre los que traten el dato y la entidad, y no entre aquéllos y quien ostente una determinada posición en la empresa. Por lo que, el uso del dato debería dirigirse a la persona jurídica, siendo el dato del sujeto, únicamente el medio para lograr esa finalidad. De este modo lo determina la Agencia de Protección de Datos Española en su informe: "*Así sucedería en caso de que el tratamiento responda a relaciones "business to business", de modo que las comunicaciones dirigidas a la empresa, simplemente, incorporen el nombre de la persona como medio de representar gráficamente el destinatario de la misma"*.

c) Dicho todo lo anterior no afecta en absoluto a las previsiones de la LSSI, pues como bien sabemos, la LOPD, señala que se aplicará todo lo dispuesto en ella salvo que exista norma habilitante que disponga lo contrario. Pero en este caso no existe realmente contradicción, ya que los principios que rigen el envío de comunicaciones comerciales por medios electrónicos se aplican tanto a personas físicas como jurídicas, y entre ellas, las mencionadas personas de contacto, por lo que no va en contra de lo dispuesto en la LOPD.

3. Inscripción de ficheros y cancelación de los datos en el ámbito laboral

3.1 Inscripción de ficheros

En cuanto a la inscripción de los ficheros, el problema reside básicamente en el desconocimiento de la ley. Muchos de los empresarios creen que sólo será de aplicación la LOPD a ficheros que estén incluidos en un software, y por tanto que haga referencia a una base de datos que esté informatizada. Pero como bien indica la LOPD, esta ley también se aplica a aquellos ficheros de datos de carácter personal que no estén informatizados, es decir, que no se encuentren automatizados.

Por lo tanto, la aplicación de la LOPD no depende de la informatización de los datos de carácter personal, y si estos están registrados en uno o varios programas de software, o en varias bases de datos. Sino que el criterio de la necesidad de inscripción del fichero depende de si el conjunto de datos de carácter personal contiene los criterios estructurales necesarios, para que resulte posible recuperar los registros relativos a un individuo determinado, lo cual define lo que es un fichero, tanto automatizado como no automatizado. Incluso cuando este es automatizado, no depende del software utilizado, pues el uso de una base de datos o un procesador de textos es indiferente para la aplicación de la LOPD.

Del mismo modo, cabe descartar que un fichero no es distinto de otro por el mero hecho de encontrarse en ordenadores distintos, es decir, que se encuentre en distintas ubicaciones, y así lo indica el informe 368/2003 señalando: *el concepto de fichero no va directamente vinculado a la exigencia de que el mismo se encuentre en una única ubicación, sino que será posible la existencia de ficheros distribuidos en lugares geográficos remotos entre sí, siempre y cuando la organización y sistematización de los datos responda a una conjunto organizado y uniformado de datos, sometido a algún tipo de gestión centralizada".* Por lo tanto, puede utilizarse un mismo fichero para finalidades distintas, siempre y cuando haya consentimiento por parte del afectado (aunque puede no ser necesario por existir una relación laboral) para el uso de esos fines, sin que por ello haya que declarar distintos ficheros (ej. Director de un departamento posee un fichero de sus empleados, y el mismo fichero lo posee el departamento de recursos humanos cuando contrató a aquellas personas).

En definitiva, para que un fichero sea de obligatoria inscripción en el Registro, no depende de si este esta automatizado o no, sino depende de los criterios estructurales utilizados durante su creación.

3.2 Cancelación y bloqueo de los datos

Antes de realizar la cancelación de los datos, es necesario el bloqueo de los datos. Ello es así

por la necesidad de poner a disposición de las *"Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos"*, según lo dispuesto en el artículo 5 b) del Reglamento 1720/2007. Por lo tanto, el empresario o empresa ha de ser consciente de que cualquier herramienta que use para la cancelación de los datos de carácter personal ha de contener un procedimiento de bloqueo de estos.

Para ello, debe delimitarse el periodo de uso y conservación de los datos y el momento en el que cesa la actividad o el hecho que legitimó su tratamiento, el cual dentro del ámbito laboral, suele ser el comienzo de la relación laboral.

Quizás el mayor problema existente es el período de bloqueo, ya que un periodo de bloqueo, y su posterior cancelación, que sea demasiado corto, puede causar problemas en cuanto a las obligaciones que puedan existir aún entre la empresa y demás organismos. Mientras que un procedimiento de bloqueo y cancelación excesivamente largo puede dar lugar a infracciones muy graves por parte de la LOPD. Por ello ha de conocer la empresa las obligaciones que genera su actividad empresarial, eligiendo un periodos de bloqueo y cancelación adecuados, para compatibilizar todas las legislaciones, y dando preponderancia al resto de legislaciones. Ya que como hemos indicado, la LOPD contempla el supuesto de *"salvo que exista norma legal habilitante en contrario"*.

Un claro ejemplo son las obligaciones tributarias, estas prescriben a los 4 años. Por tanto, los datos relativos a las retenciones practicadas aun trabajador deberían bloquearse por un periodo de 4 años a partir de la fecha límite para presentar la declaración de cada ejercicio.

Durante el periodo de bloqueo, los datos permanecerán inaccesibles a los usuarios, debiendo impedir la manipulación y acceso de aquellos, quedando como única opción posible, su puesta a disposición a las autoridades competentes.

4. Relaciones entre el departamento de recursos humanos y el empleado e interesado en materia de protección de datos

4.1 Introducción

Dado que existe una relación laboral entre la empresa o empresario y el empleado no sería necesario el consentimiento de este último mientras exista la relación negocial según indica el artículo 6.2 de la LOPD.

En cualquier caso, la exclusión del consentimiento no impide el deber de información por

parte de la empresa de que dichos datos de carácter personal van a ser tratados con un fin específico. De hecho, la ausencia de información al interesado vicia su declaración de voluntad, y esto es así porque de esta forma se garantiza que el interesado pueda ejercer sus derechos de cancelación, rectificación y oposición ante la autoridad competente.

Por lo cual, las empresas deben ser muy cautas en la elección del procedimiento por el cual se obtengan datos de carácter personal como en el momento de su captación.

4.2 Procedimientos de selección de personal

En este apartado analizaremos las medidas de seguridad que ha de adoptar los empresarios a la hora de obtener información de datos de carácter personal. Por otro lado, hemos de advertir de un problema cada vez más creciente en los procesos de selección, y es la búsqueda por parte del departamento de recursos humanos, a través de redes sociales, datos de carácter personal e íntimo de los candidatos de manera lícita e ilícita. Dado que este tema más bien de control por parte del empresario, se analizará posteriormente en este apartado.

Quizás el problema más destacado en este apartado, es el hecho de que la entrega de los currículums por parte de los interesados, se entiende implícitamente que se está dando su consentimiento de manera tácita para el tratamiento de sus datos. De cualquier modo, la empresa debe fijar procedimientos de información que supongan algún acuse o confirmación de conocer las condiciones en las que se desarrollará el tratamiento, ya sea mediante acuse de recibo, carteles o cualquier medio que garantice y permita probar y garantizar el cumplimiento del deber de información.

Se ha comprobado en la práctica, actos por parte de las empresas de desechar los curriculum de los candidatos en las papeleras más cercanas de su domicilio social incluso con comentarios sobre estos y sobre sus candidatos, y por tanto no se ha realizado ningún tipo de tratamiento obligatorio por la LOPD.

Así es el caso del procedimiento sancionador **PS/00072/2008** instruido por la Agencia Española de Protección de Datos a las entidades DISTRIBUCIONES MALABO 2000, y S.L., V SHOES DAM, S.L., el cual se inicia tras la denuncia presentada por el AYUNTAMIENTO DE MÓSTOLES. POLICÍA LOCAL, donde se hace constar el hallazgo de gran cantidad de documentación procedente, según los indicios, de un local comercial de la empresa DISTRIBUCIONES MALABO 2000, S.L., entre la que se encontraban “curriculum vitae” con datos personales, dirigidos tanto a ésta empresa como a V SHOES DAM, S.L. Ambas empresas, bajo una misma propiedad, denunciaron el robo en sus instalaciones de cuatro ordenadores y diversa

documentación fiscal de ambas compañías, pero si que constase denunciada la desaparición de los currículum. La Agencia Española de Protección de datos por tanto aclara en los fundamentos de Derecho de dicho proceso sancionador: "*Así las posibles medidas de seguridad establecidas por ambas entidades resultaron insuficientes desde el momento que no echaron a faltar la documentación que apareció en la vía pública hasta que la Policía les refirió los hechos, lo que demuestra negligencia en la actuación de dichas entidades, que descuidaron la documentación"*. Por tanto se refiere, a un incumplimiento de las medidas de seguridad, pero a nuestro parecer la sanción no debería limitarse sólo a ello, sino que debería ir más allá, ya que seguramente no se realizó ningún tipo de notificación de fichero, sobre la obtención de datos de carácter personal por parte de las empresas en los procedimientos de selección personal. El presente suceso y su posterior procedimiento sancionador dio lugar indudablemente a una sanción económica para cada empresa como bien indica el director de la Agencia: *El Director de la Agencia Española de Protección de Datos RESUELVE:*

> *PRIMERO: IMPONER a la entidad DISTRIBUCIONES MALABO 2000, S.L., por una infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de dicha norma, una multa de 6.000 € (seis mil euros), de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica.*
>
> *SEGUNDO: IMPONER a la entidad V SHOES DAM, S.L., por una infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de dicha norma, una multa de 6.000 € (seis mil euros), de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica.*

En cuanto a la cesión del curriculum a terceras empresas, incluso cuando estas formen parte del grupo empresarial, ha de constar expresamente el consentimiento del interesado o candidato en su propio curriculum o mediante la entrega de un formulario al interesado contemplando dicha cláusula de consentimiento en la cumplimentación de su curriculum.

Así lo ha demostrado la Agencia de protección de datos en el procedimiento sancionador PS/00239/2007 por el cual D.M.M.M presenta denuncia contra MANAGMENT HOTERLO PIÑERO S.L. En el citado proceso dicha empresa cedió el curriculum a BAHÍA PRINCIPE CLUB & RESORTS. La empresa MANAGMENT HOTELERO PIÑERO alegó que nunca hubo una solicitud oficial del curriculum sino que el hecho deriva de una comunicación privada entre dos personas. De este modo el Director de la Agencia de Protección de Datos acabó resolviendo: "*En el presente procedimiento se imputa a Management Hotelero Piñero, S.L. la infracción del deber de secreto contenido en el artículo 10 de la LOPD". "Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los*

titulares de los mismos". "El deber de secreto es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente, como el teléfono de contacto, no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto". "El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento".

Y acaba resolviendo:

PRIMERO: IMPONER a la entidad MANAGEMENT HOTELERO PIÑERO, S.L., por una infracción del artículo 10 de la LOPD, tipificada como grave en el artículo 44.3.g) de dicha norma, una multa de 60.101,21 € (sesenta mil ciento un euros con veintiún céntimos) de conformidad con lo establecido en el artículo 45.2 y 4 de la citada Ley Orgánica.

4.3 La contratación del empleado y el tratamiento de los datos especialmente protegidos

Primeramente hay que afirmar, como indicamos anteriormente que llegados a este punto, al existir una relación negocial, no haría falta el consentimiento del trabajador según lo señalado en el artículo 6.2 de la LOPD. Pero por otro lado, hay que dejar claro, que la existencia de ese consentimiento tácito en este sentido, no implica que el trabajador deba otorgar su consentimiento sobre servicios indirectamente o incluso, directamente relacionados con la empresa (ej. descuentos de viajes ofrecidos por otra tercera compañía a esa empresa en concreto) para la cual sería necesario u nuevo consentimiento. De igual modo, e indudablemente habrá que notificar cumpliendo el deber de información por parte de la empresa, de todos aquellos nuevos tratamientos que se lleven a cabo con carácter posterior al nacimiento de la relación laboral.

En cuanto a los datos especialmente protegidos, como bien sabemos, se tratan de datos que por su naturaleza religiosa o ideológica, o bien por pertenecer al núcleo más intimo de la persona resultan merecedores de una especial protección. Por lo tanto la empresa o empresario ha de disponer procedimientos dirigidos a garantizar:

- Un adecuada información del procedimiento de recogida de datos, ya que en este tipo de datos, la exigencia de esta información es de mayor importancia por el tipo de dato que se recoge.

- Los procedimientos de recogida de estos datos ha de ajustarse a criterios de proporcionalidad y legitimación. Para que un empresario pueda incorporar en su fichero datos especialmente protegidos de saludo por ejemplo, aquel habrá de contar un servicio de prevención de riesgos laborales y un servicio médico, siempre y cuando el conocimiento de esos datos médicos sean necesarios para el desempeño de su trabajo. Además, en cuanto al conocimiento de estos datos los responsables de la gestión de personal se limitaran al conocimiento de apto o no apto de dicho trabajador.

Si la inclusión de dicho datos especialmente protegidos relativos a la salud primordialmente, da lugar a un problema de gestión en cuanto a sus medidas de seguridad, siempre se le puede recordar al empresario, que puede segregar los datos de carácter personal de nivel alto para aplicar medidas de seguridad de nivel alto a este tipo de datos.

En cuanto a procedimientos sancionadores en este ámbito, es de especial relevancia el caso de una denuncia por parte de los trabajadores por una la cesión de datos especialmente protegidos de salud de la CAJA DE AHORROS LAYETANA (en concreto su Comité de Seguridad y Salud) a la empresa GABINENTE EVALUADOR S.L., y si existe vulneración del artículo 7.3 de la LOPD, o los hechos son lícitos de acuerdo al artículo 20.4 del Estatuo de los Trabajadores, sin infringir la dignidad humana. Se trata del procedimiento PS/00350/2009:

Por un lado el GABINETE MËDICO EVALUADOR alega: "*Las visitas realizadas desde GABINETE MEDICO EVALUADOR a los trabajadores de CAIXA D'ESTALVIS LAIETANA han sido siempre efectuadas por médicos, sujetos al secreto profesional, y orientadas a valorar su estado de salud, ofreciendo si era necesario una segunda opinión médica y actuando como Servicio Médico Complementario. Cuando, en algunos pocos casos, ha sido preciso determinar la justificación de la baja laboral o su duración prevista, a efectos de suplencia del paciente, nunca se ha transmitido información alguna que pudiera comprometer la confidencialidad de sus datos. Todo ello puede ser acreditado, en fase probatoria, mediante documentación que avala nuestra actuación, siempre orientada a valorar y mejorar el estado de salud de los pacientes.*

Por otro lado la parte demandante alega: *"el nudo gordiano a estimar para decidir si ha existido infracción legal o no, reside en la libre disposición, y uso posterior de los mismos sin control por parte del ciudadano al que se refieren (...) lo que causa tanto una injerencia indebida en la esfera íntima de dicho trabajador/a protegida constitucionalmente como derecho fundamental, como un lucro indebido para el empresario contratante". "Un tercer y último elemento sería, por la especificidad del tratamiento sanitario, y la confidencialidad de los datos del diagnóstico médico, la*

decisión del Ministerio de Sanidad, única entidad, de la Administración Pública, habilitada para conceder las prestaciones de Seguridad Social de origen sanitario, de no facilitar a los empresarios en el parte médico de IT común, el diagnóstico que efectúa el funcionario público competente de dicho Ministerio que concede la prestación. (...)El contrato suscrito entre Gabinete Médico Evaluador SL y Caixa d'Estalvis Laietana es un contrato mercantil y que por tanto, su contenido sólo vincula a las partes firmantes. (...) No se informa a los trabajadores/as de que se facilitan estos datos personales a Gabinete Médico Evaluador SL, a los efectos de que los trabajadores/as puedan ejercer su derecho de acceso, rectificación, cancelación,etc. (...)Tampoco se informa a los trabajadores/as de que utilización realizará Gabinete Médico Evaluador SL con los datos personales y médicos. "No sería admisible el argumento de Caixa Laietana de que estos datos son fundamentales que los tenga Gabinete Médico Evaluador SL para poder ejercer su derecho del artículo 20.4 del ET, ya que el contactar con los trabajadores/as para citarlos a los efectos de realizar el pertinente reconocimiento médico lo puede hacer perfectamente Caixa Laietana con sus propios medios, y sino lo hace es por una mera cuestión de costes, pero no de imposibilidad, con lo cual dicho argumento no sería admisible".

Los fundamentos jurídicos aportados por la Agencia se resumen en : "*la posibilidad de admitir un consentimiento expreso que no conste por escrito para el tratamiento de los datos de salud, debe subordinarse a que pueda acreditarse que es una manifestación de voluntad libre, inequívoca y específica que se presta previo el conocimiento de una concreta información entre la que necesariamente ha de constar la finalidad determinada y explícita del tratamiento de que sean objeto los datos personales del afectado. Lógicamente, la concurrencia de los extremos expuestos deberá constatarse en cada caso concreto". "En este caso lo que se imputa es que la finalidad del tratamiento de datos personales de salud de los trabajadores es, además de la puramente médica, la elaboración de un fichero sobre absentismo laboral en cumplimiento del contrato suscrito, razón por la que este tratamiento está excluido de la habilitación basada en el artículo 7.6 de la LOPD.*

"Por otro lado, Caixa d'Estalvis Laietana ha informado a sus trabajadores, mediante comunicado incluido en la intranet corporativa, de la prestación de servicios de realiza GME y de cual es la finalidad del mismo.

Teniendo en cuenta lo expuesto, se considera que no se ha vulnerado el principio del consentimiento para el tratamiento de los datos personales de salud de los trabajadores de la Caixa d'Estalvis Laietana"

"En la inspección realizada por la Inspección de esta Agencia a GME, se accedió al fichero en el que la empresa registra los datos de carácter personal de los trabajadores de Caixa Laietana, donde se comprobó que se incluían referencias a la enfermedad del trabajador o al tratamiento médico prescrito y valoraciones realizadas por el facultativo que

le ha atendido. La alegada Ley de Autonomía del Paciente, dispone sobre la conservación y gestión de los datos presentes en la historia clínica de los pacientes. En este caso, lo que Gabinete Médico no presentó a los inspectores de la AGPD, fueron los informes remitidos a Caixa Laietana que justificaran los servicios prestados y que, según sus manifestaciones, "se remite vía fax un informe en el que no se incluyen valoraciones médicas ni diagnósticos, tan sólo una valoración del gabinete acerca de si la baja está o no justificada".

En ningún momento se ha acreditado en este procedimiento, que Gabinete Médico remita informes médicos de los trabajadores de Caixa Laietana como se expresa en la alegación."

Y acaba resolviendo el Director de la Agencia:

***ARCHIVAR** las actuaciones practicadas contra GABINETE MÉDICO EVALUADOR al no quedar acreditada la vulneración del artículo 7.3 de la LOPD.*

En mi opinión, siempre es difícil conjugar como veremos en casos posteriores, el derecho a la intimidad del trabajador con la potestad de vigilancia que tiene el empresario sobre el trabajador con el fin de verificar de que este realiza efectivamente su trabajo. Creo a mi juicio que en este sentido, no cabe alegar el artículo 20.3 del Estatuo de los trabajadores en este caso, pues aunque exista esta potestad de vigilancia nunca debe extenderse a la potestad de recabar datos relativos a la salud con el fin de verificar un buen ejercicio de la actividad laboral. Dicha norma (el artículo 20.3 del Estatuto de los trabajadores no fue elaborada para dichos supuestos), y como bien indica el articulado, el recabar este tipo de datos con objeto de vigilancia de sus trabajadores (aunque sea para tratar a los enfermos de la empresa, y así, aligerar su recuperación), viola el derecho a la intimidad e indirectamente la dignidad humana, no ajustándose la recogida de dichos datos al principio de proporcionalidad.

En el caso concreto que nos ocupa, cierto es que los informes remitidos por Gabinete Médico SL son de carácter procedimental, es decir, "si la baja esta justificada o no", sin hacer mención a informes médicos con datos de carácter personal especialmente protegidos, lo que le excluye de la aplicación todo lo relativo a datos especialmente protegidos. He de corroborar las argumentaciones del Director de la Agencia en cuanto a la no aplicación del artículo 7.3 de la LOPD, ya que la redacción de dicho artículo va dirigido a la recogida de información sanitaria en beneficio del afectado, para su propia asistencia sanitaria, y así facilitar los procesos de urgencia médica; y nunca para crear un fichero de absentismo laboral.

4.4 El "Whistlebowling"

También denominado sistema interno de denuncias, en el cual vigilar la correcta utilización de los datos de carácter personal es muy importante, debido a que la mala utilización de estos y la vulneración de la confidencialidad puede dañar la reputación de algún miembro dentro de la empresa. Este sistema de denuncia esta compuesto por un “buzón interno”, normalmente "online", que pone de manifiesto conductas contrarias a las normas de conducta de la Empresa recogidas incluso en sus Códigos de conducta, e incluso en ocasiones también se recogen conductas contrarias a la ley. Dichas conductas puede referirse incluso a auditores de la empresa o directivos de la misma.

Al tratarse de un ámbito muy delicado, el deber de información al empleado de la existencia de este tipo de sistema de denuncias ha de hacerse mediante circulares de la empresa o bien ha de constar explícitamente en el contrato laboral, así como el tratamiento que se va a realizar de los datos que se obtengan de dicho sistema de denuncias.

En cuanto a las denuncias, han de respetar siempre el principio de proporcionalidad, es decir, siempre han de haber una concordancia entre el hecho denunciado y la empresa, de manera que los datos aportados han de ser los imprescindibles y no excesivos para describir el hecho denunciado y la persona denunciada, que haya infringido la ley o las normas de conducta de la empresa.

En cuanto a la cesión de los datos de carácter personal, en los casos en que dicho sistema de denuncias se externaliza, el denunciante como el denunciado deberán ser debidamente informados, incluyendo la posible transferencia internacional de datos a otras empresas del Grupo.

La protección de datos que abarca este mecanismo, se ha de realizar de manera distinta entre el denunciante y el denunciado. Es decir, la denuncia es válida sin con los datos aportados se ha podido identificar al denunciado, y por otro lado, sólo es válida la denuncia del denunciante si se conocen los datos de este, no cabiendo la posibilidad de denuncias anónimas. Además al denunciado nunca se le podrá facilitar los datos del denunciante. Del mismo modo, el denunciante debería poder ejercer su derecho de rectificación, cancelación y oposición sin que implique facilitar los datos de aquel al denunciado, al igual que el denunciante ha de saber en todo momento el dato que motiva la denuncia, con el fin de poder defenderse lo antes posible.

En cualquier caso, puede realizarse medidas cautelares extra para este tipo de datos debido a la importancia del deber de secreto de estos.

Por último, los ficheros creados con este fin deberán ser notificados al Registro General de la Agencia de Protección de Datos.

5. Los controles empresariales

En la actualidad este apartado, es el que más alarma social ha creado. Dado que el empresario en ocasiones abusa de su poder de vigilancia que le otorga el Estatuto de trabajadores, han aparecido en diversos medios de información conductas ilícitas que implican una violación del derecho a la intimidad y al derecho al honor. La legalidad del control de vigilancia por parte del empresario viene recogido en el artículo 20 del Estatuto de los Trabajadores que indica en sus apartados 3 y 4:

"*3.El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.*

4. El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones"

Como sabemos el uso de las tecnologías de la información en beneficio del empresario da lugar a un mayor repercusión en los derechos del trabajador. La manifestación puede realizarse a través de redes sociales, videovigilancia, correo electrónico e incluso el absentismo laboral puede controlarse a través de la huella dactilar.

La aparición de todas estas tecnologías de la información da lugar a que se tenga más en cuenta los derechos fundamentales de los trabajadores, lo que da lugar a que el uso de estas tecnologías de la información sea siempre proporcionales y respeten su dignidad, su derecho a la protección de datos y su vida privada.

Para ello la Agencia de protección de Datos Española ha seguido unos principios de plena aplicación en este ámbito y son:

- La legitimación para el tratamiento deriva de la existencia de la relación laboral y, por tanto, de acuerdo con el artículo 6.2 LOPD, no se requiere del consentimiento.
- A la hora de decidir adoptar una medida de control que comporte un tratamiento de datos personales debe aplicarse el principio de proporcionalidad.
- Debe existir una finalidad que, en este caso, no puede ser otra que la establecida por el artículo 20.3 del Estatuto de los Trabajadores de «verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales».
- Los datos que se obtengan y almacenen deberán ser exactos y puestos al día y no podrán conservarse más tiempo del necesario. Se recomienda a los empleadores fijar un plazo de conservación.
- Debe cumplirse con el deber de información a los trabajadores. Este deber resulta

particularmente relevante cuando se trate de controles sobre el uso de Internet y/o del correo electrónico. (El uso de Internet será objeto de análisis posteriormente)

En todo caso, la información previa y su prueba es esencial, ya que estos tratamientos no requieren el consentimiento del trabajador y son manifestación de los poderes de control del empresario.

5.1 Redes Sociales en el ámbito laboral

Quizás este sea uno de los puntos mas controvertidos en el presente trabajo de investigación ya que es de rigurosa actualidad, y más aún en el Derecho Comparado. Su controversia se debe a la utilización de métodos de dudosa legalidad por parte de las empresas y sus departamentos de recursos humanos para conocer más aún sobre los empleados, vulnerando en ocasiones el derecho a la intimidad de los candidatos. Ello es debido a la aparición de las redes sociales y la utilización de los departamentos de recursos humanos para obtener información de sus candidatos con o sin consentimiento de estos.

Por un lado, parte de la doctrina ve claramente la violación del derecho de la intimidad de los empleados, y en cambio otros, opinan que el acceso a los perfiles de los candidatos en las redes sociales es completamente lícito siempre y cuando se haga mediante mecanismos legales, ya que en este caso, el propio candidato mediante las herramientas de la propia red social, permite o no el acceso a su perfil, y por tanto a su intimidad.

Caso distinto, es utilizar mecanismos fraudulentos para engañar al candidato, solicitándole acceso a su perfil suplantando la identidad de una persona inexistente, lo cual no sería en mi opinión,"real" suplantación de identidad, aunque dicha persona no existiese.

Para analizar este tema y los problemas que ha generado, haremos un breve comentario sobre dicha situación en el Derecho Comparado.

5.1.1 Derecho Comparado

El caso más llamativo se ha dado sin ninguna duda en Alemania, tras los escándalos de Deutsche Telekom y Lidl, y actualmente investigando a Google por almacenar información obtenida de las fotografías realizadas para el servicio de Street View y han realizado un requerimiento a Apple en relación a la conservación de datos obtenidos a través del iPhone. . En dicho país, ante el uso masivo por parte de los empresarios de las redes sociales como medio de vigilancia de sus empleados ha dado lugar a que la cancillera Angela Merkel haya promulgado la que es conocida como la "Ley

Facebook".

Dicha ley, además de prohibir por parte del empresario grabaciones secretas a los empleados en su puesto de trabajo, salvo en determinadas áreas, y la legitimación de investigación a aquellos empleados que resulten sospechosos de un delito, pretende acabar con los usos por parte de los empresarios de acudir a las redes sociales en busca de las costumbres de sus empleados fuera del ámbito laboral, violando el derecho a la intimidad de estos, y sólo permite el acceso a redes sociales por parte de los empresarios sobre sus empleados en redes como Linkedin, de ámbito estrictamente profesional.

Parte de la doctrina no encuentra sentido a la "Ley Facebook", ya que ningún empresario puede alegar causa de despido algo que haya encontrado en la red social del empleado. En mi opinión, esto es cierto, pero no impide que el empresario pueda utilizar datos de carácter personal como indicios para destapar o potenciar una característica de la persona que se produce fuera del ámbito laboral, y hacer que se refleje dentro del ámbito laboral dentro del marco de las causas de despido. Y por tanto encuentro dicha ley como una ley preventiva más que sancionadora. No sólo por lo argumentado anteriormente, sino que la "Ley Facebook" servirá no sólo para "frenar" el control excesivo de los empresarios sino también para limitar el uso de estas redes sociales a la hora seleccionar candidatos para un puesto de trabajo. Y así lo señala bien claro la ley en su exposición de motivos:

"Para los datos guardados en las redes sociales, que sirven a la comunicación, prevalece el interés del usuario, digno de ser protegido".

El problema realmente en Alemania surge porque mientras representantes del Gobierno alemán defienden la medida como progresista en el ámbito de la protección de datos, los expertos indican que su aplicación práctica va a ser muy difícil, ya que que no se pueden comprobar las fuentes de información de un empleador. . Expertos alemanes aseguran que la única manera de evitar la intromisión en la vida privada del empleado es, o no utilizando Facebook, o no introduciendo en el datos de carácter personal.

5.1.2. Derecho Español

Las reacciones en España en lo que se refiere a la "Ley Facebook" han sido diversas, aunque aún no ha habido ningún tipo de iniciativa a implantar una ley parecida en este país. Es conocida las investigaciones que la Agencia de Protección de Datos ha realizado sobre Facebook, y ante dicha "Ley Facebook" el director de la Agencia se ha mostrado a favor de su aplicación indicando:

"Internet no puede ser un territorio sin ley. Si en el mundo real no sería lógico que un

empresario vigilase, por ejemplo, las llamadas de teléfono, lo mismo cabe el mundo virtual".

Por otro lado parte de la doctrina es reacia a la aplicación de dicha ley en España, por ejemplo, Javier Prenafeta, abogado especialista en Tecnologías de la Información, señala que:

"*Estrictamente, el uso para fines laborales de datos depositados en redes sociales requeriría de autorización debido a la normativa de protección de datos y a las condiciones de uso de Facebook, que limita el uso de la información a la propia red social".* Y por tanto, no sería necesaria la aplicabilidad de la "Ley Facebook" debido, a que la propia red social ya posee sus propios mecanismos de control de la privacidad.

La situación actual generalizada en España es de rechazo ante la posibilidad de que el empresario pueda vigilar la actividad de su empleado fuera del ámbito laboral. A la mayoría de los empleados se cuestionan "agregar como amigo" en Facebook a su jefe o incluso a otro empleado.

Dada la situación de rechazo que estamos viviendo, y la falta de aceptación de incluir las redes sociales en nuestro ámbito laboral. Empresas como Job and Talent S.L, la cual ha publicado una bolsa de trabajo en www.jobandtalent.com pretende crear un nuevo modelo de negocio. Dicha empresa crea una bolsa de trabajo, en la cual, el curriculum de los trabajadores esta unido a su red social. El método es sencillo, jobandtalent mediante las herramientas de Facebook "pasa a ser tu amigo", por lo que tu curriculum y perfil de la red social pasa a ser visible por todas las empresas que el candidato desee. De esta manera, dado que las empresas buscan la máxima transparencia de sus empleados y candidatos, y dado que estos son reacios a ella, jobandtalent pretende premiar a todos aquellos candidatos a los que no le importa ser totalmente transparentes hacia su empresa dentro y fuera del trabajo, sin que tengan nada que ocultar.

En mi opinión sobre la aplicabilidad de una "Ley Facebook" semejante en España, habría que establecer un desarrollo legislativo concreto en la ley o convenio colectivo que proceda, y así dotar de una mayor seguridad jurídica a estas situaciones, para así no acabar con las "lagunas legales" existentes en estas materias. De hecho, la solución más adecuada y práctica sería establecer esta seguridad jurídica a través de convenios colectivos debido a su flexibilidad.

En este sentido, el propio Director de la AEPD ha señalado que para dotar de mayores garantías jurídicas habría que llegar a acuerdos entre trabajadores y empresarios que recojan la amplia gama de casuística que puede darse, teniendo su marco estos acuerdos en los convenios colectivos. En efecto, tal marco legal o de concertación social permitiría una negociación y posiblemente una solución equilibrada a los derechos del empresario y a la privacidad de los trabajadores.

5.2 Videovigilancia en el trabajo

Se trata de uno de los temas de rigurosa actualidad, y ello es así porque existe una clara

colisión entre los derechos fundamentales del trabajador referidos a su honor y a su intimidad como la potestad que le otorga el Estatuto de los Trabajadores a al empresario para que pueda vigilar a sus empleados.

A favor del empresario existe el artículo 20 del Estatuto de los Trabajadores, que garantiza al empresario el empleo de las tecnologías de información,. El uso correcto por parte del empresario puede resultar muy útil ya que, como dice el artículo, supone un método para verificar el cumplimiento por el trabajador de sus obligaciones. Así, se podrá conocer su aprovechamiento, si es útil para la organización, en definitiva, si cumple con sus deberes reflejados y firmados en su contrato de trabajo, motivos por los cuales fue contratado.

Por otro lado, hay que destacar que **l**a LOPD, cuyo artículo 6 establece la necesidad de consentimiento del afectado en cuanto al tratamiento de datos de carácter personal que se efectúen sobre éste. No obstante, el apartado 2º de dicho artículo refleja: *"No será preciso el consentimiento cuando los datos de carácter personal [...] 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 [...]".*

De todas formas, esto no da derecho al empresario por sí solo al tratamiento de las imágenes. Debe informar debidamente a los trabajadores del centro donde se deseen instalar cámaras de dicha medida y acatar el mandato del artículo 4.2 LOPD de no poder utilizar los datos recogidos en los dispositivos para fines distintos.

En cualquier caso, hay que delimitar que es dato de carácter personal a efectos de la aplicación de la LOPD en el ámbito de la videovigilancia en el trabajo. En efecto, las **i**mágenes y sonidos son, a efectos de protección de datos, datos de carácter personal, y por tanto información personal, pues permiten la identificación total o parcial de la o las personas físicas que aparecen en dichas imágenes. Y más aún al tratarse de imágenes tomadas en el lugar de trabajo ya que siempre aparecerán las mismas personas, en este caso, aquellos trabajadores en su lugar de trabajo, lo que les hace perfectamente identificables.

En cuanto a la videovigilancia la Agencia Española de Protección de Datos ha dictaminado en la Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videovigilancia. En la cual señala que es de aplicación al tratamiento de los datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras, y comprende tanto la grabación, captación o transmisión, así como la conservación y almacenamiento de imágenes

Por otro lado, no es necesario y como consecuencia obligatorio especificar el lugar concreto

de la instalación porque en parte perderíamos la esencia de la finalidad intrínseca de la vigilancia. Sin embargo, ello no impide el deber de información a los trabajadores de la existencia de dichas cámaras y el correspondiente cartel de que dicha zona dentro del ámbito laboral está siendo grabada.

Además, la videovigilancia debe centrarse únicamente en imágenes no estando permitido en caso alguno la grabación de conversaciones que, aun en el puesto de trabajo, siguen siendo consideradas por ley como privadas. Y ello es así, debido a la influencia de los tribunales civiles y penales que consideran la grabación de las conversaciones como una intromisión en la intimidad de las personas, mientras que la mera reproducción de imágenes no lo es, aunque existen excepciones.

Por todo ello, la instalación de cámaras de videovigilancia en el lugar de trabajo está permitido siempre y cuando se cumpla con la normativa aplicable, y en particular, siempre que dicha instalación sea llevada a cabo por una finalidad que no pueda obtenerse mediante otros medios que resulten menos intrusivos para la finalidad de las personas. De esto modo, estaríamos respetando el artículo 20.3 del estatuto de los trabajadores ya que al indicar: *"la aplicación la consideración debida a su dignidad humana",* y por tanto se habría hecho todo lo posible por dañar lo menos posible tanto la dignidad del empleado como su esfera íntima.

Para encontrar la delimitación entre ambos derechos, hemos de analizar los informes jurídicos y resoluciones que ha realizado la Agencia de protección de datos, para observar en cada caso concreto el excesivo uso de la videovigilancia que vulnera los derechos fundamentales del trabajador, y como la Agencia de Protección de Datos ha ido definiendo el campo de la videovigilancia en el trabajo.

En primer lugar, una consulta realizada en el 2001 relativo a la videovigilancia en el trabajo, por la cual se planteó si resulta conforme a lo establecido en la LOPD la instalación de cámaras para el control de la actividad de los trabajadores de la entidad consultante.

Como puntos fundamentales, indica la necesidad de declarar el fichero haciendo referencia a que se trata de un fichero de datos de carácter personal referidos a videovigilancia, y así lo indica: *"será necesario que dichos datos se encuentren incorporados a un fichero, definido como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", por el artículo 3 b) de la Ley".* La declaración de dicho fichero, será necesario siempre que existan imágenes de la persona que aparecen en ellas siempre y cuando estas sean identificadas o identificables para estar amparadas dentro de la aplicación de la LOPD y así lo indica el informe: *"debe indicarse que las imágenes a las que se refiere la consulta sólo podrán ser consideradas datos de carácter personal en caso de que las mismas permitan la identificación de las personas que aparecen en dichas imágenes, no encontrándose*

amparadas en la Ley Orgánica en caso contrario.

Así, en supuestos en que las imágenes se tomaran del lugar de trabajo sí se produciría dicha identificación, dado que siempre aparecerían en las mismas los trabajadores de la empresa en su lugar de actividad (lo que les hace perfectamente identificables).”

El segundo informe destacable es el Informe 0006/2009 sobre la adecuación a la normativa de protección de datos de la instalación de cámaras de videovigilancia en un centro de trabajo.

El primer punto al que hace referencia es al consentimiento inequívoco por parte del trabajador para la grabación de su identidad. Dicho consentimiento viene recogido en la LOPD en su artículo 6.1 y 6.2, aplicándose el régimen general en cuanto a consentimiento se refiere como si de otro dato de carácter personal se refiere, y así lo indica el informe: “*donde se establece que* ***“el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”****, sin perjuicio de que dicho consentimiento podrá quedar excluido, de acuerdo con lo dispuesto por el artículo 6.2 cuando, el tratamiento sea necesario para el adecuado desenvolvimiento de la relación laboral de los trabajadores con la empresa.* Lo discutible aquí podría ser, la excepción al adecuado desenvolvimiento de la relación del trabajador, es decir, cuando se considera adecuado y cuando no, en cuyo caso, habría que ir caso por caso.

Este consentimiento afirma la Agencia de Protección de Datos puede ser prescindible. Pero nunca el deber de información, para aquellos que casos en los que el tratamiento sea excluido de consentimiento. Para ello, y no dar un poder discrecional al empresario, la Agencia de Protección de Datos intenta reforzar la importancia del deber de información con argumentos jurisprudenciales y así lo afirma: *“La Audiencia Nacional ha señalado en sentencia de 15 de junio de 2001 que ”se trata de un derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos, y así lo valora el texto positivo al pormenorizar su contenido y establecer la exigencia de que el mismo sea expreso, preciso e inequívoco.”* Además recuerda la existencia del artículo 4.2 de la LOPD señalando que “*los datos no podrán ser utilizados para fines distintos”.*

La importancia de este deber de información en la videovigilancia toma especial relevancia, y la Agencia de Protección de datos señala que le es aplicable de igual modo todo el artículo 5.1 relativo a los requisitos que ha de cumplir el deber de información. Pero no sólo eso, sino que ese deber de información habrá de aplicarse no sólo a cada trabajador individualmente, sino que por otro lado y cumpliendo la legislación laboral : *“exigirá su comunicación a los representantes de los trabajadores, en tanto que el artículo 64.1 ET dispone que “El comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores…”* y como indica el informe el punto 5 de dicho artículo del Estatuto de los Trabajadores: *“ El comité de empresa tendrá derecho a emitir informe, con carácter previo a la ejecución por parte del empresario*

de las decisiones adoptadas por éste, sobre las siguientes cuestiones:

f) La implantación y revisión de sistemas de organización y control del trabajo, estudios de tiempos, establecimiento de sistemas de primas e incentivos y valoración de puestos de trabajo."

De igual modo, el informe no olvida que han de cumplirse todas las formalidades respectivas a la videovigilancia con carácter general, y más concretamente la modalidad de información en materia de videovigilancia que recoge el artículo 3 de la Instrucción 1/2006.

Por último, el Informe 0495/2009 referente a la videovigilancia analiza varias cuestiones. Pero a efectos del ámbito laboral es destacable sólo algunos puntos de dicho informe. En primer lugar, no puede aplicarse las mismas disposiciones del Estatuto de los Trabajadores a los funcionarios públicos y por tanto y como bien indica el informe: *"No existe para los empleados públicos una norma correlativa al artículo 20.3 del Estatuto de los Trabajadores en la Ley 7/2007,de 12 de abril, del Estatuto Básico del Empleado Público, por ello, no existe legitimación para controlar la actividad laboral de los empleados públicos",* por lo que no podría utilizarse cámaras de videovigilancia para el control de los funcionarios. Más tajante es aún al referirse a la grabación de comunicaciones realizadas por parte de los funcionarios públicos y determina: *"Además se carece de legitimación para grabar todas las conversaciones, siendo una cuestión muy vinculada con el secreto de las comunicaciones".* La Agencia podría terminar sus argumentos con la vulneración del secreto de las comunicaciones como derecho fundamental pero además afirma que el hecho de realizar la grabación de escuchas telefónicas *"se efectúa por razones de seguridad y control del correcto desempeño de la función pública. Sin embargo estas razones no superan el juicio de proporcionalidad exigido por el Tribunal Supremo".*

En cuanto a los Cuerpos de Fuerza y Seguridad del Estado como estamento del funcionariado público, indica el informe que se regirá por ley especial ya que la LOPD prevé que la aplicación de otras leyes especiales cuando se traten de sectores con normativa propia. Aunque aclara que la Agencia de Protección de Datos que no tiene competencia sobre este tema, afirma: "*según la finalidad declarada en el Registro General de Protección de Datos, el fichero creado es para controlar y vigilar el acceso al edificio, por ello, si las responsabilidades disciplinarias, fueran derivadas del acceso al mismo (horario de entrada y salida por parte delos policía) sí podrían ser utilizadas, no pudiendo ser utilizadas para otro tipo de finalidades, que no consten declaradas",* abogando en todo momento por la uso de los datos para la finalidad correspondiente.

En definitiva, se la línea seguida por la Agencia de Protección de Datos es consentir la grabación por videocámaras como potestad por parte del empresario siempre y cuando haya un consentimiento inequívoco o bien un deber de información con todas las garantías y especialmente reforzado.

5.3 Control del correo electrónico por parte de los empresarios

En primer lugar, las diferencias entre el correo postal y el electrónico no pueden ser relevantes en cuanto a su incidencia en la protección a la intimidad. El secreto postal, se configura, en consecuencia, como un derecho derivado del derecho al secreto de las comunicaciones. La cobertura del precepto constitucional sobre el correo electrónico no parece dar lugar a duda puesto que, hay que tener en cuenta que se protege el secreto de la comunicaciones con independencia del medio utilizado.

La problemática que se plantea en torno al uso de Internet y el correo electrónico se manifiesta en un doble ámbito: en el acceso a la red a través de los medios de producción de la empresa con fines extraproductivos para enviar, recibir, consultar o almacenar información y en el propio contenido de la información o de los mensajes que a través de este medio se intercambian.

Dicho esto, habría que diferenciar entre un acceso productivo (contacto con clientes o proveedores, comunicación interna de la empresa, búsqueda de información sobre el sector o sobre información económica general, etc.) y un acceso no productivo, donde se incluye el acceso a Internet con fines privados (sean éstos lícitos o ilícitos), encuadrándose aquí tanto el envío de comunicaciones privadas (e-mail) como el acceso a páginas de información general no vinculada a la empresa, o incluso a páginas prohibidas, juegos on-line etc.

Al existir estos dos tipos de accesos, se crea una colisión de derechos por parte del empresario y del trabajador. Mientras que el segundo, opinará que su utilización es lícita y esta protegida por el derecho al secreto de las comunicaciones que está especialmente protegido en el contenido del artículo 18.3 CE , el primero creerá que el uso no productivo es provocado por un “abuso de confianza”. Esta colisión de derechos se produce porque envío y recepción de mensajes de correo a través de medios informáticos como son los ordenadores, son propiedad del empresario puestos a disposición de los trabajadores en el marco de la relación laboral, para que de los hechos se obtenga una producción laboral a favor del empresario.

Dada la peculiaridad de la situación, ha dado lugar a que la doctrina se divida en cuanto si el correo electrónico forma parte de la intimidad del empleado o no. Un sector de la jurisprudencia entiende que el principio constitucional no ampara las comunicaciones privadas realizadas a través del correo electrónico. Por tanto, no existe vulneración de este derecho constitucional en el ejercicio de las competencias de vigilancia y control reconocidas en el artículo 20.3 del Estatuto de los Trabajadores, sino por el contrario, una utilización indebida de los medios e instrumentos de la empresa para fines ajenos a los estrictamente laborales. Además se alega que la vigilancia de las comunicaciones en la empresa puede tener una finalidad legítima de control de la calidad del trabajo, posibilitando la

corrección de errores en el sistema productivo, así como una medida de protección y vigilancia ante actuaciones desleales del trabajador, como un uso particular de los elementos de la empresa, defraudaciones, acoso sexual, introducción de virus o espionaje industrial

Por otro lado, otros sectores de la doctrina y la jurisprudencia habían venido considerando al ordenador como un "efecto personal" del trabajador equiparándose a la taquilla o al resto de efectos particulares en la protección frente a los registros establecida en el artículo 18 del Estatuto de los Trabajadores, estableciéndose un principio general de prohibición de los registros, y autorizándose tan sólo excepcionalmente si existiesen sospechas de estar cometiendo un acto ilícito.

Por todo ello, el Tribunal Supremo ha tenido que dictar sentencia del 26 de septiembre de 2007 (Sala 4ª), dictada en unificación de doctrina, que ha dictaminado que el contenido del correo electrónico está protegido por el derecho constitucional al secreto de las comunicaciones, y el control que pueda hacer el empresario del uso que el trabajador haga del ordenador en el centro de trabajo puede vulnerar su derecho a la intimidad, cuya protección también se recoge en el artículo 18.1 de la Constitución y el Convenio Europeo para la protección de los Derechos Humanos.

La consolidación jurisprudencial se traduce en el hecho de que ahora será la empresa quién deberá establecer previamente las reglas de uso del correo electrónico, con aplicación de prohibiciones absolutas o parciales por parte del empresario, e informar a los trabajadores de que va a existir control y cómo va a realizarse. Mecanismos que deben ser compatibles con el respeto a la dignidad del empleado pues ha de cumplirse siempre el artículo 20.3 del Estatuto de los Trabajadores.

En mi opinión dichos controles han de hacerse siempre dentro de la negociación colectiva y a poder ser recogidos en el convenio colectivo.

5.4 El absentismo o ausentismo laboral, en particular los controles biométricos

Como bien sabemos, el empresario a través del Estatuto de los trabajadores posee las facultades y derechos necesarios para poder controlar a sus empleados, y así lo recoge el artículo 20.3 del Estatuto de los Trabajadores. Sin embargo, en esta ocasión la mayoría de controles sobre el absentismo laboral, lleva aparejado un tratamiento de datos relativos a la salud, lo que hace que estos deban de gozar de unas medidas de seguridad de nivel alto.

Por tanto, el tratamiento de datos de salud requerirá del consentimiento expreso del trabajador o de la existencia de una previsión legal que exima del mismo.

En primer lugar hay que dejar claro que las posibilidades de acceso de la empresa a estos datos

de salud y su utilización para fines distintos para los que fueron recabados resulta totalmente imposible ya que, la empresa únicamente puede conocer las condiciones de aptitud, y por tanto la incorporación de datos de salud a un fichero con la única finalidad de realizar controles del absentismo resulta desproporcionada. Podrá optarse porque ciertos ficheros contengan datos relativos a la salud y así conocer motivos por los que se da el absentismo laboral, pero en ningún momento la recopilación de los datos podrá ser únicamente de datos relativos a salud para poder así, reducir el absentismo laboral.

La elaboración de un fichero que contenga datos relativos a la salud únicamente para controlar el absentismo laboral no se ajusta al principio de proporcionalidad y así lo indicó el Tribunal Constitucional en su sentencia 202/1999 que señala: *"lo primero que conviene advertir es que entre dichas facultades no figura la de proceder al almacenamiento en soporte informático de los datos atinentes a la salud de los trabajadores -y en concreto del diagnóstico médico- prescindiendo del consentimiento de éstos. Por otra parte, y con independencia de ello, lo verdaderamente relevante es que la medida adoptada por la empresa, sometida a los cánones establecidos para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, no reviste la consideración de solución idónea, necesaria y proporcionada para la consecución del fin, en este caso, el control del absentismo laboral"* y además señala *"pues no se trata de medida de suyo ponderada y equilibrada, ya que de ella no se derivan más beneficios o ventajas para el interés general o para el interés empresarial que perjuicios sobre el invocado derecho a la intimidad*." La sentencia destaca que el principio de proporcionalidad no se ajusta, aunque exista consentimiento del trabajador, pues dicho consentimiento es independiente de la obtención de datos de carácter personal sobre datos relativos a la salud con el fin de controlar el absentismo laboral, ya sea sea proporcionado o no, ya que aunque exista consentimiento, puede vulnerarse el derecho a la intimidad.

En cualquier caso, mientras la obtención de datos relativos a la salud sea proporcional al control del absentismo laboral, por ejemplo, mediante el control relativos a la salud que señalen la aptitud o no aptitud del trabajador para desempeñar su trabajo; hay que señalar que en todo momento no existe obstáculo a que se persiga la doble finalidad de verificar el estado de salud del trabajador y controlar el absentismo. Pero, si existe un tratamiento relacionado con la salud deberá obtenerse el consentimiento expreso del trabajador.

En cuanto a los controles biométricos, la biometría permite registrar de manera automática determinados rasgos distintivos, irrepetibles, de una persona y convertirlos en formato digital. La implantación de estos controles biométricos se ha dado tanto en el ámbito laboral privado como en el público. En Cantabria lo utilizan ya algunas empresas y organismos públicos. Incluso en el local de CC OO hay un equipo biométrico que analiza la geometría de la mano de los empleados. Además el

Gobierno autonómico comenzó a aplicarlo en la Dirección General de Montes, en el año 2000, a modo de prueba.

El Tribunal Constitucional en 2007 se pronunció al respecto ratificando una Sentencia del Tribunal Superior de Justicia de Cantabria debido a una denuncia de un funcionario público en Cantabria. Donde el Tribunal Superior de justicia apreciaba proporcionalidad, estimando que la Administración puede optar por el sistema de control horario que considere más conveniente, siempre que se ajuste a la legalidad. De modo que, una vez cumplido el requisito de publicación en el BOE de la creación de la base de datos, los magistrados no ven más objeciones a su implantación.

En cuanto a la necesidad del consentimiento por parte del trabajador, será posible el tratamiento inconsentido, ya que el artículo 6.2 de la LOPD prevé que no será preciso el consentimiento cuando los datos "se refieran a las partes de un contrato o pre-contrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".

Sobre la huella dactilar existe un informe jurídico por parte de la Agencia de Protección de Datos respecto al tratamiento de la huella digital de los trabajadores. El citado informe indica: *"El problema consiste en determinar si el tratamiento de la huella digital puede ser considerado excesivo para el fin que lo motiva, atendiendo al principio de proporcionalidad consagrado por la Ley*" y que *"los mismos no contienen ningún aspecto concreto de la personalidad, limitando su función a identificar a un sujeto cuando la información se vincula con éste, su tratamiento no tendrá mayor trascendencia que el de los datos relativos a un número de identificación personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos".* En este sentido, y como argumentare a continuación, la afirmación "*no contención de aspectos de la personalidad"* no es absolutamente correcta, y tan sólo relativamente.

En mi opinión la polémica es importante, ya que los controles biométricos en la actualidad, dado el avance tecnológico no sólo son capaces de registrar los parámetros físicos para una identificación. Aparentemente, el sistema en cuestión, capta únicamente la longitud, anchura, grosor y superficie de la mano, pero determinados equipos biométricos pueden registrar parámetros que permitirían obtener datos del usuario (por ejemplo, acerca de la salud) cuyo uso por terceros podría acarrearle graves consecuencias.

Puede darse el caso, de que la obtención de dichos datos de salud puestos a disposición de entidades que tienen relación entre sí, donde cada una desarrolla una función diferente de la otra, puedan generar sobre una persona una plena identificación no sólo física, sino que pueden obtener un perfil en cuanto a tu salud se refiere, y por tanto, sobre aquellas enfermedades que tiene riesgo de padecer en un futuro. Ello, evidentemente, sería muy perjudicial para aquellas personas que pretenden contratar un seguro de salud o contrato hipotecario, pero son víctimas de esa enfermedad "potencial".

6. Prevención de Riesgos Laborales y Protección de Datos

Sin duda, la prevención de riesgos laborales lleva aparejada un tratamiento de datos de carácter personal de los trabajadores, incluso datos de los propios trabajadores pueden hacer referencia a su salud para poder evaluar y evitar ciertos riesgos laborales, por ejemplo, una persona que sea alérgica a determinados productos químicos que se desarrollen en un determinado laboratorio, será necesario su conocimiento para que no esté en contacto con aquellos.

En este caso, el consentimiento del empleado para el tratamiento de los datos de carácter personal no es "conditio sine qua non". La ley de Prevención de Riesgos Laborales contempla en su artículo 21.1: *" «El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo. Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento.(...)",* lo que otorga un consentimiento voluntario, pero sin embargo, esta vigilancia puede ser obligatoria conforme al artículo 21.1 de la Ley de Prevención de Riesgos Laborales, con la realización de un previo informe de los representantes de los trabajadores en aquellos casos en los que la realización de los reconocimientos sea necesaria para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para comprobar si el estado de salud del trabajador puede constituir un peligro para el mismo, o incluso, para los demás trabajadores o para otras personas relacionadas con la empresa. O también cuando así lo disponga una una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad.

En cualquier caso, no ha de olvidarse en ningún momento el deber de información al empleado sobre el tratamiento de sus datos, y hay que considerar siempre la existencia del principio de proporcionalidad entre los datos recabados y la prevención del riesgo que se pretenda.

En la actualidad, la mayoría de las empresas sub-contratan con empresas para que lleven a cabo la prevención de riesgos laborales, por lo que se constituye una cesión de datos de carácter personal. La condición de responsable del fichero o del tratamiento varía según se trate de un servicio de prevención propio, ajeno o mancomunado. Si se trata de un servicio propio la empresa, realizado por tanto por una empresa externa. será responsable del fichero que se genere para la gestión de la prevención. Así lo ha indicando el Informe 0299/2009 indicando que las empresas que actúan como servicios de prevención ajenos tienen la consideración de responsables del tratamiento.

Cuando se trate de prevención de riesgos laborales según recomendación de la Agencia de Protección de Datos habrá que tener en cuenta básicamente:

En primer lugar, los sistemas de información para la prevención de riesgos de seguridad

tendrán en cuenta:

- El nivel de seguridad. Que será alto en todos aquellos casos en los que se incluyan datos de salud con identificación precisa de las enfermedades, traumatismos etc., o se gestionan historias de salud laboral.
- Deberán definir de modo muy preciso los perfiles de acceso y las funciones de cada uno de los usuarios.

En segundo lugar, historia clínica del trabajador debe regirse además de por lo previsto en la Ley Orgánica de Protección de datos por los principios de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Por último, deben establecerse procedimientos para garantizar los derechos de acceso, rectificación y cancelación de los trabajadores.

Para concluir este apartado, en mi opinión la obtención de datos de carácter personal han de ajustarse en todo momento, como bien se ha indicado al principio de proporcionalidad, utilizando en la medida que se pueda conceptos como apto/o no apto para prevenir ciertas situaciones de riesgo y así proteger la intimidad del trabajador en la medida de lo posible.

7. Relaciones con los sindicatos y protección de datos

El hecho de desarrollar el derecho fundamental de libertad sindical requiere el tratamiento de datos personales, pues se establecen ciertos flujos de información entre los representantes sindicales y el comité de empresa.

A la hora de realizar una publicación amparada por el derecho a la libertad sindical como derecho fundamental, su publicación constituye un tratamiento que puede dar lugar al acceso a datos de carácter personal por terceras personas carentes de legitimación.

La prevalencia del derecho sindical como derecho fundamental sobre el derecho a la protección de datos de carácter personal ha sido claro en el recurso de reposición E/00729/2008 sobre el proceso sancionador de 19 de Diciembre de 2007 que indica: *"el derecho a la libertad sindical, (...) ha de prevalecer sobre el derecho a la protección de datos personales, cuando, como sucede en el caso examinado, la acción sindical ampara la actuación del sindicato recurrente para divulgar entre los trabajadores de los centros los datos precisos, y únicamente necesarios, para el entendimiento de la noticia, teniendo un conocimiento cierto de la información relevante desde el punto de vista sindical."*

De esta forma, la Agencia de Protección de Datos ha declarado varios aspectos para conservar en todo momento los datos de carácter personal de las personas afectadas:

- Será responsable del tratamiento de datos en el tablón de anuncios y por tanto de las informaciones publicadas en el mismo, aquél órgano u organización que decida sobre su uso y finalidad y sitúe materialmente la información en él.
- Debe considerarse el espacio físico o virtual concreto en el que se situará el tablón con la finalidad de que, en caso de contener información personal, ésta sólo resulte visible a los usuarios legitimados para consultarla.
- Es fundamental que los tablones sindicales "online" se sitúen en las intranet de la empresa, nunca en Internet.
- Debe tenerse muy en cuenta el principio de calidad desde el punto de vista de la proporcionalidad de los tratamientos y de la finalidad de los mismos.
- Es recomendable considerar la posibilidad de que los tablones impidan el acceso a la información por terceros no autorizados.

Sin embargo, la Agencia de Protección de Datos de la Comunidad de Madrid ha determinado que la cesión de datos a delegados de personal y Comité de Empresa sólo podrá producirse en el caso de que cada uno de los trabajadores afectados otorgue su consentimiento expreso, por lo que refuerza el derecho a la intimidad del trabajador por encima del derecho fundamental de libertad sindical.

En cualquier caso, podemos resumir que los datos de carácter personal en el ámbito sindical deberán ser siempre adecuados, pertinentes y no excesivos y vinculados siempre a la finalidad para la que se obtuvieron, no pudiendo ser empleados para fines distintos. Así, en consecuencia, los parámetros que deben emplearse para la recogida y manipulación de los datos tienen que ser la pertinencia, proporcionalidad y adecuación a un fin empresarial, legítimo y serio.

8. Conclusiones

Analizado detalladamente cada uno de los sectores donde el derecho fundamental de protección de datos y las relaciones laborales convergen, podemos concluir en primer lugar, la existencia continuada de una colisión entre los derechos que se generan en el ámbito laboral y el derecho fundamental de protección de datos.

Actualmente, tal y como esta contemplado hoy el derecho a la intimidad en nuestra Constitución, siendo un concepto que abarca incluso campos que van más allá de la estricta intimidad,

no parece dar lugar a duda de que la interpretación por los tribunales y por las Agencias de Protección de Datos sea en la mayoría de los casos, la correcta.

Si bien la aparición de nuevas tecnologías en el ámbito laboral, y particularmente las nuevas tecnologías referentes a tecnologías de la información, hacen que el derecho a la intimidad del trabajador se vea amenazado. Regular las nuevas tecnologías puede resultar satisfactorio, y en cierta medida resulta necesario.

Por otro lado es verdad , que resulta prácticamente imposible regular el uso de Internet dentro del ámbito laboral (como puede ser por ejemplo, el control de los empleados mediante el uso de Internet, o las redes sociales en el ámbito laboral). Cierto es, que la ley nunca ha podido ir por delante de los fenómenos sociales; y por contra, se regula "a posteriori" y como reacción a la evolución de la sociedad. Pero tampoco es cierta la afirmación de que Internet sea un "espacio sin ley". Hay que recordar que, de hecho, hay múltiples leyes que rigen la actividad económica por Internet y que se aplican al uso por parte de los usuarios de la red, por lo cual ciertos aspectos de su uso son regulables.

En términos generales, son todas aquellas que son aplicables al mismo género de actividad presencial o en el "mundo real" como pueden ser leyes sectoriales, legislación del comercio minorista, de defensa del consumidor, de condiciones generales de la contratación, de publicidad y de competencia, de propiedad intelectual, legislación tributaria, etcétera, además de las quizás más conocidas ley del comercio electrónico (LSSICE) y de protección de datos (LOPD).

El hecho de poder regular las nuevas tecnologías y algunos ámbitos de Internet para determinar, o mejor dicho, enfocar su uso, hace que podamos en todo momento ajustar las nuevas tecnologías al principio de proporcionalidad, Al cual se hace referencia en todo momento, tanto por la jurisprudencia, como las Agencias de protección de datos.

9. Anexo

- Informe 78/2008 de la Agencia de Protección de Datos Española.
- Informe 368/2003 de la Agencia de Protección de Datos Española.
- Procedimiento Sancionador PS/00072/2008 de la Agencia de Protección de Datos Española.
- Procedimiento Sancionador PS/00239/2007 de la Agencia de Protección de Datos Española.
- Procedimiento Sancionador PS/00350/2009 de la Agencia de Protección de Datos Española.
- Instrucción Instrucción 1/2006 de la Agencia de Protección de Datos Española.

- Informe 0006/2009 de la Agencia de Protección de Datos Española.
- Informe 0495/2009 de la Agencia de Protección de Datos Española
- Sentencia del 26 de septiembre de 2007 (Sala 4ª) del Tribunal Supremo.
- Sentencia 202/1999 del Tribunal Constitucional.

10. Bibliografía

- Guía de Protección de Datos en las relaciones laborales proporcionada por la Agencia de Protección de Datos.

Sitios Web:

http://www.elpais.com/articulo/sociedad/Alemania/prohibe/jefe/buscar/datos/empleado/Facebook/elpepisoc/20100827elpepisoc_3/Tes

http://leyprotecciondatos.blogspot.com/2009/04/una-rosa-es-una-rosa-y-dos-son-dos.html

http://derechoytic.blogspot.com/2009/01/vigilancia-en-el-lugar-de-trabajo.html

http://www.gvconsulting.com/attachments/370_VIDEOVIGILANCIA.pdf

http://www.diagonalperiodico.net/cantabria/spip.php?article29

http://www.informatica-juridica.com/trabajos/cesiones_de_datos.asp