Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

TRABAJADORES Y PROTECCIÓN DE DATOS: DERECHO DE CONTROL DEL EMPRESARIO

Iñaki PARIENTE DE PRADA
Director. Agencia Vasca de Protección de Datos.

Controles empresariales: el artículo 20.3 del Estatuto de los Trabajadores y su interpretación. Algunas sentencias y resoluciones de interés.

- Sistemas biométricos y su instalación en el entorno laboral: la huella dactilar
- Videovigilancia en el entorno laboral
- Posibilidades de supervisión del correo electrónico por el empresario
- Sistemas electrónicos de vigilancia del trabajador
- Control mediante GPS.

1. Sistemas biométricos: ¿afectan a la intimidad?

- Sentencia de 2 de julio de 2007

SENTENCIA

En la Villa de Madrid, a dos de Julio de dos mil siete.

Visto por la Sala de lo Contencioso-Administrativo del Tribunal Supremo, constituida en su Sección Séptima por los Magistrados indicados al margen, el recurso de casación nº 5017/2003, sobre derechos fundamentales, interpuesto por la CONFEDERACIÓN GENERAL DEL TRABAJO DE CANTABRIA (CGT CANTABRIA), representada por la Procuradora doña Ana Lobera Argüelles, y por el SINDICATO DE TRABAJADORES DE LA ENSEÑANZA DE CANTABRIA (STEC), representado por el Procurador don Román Velasco Fernández, contra la Sentencia dictada el 21 de febrero de 2003 por la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Cantabria, recaida en el recurso nº 763/2002, sobre la implantación del nuevo sistema de control horario.

Se ha personado, como parte recurrida, el GOBIERNO DE CANTABRIA, representado por el Letrado de los Servicios Jurídicos de dicho Gobierno.

Ha comparecido el MINISTERIO FISCAL.

ANTECEDENTES DE HECHO

PRIMERO.- La Sentencia recurrida dispone lo siguiente:

"FALLAMOS

Que debemos desestimar el recurso contencioso-administrativo promovido por la CONFEDERACION GENERAL DEL TRABAJO DE CANTABRIA Y SINDICATO DE TRABAJADORES DE LA ENSEÑANZA DE CANTABRIA contra la Resolución de la Consejería de la Presidencia, publicada en el B.O.C. el 28 de Mayo de 2002 sobre la implantación del nuevo sistema de control horario, y en la Orden de la misma Consejería de Presidencia de fecha 5 de Junio de 2002, sobre la puesta en funcionamiento del sistema de control horario fijándose la fecha del próximo día 17 de Junio de 2002, sin que proceda hacer mención expresa acerca de las

QUINTO.- Es hora de proceder al examen de los cuatro motivos que los recurrentes dirigen contra la Sentencia de instancia.

Un mecanismo de lectura biométrica de la mano mediante un escáner que utiliza rayos infrarrojos y que es inocuo para la salud no puede considerarse lesivo para el derecho a la integridad física y moral que alegan los recurrentes. Y, aún siendo verdad que en la explicación desarrollada en los escritos de interposición se confunde con el derecho a la intimidad, del que debemos hablar más adelante, conviene resaltar cuáles son los contornos de ese derecho reconocido en el artículo 15 de la Constitución. Ha sido definido por el Tribunal Constitucional como "la protección de la inviolabilidad de la persona frente a ataques tendentes a lesionar su cuerpo o espíritu y frente a toda clase de intervenciones en uno de esos bienes que carezca de consentimiento del titular" (STC 120/1990, reiterada por STC 119/2001). En términos sustancialmente coincidentes, en sede académica, ha sido conceptuado como "el derecho a disponer de la propia integridad personal y a no sufrir intervención alguna en ella sin consentimiento del titular, así como a su protección frente a cualquier ataque o riesgo en una sociedad tecnológicamente avanzada".

En cualquiera de estas dos aproximaciones a esa categoría se subraya el elemento de la agresión o injerencia no consentida y el resultado perjudicial, físico o moral, para quien la sufre. Pero no hay traza de nada de ello en la lectura biométrica de la mano mediante un escáner.

Cuanto acabamos de decir es suficiente para descartar la infracción de este precepto. No obstante, como advierte el Ministerio Fiscal, los recurrentes desvían la argumentación del motivo al ámbito de la intimidad corporal. Es decir, al artículo 18.1 de la Constitución. La Sentencia descartó que el mecanismo de control horario que nos ocupa produjera el efecto de vulnerar esa intimidad. Para ello, recordó los términos en que el Tribunal Constitucional la ha contemplado y subrayó la dimensión cultural que es propia de tal noción. Poco más puede añadirse a lo ya dicho por la Sala de Santander sobre el particular. La captación por infrarrojos de una imagen tridimensional de la mano que acaba convertida en un registro de nueve bytes válido para, mediante tratamiento informático que lo relaciona con otros datos, identificar a los empleados públicos del Gobierno de Cantabria y así controlar el cumplimiento del horario de trabajo, no responde al patrón de las intromisiones ilegítimas en la esfera de la intimidad, tanto por la parte del cuerpo utilizada, como por las condiciones en que se usa.

El Gobierno de Cantabria ha comparado la operación de colocar la mano ante el lector con la acción de girar el pomo para abrir una puerta. Cualquiera que sea el acierto de esa comparación, sirve para poner de relieve la intrascendencia de la operación desde la perspectiva del artículo 15 de la Constitución y, también, desde la de su artículo 18.1.

SÉPTIMO.- El tercer motivo sostiene la infracción del artículo 18 de la Constitución en relación con la Ley Orgánica 15/1999. Al respecto debemos precisar cuál es el derecho fundamental al que, en realidad, se refieren los recurrentes. Se trata y conviene decirlo, porque ni en la Sentencia, ni en los escritos de las partes se advierte, que es el denominado por el Tribunal Constitucional, en su Sentencia nº 290, de 30 de noviembre de 2000, como derecho fundamental a la protección de datos de carácter personal y que extrae de la interpretación del apartado 4 del artículo 18 de la Constitución.

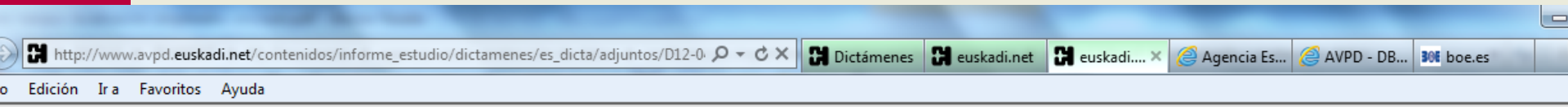
Pues bien, se trata de ver si ese derecho, afirmado como una categoría distinta del derecho a la vida privada por la Carta de los Derechos Fundamentales de la Unión Europea, así como por el Tratado por el que se establece una Constitución para Europa --que, además, lo concibe como un elemento de la vida democrática-- ha sido infringido por la Sentencia de instancia.

Es cierto que el Gobierno de Cantabria se esfuerza en subrayar que el algoritmo informatizado no sirve por sí mismo como elemento de identificación de personas. Desde esa perspectiva, es como si pretendiera negar que se tratase de un dato de carácter personal. No obstante, de acuerdo con el artículo 3 a) de la Ley Orgánica 15/1999, por dato de carácter personal ha de entenderse "cualquier información concerniente a personas físicas identificadas o identificables". Por tanto, en la medida en que el registro en cuestión se integra en un fichero que incluye nombre y apellidos y Documento Nacional de Identidad y, por tanto, es susceptible de identificar a personas, cae bajo las previsiones de ésta la Ley Orgánica.

Sucede, sin embargo, que no se ha puesto de manifiesto que el sistema implantado por las resoluciones impugnadas en la instancia incurriera en infracciones a la misma y, por tanto, vulnerara el derecho fundamental a la protección de datos de carácter personal. Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Además, no parece que la toma, en las condiciones expuestas, de una imagen de la mano incumpla las exigencias de su artículo 4.1. Por el contrario, puede considerarse adecuada, pertinente y no excesiva.

Ciertamente, el registro formado por estos datos personales junto a los demás de este carácter incluidos en el fichero sí está sujeto a las previsiones de dicha Ley Orgánica entre las cuales se hallan las relativas a la información a los afectados prevista en el artículo 5.1 y a la notificación del fichero a la Agencia Española de Protección de Datos. Este extremo consta acreditado en el expediente y, respecto del primero, el Gobierno de Cantabria mantiene que la publicación de las resoluciones de la Consejería de Presidencia ha ofrecido esa información a los empleados públicos. Como sobre este aspecto nada dicen los escritos de interposición, tampoco debemos extender más allá nuestro examen.

Dictamen 12/35 AVPD



Datuak Babesteko
Euskal Bulegoa

Agencia Vasca de
Protección de Datos

CN12-35

DICTAMEN QUE SE EMITE EN RELACIÓN A LA CONSULTA PLANTEADA POR XXX, SOBRE LA ADECUACION A LA NORMATIVA DE PROTECCION DE DATOS DE LA IMPOSICIÓN A CUATRO TRABAJADORAS DE UN SISTEMA DE CONTROL HORARIO BASADO EN EL TRATAMIENTO DE LA HUELLA DIGITAL.

ANTECEDENTES

(. .)

información se vincula a la identidad de una persona es posible identificarla con toda certeza, de modo que los datos que se recaban no pueden considerarse de mayor trascendencia que los relativos a un número personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos.

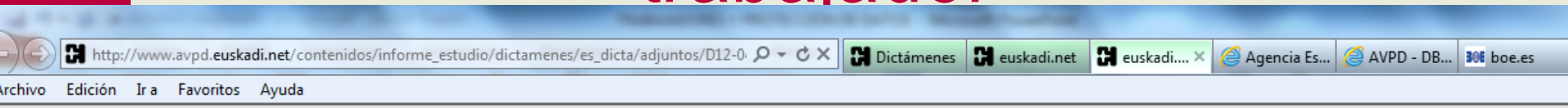
Por otra parte, en cuanto a la necesidad de que el interesado preste su consentimiento (o pueda oponerse) al tratamiento de su huella digital, debe indicarse que si bien el artículo 6.1 de la LOPD exige el consentimiento del interesado para el tratamiento automatizado de los datos de carácter personal, el artículo 6.2 prevé que no será preciso el consentimiento cuando los datos "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". En este caso, del tenor de la consulta parece deducirse que el tratamiento al que se hace referencia trae su origen, precisamente de la necesidad de asegurar el debido cumplimiento de las obligaciones derivadas de la relación laboral que vincula al trabajador con la empresa, lo que unido a lo hasta ahora señalado parece permitir el tratamiento de los datos.

(...)

Además, en lo atinente a las medidas de seguridad en el tratamiento, debe señalarse que, teniendo en cuenta lo que se ha indicado en cuanto al dato biométrico de la huella digital, el mismo no puede ser considerado en modo alguno dato especialmente protegido o sensible, por lo que resultarán de aplicación al tratamiento las medidas de seguridad de nivel básico, previstas en el Reglamento de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio."

En definitiva, ninguna duda cabe sobre la posibilidad de que el empresario, en este caso la Administración xxx- utilice esta tecnología para llevar a cabo el control horario.

Cuestión relevante: información al trabajador



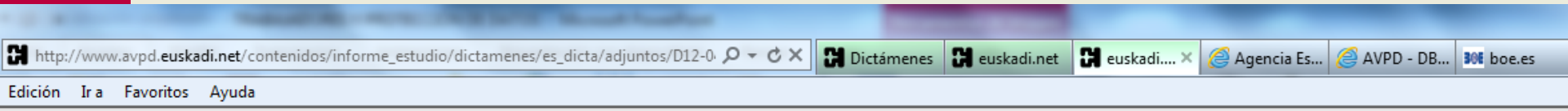
II

En cuanto a la exigencia de que la Administración cumpla con las obligaciones relativas a la creación y notificación del preceptivo fichero, señalar que mediante Orden de xxx, por la que se regulan determinados ficheros de datos de carácter personal del Departamento de xxx, se regula el fichero denominado "Recursos Humanos", entre cuyas finalidades se encuentra el control horario y que enumera en la estructura de los datos de carácter identificativo la "huella". Este fichero se encuentra inscrito en el Registro Vasco de Protección de Datos.

Respecto al deber de informar a los trabajadores en los términos contenidos en el artículo 5.1 de la LOPD, manifestar que para que los datos de los afectados entren a formar parte de la base de datos referenciada aquéllos deberán ser previamente informados sobre los aspectos citados en ese artículo, y en especial, sobre la existencia de un tratamiento de datos, la identidad y dirección del responsable del tratamiento, la posibilidad de ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como ante quién podrán efectuarse, y la finalidad del tratamiento.

Esta información se podría ofrecer en el documento que se utilice para comunicar al trabajador el uso del dato biométrico de su huella digital para el control horario o incluso en el contrato de trabajo para las nuevas contrataciones.

CONCLUSIÓN



CONCLUSIÓN

1.- La instalación de un sistema de control horario basado en la identificación de los trabajadores a través de un dato biométrico, como la huella digital, conlleva el tratamiento de sus datos personales.

2.- La administración pública podrá requerir y tratar el dato biométrico de la huella digital de sus empleados públicos sin necesidad de tener su consentimiento, dada la habilitación que le confiere el artículo 6.2 de la LOPD, pero deberá dar cumplimiento al deber de información a los afectados, conforme al artículo 5 LOPD.

3.- El análisis de la situación generada por los diferentes sistemas de control horario dentro del colectivo de trabajadores del xxx no se encuentra incluido entre las funciones otorgadas a esta Agencia por la Ley 2/2004, de 25 de febrero.

4.- En el caso de que se produjera alguna infracción de la LOPD, la misma podrá ser puesta en conocimiento de la Agencia Vasca de Protección de Datos para que ésta inicie el correspondiente procedimiento de conformidad con lo previsto en el Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero de 2004, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos.

Qué dice el artículo 6 LOPD?

- **Artículo 6.** *Consentimiento del afectado.*
- 1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
- 2. 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 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.

- *Artículo 20 Dirección y control de la actividad laboral*
- **1.** (…)
- **2. (…)**.

- **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.

2. VIDEOVIGILANCIA EN EL ENTORNO LABORAL

- SENTENCIA 29/2013 de 11 de febrero de 2013 DEL TRIBUNAL CONSTITUCIONAL SOBRE VIDEOVIGILANCIA DE LOS TRABAJADORES: FINALIDAD DE LAS CÁMARAS.

instaladas en los accesos a las dependencias.

b) La Universidad de Sevilla tiene concedida autorización administrativa de la Agencia Española de Protección de Datos para, entre otros fines, el control de acceso de las personas de la comunidad universitaria y del personal de empresas externas a sus campus y centros. En virtud de dicha autorización tiene instaladas varias cámaras de vídeo-grabación (fijas y móviles) en los accesos al recinto de la sede sita en la antigua Fábrica de Tabacos, con la debida señalización y advertencia públicas; y, concretamente, dos cámaras de videograbación en los dos únicos accesos directos a la oficina donde el señor Fraile presta sus servicios.

c) En las hojas de control de asistencia de su unidad administrativa, correspondientes a los meses de enero y febrero de 2006, el trabajador consignó y firmó cada día como momento de entrada las 8:00 horas y, de salida, las 15:00 horas. Gracias al control realizado se pudo constatar, en cambio, que permaneció en las dependencias de su unidad en horarios muy diferentes a los señalados en tales hojas, acreditándose en la mayor parte de los días laborables (cerca de una treintena, según concretan los hechos probados de las resoluciones recurridas) una demora variable en la hora de entrada al trabajo de entre treinta minutos y varias horas.

d) En febrero de 2006 el recurrente pidió licencia por asuntos particulares para los días 16, 17, 20, 21 y 22 de ese mes y se ausentó de su puesto de trabajo en dichas fechas. El permiso le fue denegado, aunque la decisión se le comunicó a través de correo electrónico el mismo día en el que se iniciaba el período de ausencia solicitado.

e) En marzo de 2006 se acordó la incoación de un expediente disciplinario. Por

No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo.

Por otra parte, más allá de que ese derecho a la información expresa y previa es el realmente determinante, podríamos no obstante añadir que tampoco había evidencia alguna de que aquélla fuera la finalidad del tratamiento de los datos, o uno de sus posibles objetos, pues ni siquiera estaban situados los aparatos de video-vigilancia dentro de las concretas dependencias donde se desarrollaba la prestación laboral, sino en los vestíbulos y zonas de paso públicos, según se indicó en los antecedentes de esta resolución al recoger el contenido de la Sentencia de 5 de septiembre de 2007, del Juzgado de lo Social núm.3 de Sevilla. En el mismo sentido apuntan, por lo demás, otros documentos que obran en las actuaciones, según los cuales la video-vigilancia respondía a una «medida de seguridad pública en un lugar tan abierto al público» (alegaciones de la propia universidad en el procedimiento ante la Agencia Española de Protección de Datos),

resolución al recoger el contenido de la Sentencia de 5 de septiembre de 2007, del Juzgado de lo Social núm.3 de Sevilla. En el mismo sentido apuntan, por lo demás, otros documentos que obran en las actuaciones, según los cuales la video-vigilancia respondía a una «medida de seguridad pública en un lugar tan abierto al público» (alegaciones de la propia universidad en el procedimiento ante la Agencia Española de Protección de Datos), y no por tanto a un fin declarado y específico de control de la actividad laboral. A la misma conclusión sobre el derecho de información del denunciante llegó la Agencia Española de Protección de Datos en su resolución 0987/2008, de 1 de septiembre; resolución que no podría condicionar nuestro juicio de constitucionalidad pero que, sin duda, resulta indicativa.

En definitiva, por todo lo dicho, las sanciones impuestas con base en esa única prueba, lesiva de aquel derecho fundamental, deben declararse nulas. Y es que privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo fue también de su derecho fundamental a la protección de datos, toda vez que, como concluyó en este punto la STC 11/1981, de 8 de abril (FJ 8), «se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección». A la vista de tal incumplimiento, generador de la vulneración del art. 18.4 CE, no es preciso analizar el resto de las quejas, ni tampoco examinar el tratamiento de datos personales desde otros enfoques, como el de la proporcionalidad, por lo que procederá anular las resoluciones judiciales impugnadas y la resolución rectoral que impuso las sanciones de suspensión de empleo y sueldo al recurrente en amparo.

3. Facultades de supervisión del correo electrónico por el empresario

- La Sentencia del Tribunal Constitucional de 7 de octubre de 2013.
- Hechos: Persona que trabaja en una empresa de productos químicos utiliza el correo corporativo para filtrar información a la competencia y es despedido por ello.
- A instancias de la empresa se persona en ella un notario y un informático que comprueban que ha utilizado el correo electrónico para enviar mensajes a la competencia.
- El artículo 59.11 del convenio colectivo de la industria química establece que la utilización de los medios informáticos propiedad de la empresa, en los que se incluye el correo electrónico, para fines distintos de los relacionados con la prestación laboral, es una falta leve.

- Preguntas:
- ¿Está cubierto el trabajador por el derecho al secreto de las comunicaciones? ¿Se afecta al derecho al secreto de las comunicaciones si se extraen correos electrónicos del ordenador o del servidor?
- ¿Se afecta al derecho a la intimidad del trabajador?
- Intimidad: «ámbito reservado de la vida de las personas excluido del conocimiento de terceros en contra de su voluntad».

- «no cabe duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales». STC 241/2012.
- «En atención al carácter vinculante de la regulación (convenio colectivo) cabe concluir que sólo le estaba permitido al trabajador el uso profesional del correo electrónico de titularidad empresarial» STC 170/2013.

- «Se interpreta así que el poder de control de la empresa sobre las herramientas informáticas de titularidad empresarial puestas a disposición de los trabajadores podía legítimamente ejercerse.. para fiscalizar que su utilización no se destinaba a fines personales o ajenos al contenido propio de su prestación de trabajo» STC 170/2013
- «… no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial.» STC 170/2013

- «En el presente supuesto la remisión de mensajes enjuiciada se llevó pues a cabo a través de un canal de comunicación que, conforme a las previsiones legales y convencionales indicadas, se hallaba abierto al ejercicio del poder de inspección reconocido al empresario». STC 170/2013.
- «La conducta empresarial denunciada realizada además cuando el proceso de comunicación podía entenderse ya finalizado, no ha supuesto una interceptación o conocimiento antijurídicos de comunicaciones» STC 170/2013

Principios generales

- El ordenador es un instrumento útil para la emisión o recepción de correos electrónicos y con carácter general, ha venido reiterando que el poder de dirección del empresario, es imprescindible para la buena marcha de la organización productiva (organización que refleja otros derechos reconocidos constitucionalmente en los arts. 33 y 38 CE). Expresamente en el art. 20 del texto refundido de la Ley del estatuto de los trabajadores (LET) se contempla la posibilidad de que el empresario, entre otras facultades, adopte las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales. Mas esa facultad ha de producirse, en todo caso, dentro del debido respeto a la dignidad del trabajador, como expresamente nos lo recuerda igualmente la normativa laboral en los arts. 4.2 c) y 20.3 LET (STC 186/2000, de 10 de julio, FJ 5).

4. EL CONTROL EMPRESARIAL SOBRE EQUIPOS INFORMÁTICOS:STC 241/2012 17-12-12

- Hechos: En la empresa existe un ordenador, de uso indistinto por todos los trabajadores, sin clave para acceder a la unidad C. En el mismo, dos trabajadoras instalaron, sin conocimiento ni autorización de la empresa, que lo había prohibido expresamente, un programa de mensajería instantánea. Con dicho programa llevaron a cabo comentarios críticos, despectivos e insultantes en relación con sus compañeros de trabajo, superiores y clientes. Otro empleado accedió a dicha información y dio parte a la empresa.
- La empresa, una vez conocido el hecho, convocó a las trabajadoras a una reunión, donde se leyeron varias conversaciones, reconociendo las trabajadoras que habían sido efectuadas por ellas. La empresa sancionó a las trabajadoras.

- dos elementos fácticos relevantes:
- 1) el ordenador era de uso común para todos los trabajadores de la empresa; y
- 2) la empresa había prohibido expresamente a los trabajadores instalar programas en el ordenador, prohibición ésta que en modo alguno aparece como arbitraria en tanto que se enmarca en el ámbito de las facultades organizativas del propio empresario

- La posibilidad de uso común del ordenador por todos los empleados permite considerar que la información archivada en el disco duro era accesible a todos los trabajadores, sin necesidad de clave de acceso alguna. Esta disposición organizativa de uso común permite afirmar su incompatibilidad con los usos personales y reconocer que, en este caso, la pretensión de secreto carece de cobertura constitucional, al faltar las condiciones necesarias de su preservación.

- En el presente caso, estamos ante comunicaciones entre dos trabajadoras que se produjeron al introducirse el programa en un soporte de uso común para todos los trabajadores de la empresa sin ningún tipo de cautela. En este sentido, quedan fuera de la protección constitucional por tratarse de formas de envío que se configuran legalmente como comunicación abierta, esto es, no secreta.
- No puede calificarse como vulneradora del derecho al secreto de las comunicaciones la intervención empresarial

Sentencia TSJ Andalucía 14.XI.2013

- **CUARTO**.-En fecha 10 de febrero de 2012, las tres demandantes al igual que el resto de trabajadores de la empresa, suscribieron un documento sobre obligaciones del personal

- **QUINTO**.-**Por parte del técnico de informática equipos informáticos de la empresa, se ha instalado en los equipos informáticos de los trabajadores de las demandadas un programa denominado Ardamax, una imagen de la pantalla de cada uno que captura cada 10 segundos una imagen de la pantalla de cada uno de los ordenadores. A los trabajadores no se les ha comunicado que iba a establecer algún sistema de vigilancia o control del uso de los equipos. La información obtenida se conserva por parte del informático durante seis meses.**

- **SEXTO**.-Cuando se les comunicó la carta de despido, las trabajadoras reconocieron haber hecho uso del ordenador para fines privados, manifestando que creían que eso estaba permitido

- El conflicto surgirá, pues, si las órdenes del empresario sobre la utilización del ordenador -propiedad del empresario-, o si las instrucciones del empresario al respecto -en su caso la inexistencia de tales instrucciones- **permitiesen entender, de acuerdo con ciertos usos sociales, que existía una situación de tolerancia para un uso personal moderado de tales medios informáticos, en cuyo caso existiría una "expectativa razonable de confidencialidad" para el trabajador** por el uso irregular, aparentemente tolerado, con la consiguiente restricción de la facultad de control empresarial, que quedaría limitada al examen imprescindible para comprobar que el medio informático había sido utilizado para usos distintos de los de su cometido laboral.

- Sólo si hay un derecho que pueda ser lesionado habrá un conflicto entre este derecho y las facultades de control del empresario, que, a su vez, pueden conectarse con la libertad de empresa, el derecho de propiedad y la posición empresarial en el contrato de trabajo.

- La cuestión clave -admitida la facultad de control del empresario y la licitud de una prohibición absoluta de los usos personales consiste en determinar si **existe o no un derecho del trabajador a que se respete su intimidad cuando, en contra de la prohibición del empresario o con una advertencia expresa o implícita de control, utiliza el ordenador para fines personales.**

- La respuesta parece clara: si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso personal**, tampoco existe ya una expectativa razonable de intimidad** y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo.

5. Control mediante GPS.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Vedi anche newsletter del 3 novembre 2014

[doc. web n. 3474069]

Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a. - 11 settembre 2014

Registro dei provvedimenti
n. 401 dell'11 settembre 2014

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

1. Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone.

1.1. Ericsson Telecomunicazioni s.p.a. (di seguito: la società) ha presentato il 1° aprile 2014 una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, in relazione al trattamento di dati personali connesso all'attivazione di una nuova funzionalità di localizzazione di dispositivi smartphone che verrebbero forniti in dotazione dalla società ai propri dipendenti nell'ambito di un sistema di Work Force Management (WFM) già esistente.

Tali dispositivi, dotati di GPS (Global Positioning System) capace di effettuare la localizzazione geografica "con un'accuratezza di 31 m circa", sarebbero in grado di comunicare al sistema WFM la propria posizione con una periodicità temporale prestabilita pari a 15 minuti. Il dato relativo alla geolocalizzazione così raccolto non sarebbe acquisito in modo permanente dal sistema bensì automaticamente cancellato in modo tale che "sarà disponibile solo l'ultimo dato di localizzazione pervenuto, ovvero la nuova posizione rilevata annulla e sostituisce la precedente" (cfr. comunicazione dell'1.4.2014, par. 1, "Chiarimenti sul funzionamento del sistema di geo-localizzazione"). Secondo quanto dichiarato dalla società, pertanto, tramite l'attivazione di tale funzionalità "non viene mantenuto e non si ha a disposizione il tracciamento del percorso. Il sistema mantiene solo i dati master (ad esempio siti, attrezzature, ecc) mentre i dati transazionali (ad esempio dettaglio dei WO) vengono eliminati dal sistema dopo 16 giorni dalla chiusura. Dopo questo periodo di tempo i dati vengono distrutti" (cfr. comunicazione cit., par. 4, "Storicizzazione delle informazioni").

I dati personali complessivamente trattati dal sistema sarebbero: "cognome, nome, Service Area, Skill tecnico (es. radio, transmission, power, ecc), Home Base (ovvero dove il tecnico prende servizio), Attività svolta, dato dell'ultima localizzazione rilevato tramite funzionalità GPS dell'applicazione" (cfr. comunicazione cit., par. 4, "Trattamento Dati e Principio di base").

Gli scopi che la società intende perseguire (cfr. comunicazione cit., par. 2, "Specifica delle esigenze che impongono l'introduzione del

Finalidad del sistema previsto:

n empleados ericsson.pdf - Adobe Reader

tana Ayuda

a. disporre l'intervento di propri tecnici in modo tale da consentire il rispetto dei termini contrattuali stipulati con i clienti, risultano "particolarmente stringenti in quanto l'attività di manutenzione condotta [dalla società] deve supportare la continuità servizio pubblico offerto dal cliente, inclusa la pronta gestione dei ripristini in caso di emergenze non ultime quelle generat disastri naturali/ambientali";

b. intervenire (più) rapidamente con personale specializzato in caso di calamità naturali;

c. migliorare il coordinamento operativo dei "circa 330 tecnici dislocati sul territorio", in modo tale da poter "indiriz prontamente i tecnici in servizio con le idonee competenze più prossimi al sito oggetto dell'intervento richiesto";

d. incrementare la sicurezza dei tecnici stessi in caso di incidenti o situazioni di difficoltà.

posto, "nessun utilizzo dei dati potrà avvenire per finalità diverse da quelle dichiarate, come ad esempio per scopi disciplinari".

Precisiones sobre el sistema:

a. il trattamento di dati personali relativi alla localizzazione dei dispostivi smartphone avviene mediante accesso dell'utente "all'applicazione «WFM Click Mobile Touch» attraverso un'autenticazione basata su userid e password"; la password deve essere modificata dopo il primo accesso rispettando determinati requisiti minimi di sicurezza (cfr. nota del 20.5.2014, p. 1);

b. la possibilità tecnica di accedere alla posizione geografica del dispositivo in un momento dato al di fuori dell'intervallo temporale prestabilito (15 minuti) "non sussiste" (cfr. nota cit., p. 5);

c. i dati c.d. transazionali, "di natura operativa e [che] contengono le informazioni relative agli ordinativi di lavoro […] sono memorizzati localmente e quindi sono presenti solo sul dispositivo mobile. [...] L'operazione di cancellazione compiuta dall'utente tramite la funzione «clear stored data» determina la rimozione dei suddetti dati dal dispositivo mobile" (cfr. nota cit., p. 5);

d. posto che "al termine dell'orario di lavoro ovvero in occasione delle consentite interruzioni dell'attività lavorativa (es. pausa pranzo) il dipendente può disattivare manualmente l'applicazione" in ogni caso, anche qualora il dipendente non provvedesse alla disattivazione manuale "l'applicazione si disattiverà automaticamente dopo 120 minuti di inattività" (cfr. nota cit., p. 5);

e. in caso di furto o smarrimento del dispositivo si prevede "l'immediato blocco dell'utenza mobile attraverso la denuncia alle AA.GG. e la richiesta di blocco all'operatore telefonico" (cfr. nota cit., p. 6);

f. quanto ai tempi di conservazione "il sistema WFM, relativamente ai dati di localizzazione, mantiene solo la località di partenza del FT e l'ultima posizione conosciuta. Nessuna informazione storica relativa alla localizzazione è mantenuta nel Sistema" (cfr. All. nota cit., punto 2.4 "Conservazione dei dati").

Licitud del tratamiento sin consentimiento del trabajador

3. Liceità del trattamento dei dati di localizzazione: bilanciamento di interessi.

3.1 Le finalità del trattamento, così come rappresentate dalla società, risultano lecite. La funzionalità di localizzazione geografica consente infatti di ottimizzare la gestione ed il coordinamento degli interventi effettuati dai tecnici sul campo, incrementandone la tempestività a fronte delle richieste dei clienti, soprattutto in caso di emergenze e/o calamità naturali. La localizzazione consente altresì di rafforzare le condizioni di sicurezza del lavoro effettuato dai tecnici stessi, permettendo l'invio mirato di eventuali soccorsi soprattutto in aree remote o non facilmente raggiungibili e comunque di supportare più rapidamente i lavoratori in caso di difficoltà.

I trattamenti di dati personali, pertanto, sarebbero effettuati nell'ambito del rapporto di lavoro per soddisfare esigenze organizzative e produttive ovvero per la sicurezza del lavoro, coerentemente con quanto stabilito dalla disciplina di settore in materia di controllo a distanza dei dipendenti (cfr. artt. 11, comma 1, lett. a) e 114 del Codice e 4, legge n. 300/1970). In proposito la società ha dichiarato che le informazioni riferibili ai possessori dei dispositivi saranno utilizzate per finalità non riconducibili a quelle di controllo degli stessi, tanto che nessun "utilizzo dei dati potrà avvenire per finalità diverse da quelle dichiarate, come ad esempio per scopi disciplinari" (comunicazione 1.4.2014, par. 2.3). Il menzionato sistema, sempre in base a quanto sostenuto, non potrà interagire con altri sistemi aziendali, compresi quelli volti a valutare il corretto adempimento della prestazione lavorativa.

3.2 Pertanto, considerato anche che la società ha dichiarato che procederà ad attivare le procedure previste dall'art. 4, comma 2, della legge n. 300/1970 visto che la localizzazione di dispostivi associati a dipendenti identificati può comportare il controllo a distanza dell'attività degli stessi, il menzionato trattamento potrà essere lecitamente effettuato anche senza il consenso degli interessati, per effetto del presente provvedimento che, in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g) del Codice), individua un legittimo interesse al trattamento di tale tipologia di dati (diversi da quelli sensibili) in relazione alle finalità rappresentate.

AUTORIZACIÓN DEL GARANTE

2. ai sensi dell'art. 24, comma 1, lett. g) del Codice, in applicazione della disciplina sul c.d. bilanciamento di interessi, per effetto del presente provvedimento il trattamento descritto può essere effettuato senza che sia necessario acquisire il consenso degli interessati, individuando in capo ad Ericsson Telecomunicazioni s.p.a., in relazione all'installazione di un sistema di localizzazione degli smartphone dati in dotazione ai dipendenti, un legittimo interesse volto a soddisfare esigenze organizzative, produttive e legate alla sicurezza del lavoro previa attivazione delle procedure previste dall'art. 4, comma 2, della legge n. 300/1970 (punto 3.2).

Ai sensi degli artt. 152 del Codice e 10 del d.lg. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 11 settembre 2014

IL PRESIDENTE
Soro

IL RELATORE
Califano

IL SEGRETARIO GENERALE
Busia

ESKERRIK ASKO- MUCHAS GRACIAS

- D. Iñaki PARIENTE DE PRADA

  - DIRECTOR. AGENCIA VASCA DE PROTECCIÓN DE DATOS.
- i-pariente@avpd.es www.avpd.es
- 945 016250

Muchas gracias por su atención

http://www.flickr.com/photos/rosino/3658259716/