Grado de Relaciones Laborales y Recursos Humanos

UNIVERSIDAD DE VALLADOLID

Facultad de Ciencias del Trabajo

LA PROTECCIÓN DE DATOS EN LAS RELACIONES LABORALES

Autor/a: Carmen González García

Año académico 2013/2014

Páginas

ABREVIATURAS

AEAT	*Agencia Española de Administración Tributaria*
AEPD	*Agencia Española de Protección de Datos*
CE	*Constitución Española*
LOARTAD	*Ley Orgánica 5/1992 de 29 de Diciembre sobre Regulación del Tratamiento de Datos de Carácter personal (Derogada)*
LOPD	*Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.*
ET	*Estatuto de los Trabajadores.*
RD 1720/2007	*Real Decreto de 21 de Diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal.*
RDLOPD	*Real Decreto 1720/2007 en el que se desarrolla la LOPD.*

1. INTRODUCCIÓN

En este trabajo de Grado quiero hacer un estudio de la evolución que ha tenido la Ley Orgánica de Protección de Datos de carácter personal y la repercusión de la misma en el ámbito laboral.
Hasta hace poco tiempo, la protección de datos era una materia muy poco conocida, salvo para algunos estudiosos del tema o profesionales del Derecho.

El uso de las nuevas tecnologías de la información hizo recomendable que se promulgara la Ley Orgánica 5/1992, reguladora del Tratamiento Automatizado de Datos de carácter personal (en adelante, LOARTAD). Era una ley novedosa, que ponía límites al uso de la informática y a otras técnicas de tratamiento automatizado de datos.

Esta Ley, vino a dar cumplimiento por primera vez, al mandato constitucional contenido en el artículo 18.4 de la Constitución Española (en adelante CE) que regularía la limitación del uso de la informática para garantizar el honor a la intimidad personal y a la propia imagen de los ciudadanos.
Sin embargo, aunque aún quedaba mucho por hacer, esta ley fue sin duda la base de unos principios inspiradores que la evolución de la informática exigía.

Años después, la Directiva 95/46/CE del Parlamento y de Consejo de 24 de Octubre de 1995, convierte la protección de datos en un instituto de garantía de derechos y libertades, aunque pueden verse lesionados por el manejo de los datos personales por parte de terceros.

La Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal (en adelante LOPD), incorpora a nuestro ordenamiento jurídico el nuevo acervo comunitario.

Esta ley, que ha entrado a formar parte de nuestra vida cotidiana, afecta a todos los sectores, pero en este estudio analizaré la compatibilidad existente en el derecho laboral; por un lado, se utilizará el Estatuto de los Trabajadores 8/1980, donde se recoge la mayor parte de la normativa, principios generales y derechos de los trabajadores; también estará presente La Ley de Prevención de Riesgos Laborales 31/1995; ambas deberán combinarse con la LOPD, para que exista una cohesión estable como para poder afirmar que existe Reglamento 1720/2007 (en adelante, RLOPD), por el cual se desarrolla la LOPD.

Concurren pues, aspectos diversos: el de trasplantar el régimen jurídico propio del derecho a la protección de datos, a la singularidad de la relación laboral y al derecho también reconocido constitucionalmente dentro del ejercicio de las facultades y potestades empresariales.

El tratamiento de datos existe en diversos aspectos del control de la actividad empresarial; en la gestión de Recursos Humanos, es una realidad incuestionable, un aspecto más de la organización empresarial.

De cada punto objeto de estudio, iré presentando las sentencias más representativas, así como la jurisprudencia del Tribunal Constitucional.

2. LA PROTECCION DE DATOS PERSONALES COMO DERECHO FUNDAMENTAL

2.1 EL ARTICULO 18.4 DE LA CONSTTITUCIÓN ESPAÑOLA

Podíamos definir el derecho a la protección de datos como aquel derecho que reconoce al ciudadano la facultad de controlar sus datos personales, la capacidad para disponer y decidir sobre los mismos.

La Constitución española, en su artículo 18, garantiza el derecho al honor, la intimidad personal y familiar y a la propia imagen. En particular en su apartado cuarto que en el proceso de elaboración de la Constitución, este apartado que figuraba ya en el Anteproyecto como limitación al uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos, fue objeto de diversa controversia, como destaca MARIA MERCEDES SERRANO PÉREZ [1] establece la necesidad de proteger estos derechos fundamentales, dentro del ámbito relacionado con el uso de la informática. De esta manera, el artículo 18.4 de nuestra CE, dispone:

> "La Ley limitará el uso de la informática para garantizar el honor y la intimad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"

Como consecuencia de este mandato se desarrollo la LOARTAD [2]. De su literalidad, sin embargo, no se extrae el fundamento de este derecho de nueva creación que en su esencia está dotado de una finalidad instrumental de garantía de otros derechos de la personalidad.

El derecho fundamental surge dentro de la llamada "Sociedad de la Información", como un concepto indefinido jurídicamente. El avance de las nuevas tecnologías ha hecho necesario plasmar este nuevo concepto en los textos constitucionales de todos los Estados Miembros de la Unión Europea.

---

[1] SERRANO PÉREZ MARIA MERCEDES –El Derecho Fundamental a la Protección de datos- Derecho Español y Comparado- Ed. Civitas 2003

[2] Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal

En el ámbito europeo, la rápida evolución de las técnicas de tratamiento informático fue motivo para la promulgación del Convenio 108 (28/01/1981) del Consejo de Europa y España ratificó este Convenio el 27 de Enero de 1984.

Posteriormente se promulgó en el marco de la Unión Europea la Directiva 95/46/CEE en la que se recogen los principios mínimos de protección que todos los países de la Unión Europea deberían garantizar en su legislación nacional interna.

En cumplimiento de esta Directiva se promulgó la LOPD[3], que derogó a la LOARTD, y que supone la transposición de la Directiva 95/46/CE[4] al derecho interno de nuestro país. Y esta ley orgánica ha sido desarrollada por el RD 1270/2007 [5] (en adelante RDLOPD), que entró en vigor el 19 de Abril de 2008.

Por tanto, este derecho fundamental, presenta una doble dimensión; por un lado, comporta el derecho a impedir cualquier intromisión a través de un uso abusivo de la informática en la vida privada y, por otro, supone el derecho de disponer de capacidad de decisión sobre el flujo de información que circule sobre el espacio informático y que concierne a los derechos de la personalidad del individuo [6]

2.2 JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL Y EVOLUCIÓN SOBRE LA MATERIA

La primera sentencia relacionada con la protección de datos, aunque tangencialmente, es la STC 110/1984 de 21 de Diciembre. Venía a resolver un recurso de amparo constitucional en el que se pedía la anulación de la Resolución de 10 de Marzo de 1983 de la Dirección General de Inspección Financiera y Tributaria autorizando la investigación de las operaciones activas y pasivas de un contribuyente en determinadas entidades bancarias. El Tribunal desestimó el recurso de amparo al considerar que no había vulnerado el derecho a la intimidad personal y familiar.

El interés de esta sentencia es la referencia que se hace al contenido del derecho a la intimidad en el FJ 3º. Dice así:

El reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas constituciones, entre ellas la española. Pero su idea originaria, que es el respeto a la vida privada, aparece ya en algunas de las libertades tradicionales. La inviolabilidad del domicilio y de la correspondencia, que son algunas de estas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las

---

3 Ley Orgánica 15/1999 de12 de Diciembre de Protección de Datos de Carácter Personal

4 Directiva 95/46 CE del Parlamento Europeo y del Consejo de Octubre de 1995

5 Real Decreto 1720/2007 de 21 Diciembre que desarrolla la LOPD

6 La Ley de Protección de Datos-Análisis y Comentarios a su Jurisprudencia
Editorial LEX NOVA - ISBN 978 84*85012-91-6

intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas han obligado a extender esa protección.

Las modernas tecnologías se conciben como potencialmente agresoras de la privacidad, del espacio reservado a cada individuo, siendo concebida aquí como una manifestación más del derecho a la intimidad.[7]

Esta vinculación de la protección de datos al derecho fundamental a la intimidad se mantiene incluso en sentencias posteriores del Tribunal Constitucional al reconocimiento del derecho a la protección de datos como derecho fundamental autónomo y diferenciado. Así, la sentencia 44/1999, de 22 de Marzo, vino a estimar un recurso de amparo promovido por un trabajador de RENFE, afiliado al sindicato de CCOO., que no había participado en una huelga convocada por su sindicato, pero al que la empresa había descontado las horas correspondientes utilizando para ello los datos informáticos que constaban en su poder referentes al pago de la cuota sindical a través de la nómina. La demanda de tutela de derechos fundamentales consideraba vulnerados los derechos de libertad sindical y de intimidad del actor. Se entendía que la empresa no estaba facultada para la utilización de datos para fines distintos de los autorizados.

El Tribunal Constitucional aborda la protección de datos personales desde la perspectiva constitucional, como un derecho fundamental autónomo diferenciado del derecho a la intimidad en la sentencia 254/1993 de 20 de Julio. La cuestión que se planteaba en este recurso de amparo era de si la negativa de la Administración a administrar a un particular información sobre sus datos personales contenidos en sus ficheros automatizados vulneraba o no los derechos fundamentales a la intimidad y a la propia imagen que reconoce el art. 18 de la CE.

El planteamiento que hace el Tribunal Constitucional determina que no se ha vulnerado el derecho a la intimidad pues la Administración disponía lógicamente de los datos, de ahí que el Tribunal obvie toda referencia al derecho a la intimidad del artículo 18.1 e insista en la autonomía del derecho fundamental de nuevo cuño, sentando ya un precedente de configuración del derecho a la protección de datos personales como un derecho autónomo, diferenciado del derecho a la intimidad, posteriormente consagrado en la sentencia STC 292/2000 de 30 de Noviembre, a la que me refiero a continuación.

Pero esta sentencia no se limitó al reconocimiento de este derecho fundamental de nuevo cuño, sino que también determinó que tenía un contenido esencial que debía ser respetado con independencia del desarrollo legislativo de que fuera objeto.[8]

2.3 LA SENTENCIA 292/2000 DE 30 DE NOVIEMBRE

A) DERECHO FUNDAMENTAL AUTÓNOMO

Esta sentencia es la más relevante de las dictadas por el Tribunal Constitucional hasta ese momento en materia de protección de datos. Vino a resolver un recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra a los incisos de los artículos 21.1. (“Comunicación de datos entre Administraciones Públicas”) y

[7] STC 110/1984 de 21 de Diciembre

[8] La Ley de Protección de Datos – LEX NOVA (PAG.51-54)

24.1 y 2 (“otras excepciones a los derechos de los afectados”) de la Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal por vulneración de los artículos 18.1 y 4 y 53.1 de la CE.

Nuestro Tribunal Constitucional en su sentencia 292/2000, de 30 de Noviembre, ha singularizado el derecho a la protección de datos personales como un nuevo derecho fundamental independiente y desvinculado a los derechos fundamentales a la intimidad personal y familiar. Este nuevo derecho fundamental, se define como un derecho autónomo consistente en el poder de control y disposición que cada ciudadano tiene de sus datos personales, sean estos públicos o no, siguiendo así la línea de lo previsto en la Carta de Derechos Fundamentales de la Unión Europea firmada en Niza el 7 de diciembre de 2000, cuyo artículo 8 establece que toda persona tiene derecho a la protección de datos de carácter personal que la conciernen.

Así, la Jurisprudencia Constitucional presenta unos perfiles definidos de la protección de los datos personales.

En este sentido, el objeto de protección del derecho fundamental a la protección de datos, no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual (protegida en el artículo 18.1 CE), sino los datos de carácter personal, Asimismo también alcanza a aquellos datos personales públicos (son accesibles al conocimiento de cualquiera).[9]

Estas facultades de disposición y control de los datos se concretan en el derecho a consentir y a conocer su posesión y su uso por parte de terceros. Este control y poder de disposición se hace efectivo a su vez a través del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Es por ello, que tal y como ha valorado y analizado el Tribunal Constitucional en su sentencia, el derecho fundamental a la protección de datos, no puede ser entendido de una forma aislada, sino que debe quedar incardinado con el resto de los derechos fundamentales, sirviendo de límite y siendo limitado igualmente por ellos.

Las consecuencias que se derivan de la cualidad de derecho fundamental son las siguientes:

a) Es un derecho irrenunciable del individuo.
b) Su desarrollo debe hacerse a través de Ley Orgánica
c) Prevalece sobre el ejercicio de otros derechos no fundamentales.
d) Posee una protección reforzada, pudiendo ejercitarse ante los Tribunales Ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y a través del recurso de amparo ante el Tribunal Constitucional (artículo 53 CE.[10]

[9] PRODAT – Guía Básica de Protección de Datos de Carácter Personal
[10] Ley de protección de Datos – LEX NOVA (Obra citada)

B) DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS COMO DERECHO DIFERENCIADO DEL DERECHO A LA INTIMIDAD

Comienza el Tribunal señalando que el derecho fundamental a la intimidad no aporta por sí solo una protección suficiente frente a las amplias posibilidades que la informática ofrece, dado que una persona puede ignorar no solo qué datos suyos se hallan recogidos en un fichero, sino también si se han trasladado a otro y con qué finalidad. Recuerda la doctrina de la pionera sentencia STC 254 /1993 de 20 de Julio, seguida por otras posteriores, en cuanto el artículo 18.4 de la C. E. es, en sí mismo, un derecho o libertad fundamental frente a potenciales agresiones a la dignidad y a la libertad de la persona provenientes del uso ilegítimo del tratamiento de datos, lo que la Constitución llama la informática. Garantía que se traduce en un derecho a controlar los datos insertos en un programa informático (habeas data), así como su uso y desuso, con el propósito de impedir un tráfico ilícito y lesivo para el afectado.

C) CONTENIDO ESENCIAL DEL DERECHO

Insiste el Tribunal que el objeto de este derecho fundamental no se reduce solo a los datos íntimos de la persona, sino a cualquier dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, por lo que también alcanza a aquellos datos personales públicos que son accesibles al conocimiento de cualquiera, y no escapan al poder de disposición del afectado. También este derecho faculta a la persona para decidir cuales de estos datos proporcionar a un tercero, o cuáles puede el tercero recabar, y también le permite saber quién posee esos datos personales y para qué, pudiendo oponerse a su posesión o uso.

Un régimen normativo que autorizase la recogida de datos, incluso con fines legítimos, vulneraría el derecho a la intimidad si no incluyese garantías adecuadas frente al uso potencial invasor de a la vida privada.

Se configura así el derecho fundamental como un derecho defensivo en la medida en que protege a los datos personales, sean íntimos no, del conocimiento ajeno, pero también como un derecho de acción al comprender facultades positivas de control sobre los propios datos. En palabras del Tribunal, el derecho a la protección de datos, garantiza a los individuos un poder de disposición sobre esos datos.

D) RESERVA DE LEY

El derecho fundamental a la protección de datos es un derecho de configuración legal, esto es un derecho para cuya plena eficacia es indispensable la intervención del legislador.

La Constitución establece un contenido mínimo o esencial que vincula al propio legislador pero es a este a quien corresponde delimitar su objeto, contenido, límites y alcance.

Precisamente el centro de la impugnación del recurso de inconstitucionalidad se basaba en la vulneración de la reserva de Ley del artículo 53.1 de la C.E. por estimarse que sólo la Ley y no una norma reglamentaria, pueden precisar en qué casos cabe limitar el derecho fundamental.

E) LIMITES

El derecho a la protección de datos no es ilimitado, y de hecho la Constitución ha querido que por Ley, y sólo por Ley, puedan fijarse los límites de tal derecho fundamental (artículo 18.4) , límites que han de hallarse constitucionalmente previstos, por lo que el apoderamiento legal que permita a un poder público recoger, almacenar, tratar y ,en su caso, ceder los datos, sólo está justificado si responde a la protección de otros derechos o bienes constitucionalmente protegidos.[11]

3 DERECHOS CONCURRENTES: LIBERTAD DE EMPRESA FRENTE A PROTECCION DE DATOS DE CARÁCTER PERSONAL.

A) STC 129/1989 DE 17 DE JULIO
B) STC 99/1994 DE 11 DE ABRIL

El tratamiento de datos aparece tanto en aspectos de control de la actividad empresarial como en el proceso de selección e identificación de aspectos personales, como pueden ser algunos relativos a la salud del trabajador. En la gestión de RRHH la utilización o tratamiento de datos es una realidad incuestionable, un aspecto más de la organización empresarial.

Concurren por tanto, diversas perspectivas, siendo la primera, la dificultad de trasplantar el régimen jurídico propio del derecho de protección de datos a las peculiaridades de la relación laboral.

La segunda, la dificultad de delimitar jurídicamente el ámbito del derecho fundamental a la protección de datos, frente a otro derecho reconocido constitucionalmente dentro del ejercicio de las facultades y potestades empresariales, y por tanto las posibles colisiones con los derechos fundamentales de los trabajadores.

El poder de dirección empresarial reconocido en el artículo 20 del Estatuto de los Trabajadores (en adelante ET) ¿es un poder ilimitado? La respuesta la encontramos en la propia Constitución y en el reconocimiento de derechos que la Carta Magna reconoce al trabajador como ciudadano. Derechos que no se pierden por la simple inserción de este en el ámbito organizativo empresarial.

El Legislador no ha dado la respuesta a la cuestión de dónde se encuentra el equilibrio entre el derecho fundamental del trabajador y la libertad organizativa del empresario, y es a través de la jurisprudencia, sobre todo la constitucional, donde encontramos una respuesta a la posible colisión que puede darse entre empresario y trabajador.

---

[11] Obra Citada LEX NOVA

Así, en la STC 129/1989, de 17 de Julio se recoge: *" la vigencia de los derechos fundamentales puede resultar singularmente apremiante en el ámbito laboral, en el que la desigual distribución de poder social entre trabajador y empresario y la distinta posición que estos ocupan en las relaciones laborales elevan en cierto modo el riesgo de eventuales menoscabos de los derechos fundamentales del trabajador."* La celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano.[12]

También, la STC 99//1994 dice: la relación laboral tiene como efecto la sumisión de ciertos aspectos de la vida del trabajador a las necesidades de la organización productiva, pero no bastaría afirmar el interés empresarial para comprimir los derechos fundamentales del trabajador.[13]

El contrato de trabajo genera un complejo de derechos y obligaciones recíprocas que condiciona, junto a otros, también el ejercicio del derecho fundamental que se trata, de modo que manifestaciones del mismo, que en otro contexto pudieran ser legítimas, no tienen por qué serlo necesariamente en el ámbito de dicha relación. El trabajador al ser contratado se inserta dentro del poder organizativo y disciplinario del empresario y queda sometido a las instrucciones, órdenes, controles y sanciones de su superior jerárquico, lo que supone una limitación de sus derechos fundamentales como ciudadano.

Los derechos fundamentales del trabajador, en la empresa, sólo podrán limitarse en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva. El ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir en ningún caso a la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador, ni a la sanción del ejercicio legítimo de tales derechos por parte de aquel.

4. LA AGENCIA DE PROTECCIÓN DE DATOS

El Convenio 108, de 28 de enero de 1981 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, previó que las distintas Partes designaran una autoridad para concederse ayuda mutua.[14]

Sin embargo el convenio no obligaba a la creación de una específica autoridad de Control competente en materia de protección de datos personales. Fue el Protocolo Adicional al Convenio el que lo fijó como exigencia para todos los Estados para que se pudiera homogenizar esta materia.

Cada Estado crea el órgano de control y fija sus competencias, aunque siempre han de tener poderes de investigación e intervención.

---

12 STC 129/1989 de 17 de Julio-BOE 189 DE 9/8/1989

13 STC 99/1994 de 11 de Abril –BOE 285 DE 28/11/1984

14 Convenio 108 del Consejo de Europa para el Tratamiento de Datos automatizados de Datos de Carácter personal. España ratificó el Convenio el 31-01-1984. Entró en vigor en España el 01-10-1985

Siguiendo estas pautas la Ley Orgánica 5/1992 de 29 de Octubre, LOARTAD, encomendó el control de su aplicación a una Administración independiente para asegurar la máxima eficacia de sus disposiciones. A esta Administración, hoy denominada Agencia Española de Protección de datos, se le atribuyó el estatuto de ente publico en los términos del artículo 6.5 de la Ley General Presupuestaria**.**

La Agencia Española de Control de Datos,[15] es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos y garantiza y tutela el derecho fundamental a la protección de datos de carácter personal.

Su actividad se aposenta en tres pilares: capacidad de aplicación de la ley, asesoría a través de servicio legal y de atención al ciudadano y comunicación.

La agencia actúa con independencia de las administraciones públicas en el ejercicio de sus funciones.

Este organismo viene regulado en los artículos 35 y siguientes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *El primero de estos preceptos señala que la Agencia Española de Protección de Datos es un ente público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones*. Se regirá por lo dispuesto en la Ley de Protección de Datos y en un Estatuto propio que será aprobado por el Gobierno.

La Agencia Española de Protección de Datos (en adelante AEPD), tiene las siguientes funciones:

Generales: Velar por el cumplimiento de la Legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de los datos.

En relación con las normas: Informa de los proyectos de normas de desarrollo de la LOPD.

Dicta instrucciones y recomendaciones en relación con la LOPD. Dicta recomendaciones en materia de seguridad y control de acceso a ficheros.

En relación con los administrados que tratan datos: Emiten autorizaciones previstas en la Ley

Requieren medidas de corrección. Ordenan en caso de irregularidad el cese en el tratamiento y la cancelación de los datos. Ejercen la potestad sancionadora. Autorizan las transferencias internacionales de datos.

En relación con los afectados: Informan de los derechos reconocidos en la Ley

Atienden a las peticiones y reclamaciones.

4.1 REGIMEN JURÍDICO DE SUS ACTOS

Además de las potestades de inspección y sancionadora, tiene especial importancia la función instructora o investigadora llevada a cabo por la AEPD en la tramitación de los expedientes sancionadores. Dentro de su organigrama, corresponde a la Subdirección General de Inspección de Datos esta función (artículo 29 del Estatuto), que es la consecuencia obligada de la existencia de la potestad sancionadora atribuida en exclusiva al Director de la Agencia (artículo 37.g. de la LOPD) y la necesaria garantía del procedimiento sancionador cuyo ejercicio exige la separación entre la fase instructora y la sancionadora, encomendándolas a órganos distintos

[15] AEPD creada por R. Decreto 428/1993 de 26 de Marzo

(artículo 134 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común).

La sentencia del Tribunal Supremo de 16 de Febrero de 2007, se ha pronunciado sobre la naturaleza y alcance de las facultades reconocidas en la Ley al Director de la AEPD para dictar normas de desarrollo en esta materia.

El Alto Tribunal considera que la potestad reglamentaria en desarrollo de la Ley mediante la elaboración de las correspondientes disposiciones generales la tiene el GOBIERNO y la AEPD sólo tiene facultades de INFORME, siendo esto lo que dispone la Ley en su disposición final. No se trata de atribuir a la AEPD el desarrollo reglamentario de la Ley sino de que esta, como ente público al que se recomienda el control de la aplicación de la Ley, dirija tal aplicación estableciendo las instrucciones que entienda precisas para conseguir que el tratamiento de datos se ajuste a los principios que la Ley dispone, delimitando así el ámbito de la potestad reconocida.

El legislador establece un ente público para el control de la aplicación de la Ley, que actúa con plena independencia en el ejercicio de sus funciones. Esta potestad reglamentaria específica y no genérica como la atribuida al Gobierno, es por lo que la AEPD no ha de sujetarse a las normas procedimentales previstas para la elaboración de las disposiciones generales (normas hoy recogidas en la Ley de Gobierno), concretamente el trámite de audiencia, el informe de la Secretaría General Técnica y el Dictamen del Consejo de Estado.[16]

5. CUESTIONES GENERALES

5.1 SUPUESTOS DE NO APLICACION DE LA LOPD

Una de las novedades que incorpora el Reglamento de desarrollo de la Ley Orgánica de protección de datos, es la exclusión, bajo ciertas condiciones, de su aplicación a los datos de las definidas como “personas de contacto”.

“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 aquellas, 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 (art.2.2 RDLOPD)”. El Reglamento plantea una excepción a la aplicación de las normas que garantizan el derecho a la protección de datos y por ello debe interpretarse en sentido estricto y de modo restrictivo. Para ello deben cumplirse varios requisitos:

1. Que los datos tratados se limiten efectivamente a los meramente necesarios para identificar al sujeto en la persona jurídica a la que presta sus servicios.
2. Cualquier tratamiento que contenga datos adicionales a los citados se encontrará plenamente sometido a la LOPD.

“Por ello no se encontrarán 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 el mantenimiento del contacto

[16] Ley de Protección de Datos – Editorial LEX NOVA –Obra Citada

empresarial. Igualmente 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 aquel atribuyen las leyes.

La finalidad del tratamiento debe perseguir una relación directa entre quienes traten el dato y la entidad y no entre aquellos y quien ostente una determinada posición en la empresa. De este modo, el uso del dato debería dirigirse a la persona jurídica, siendo el dato del sujeto únicamente el medio para lograr esta finalidad.(informe 78/2008)[17]

5.2 INSCRIPCIÓN DE FICHEROS

La empresa como responsable de los diferentes tratamientos de datos personales que se realizan en la misma (trabajadores, clientes, proveedores, etc.). Debe conocer cuáles son las principales obligaciones que debe cumplir en su calidad de responsable de sus ficheros y/o tratamientos.[18]

La primera obligación en relación al cumplimiento de la normativa de protección de datos, es la notificación de los ficheros (clientes, trabajadores, etc.) a la AEPD para que se inscriban en el registro general de protección de datos. Esta obligación de inscripción, de carácter formal y que en nada presupone el cumplimiento del resto de las obligaciones previstas en la Ley y el reglamento, ha de ser previa al uso de los ficheros y al inicio del tratamiento

Coloquialmente se identifica el concepto de "fichero" o "base de datos" con los programas existentes que ofrecen este tipo de prestación. Sin embargo la definición legal es mucho mas amplia. Por tanto, el objeto al que se aplica la LOPD no se identifica con un programa informático determinado.

"Fichero: todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterio determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. /art. 5 RDLOPD)".

Para que se trate de un fichero sujeto a la LOPD debe permitir el acceso a los datos "con arreglo a criterios determinados" por tanto debe contar con algún criterio de ordenación que permita recuperar datos de una persona determinada.

Ej. Apellidos, nombre, número o código de cliente o factura, fecha, domicilio, teléfono….

El concepto de fichero no solo se aplica a programas informáticos. La LOPD se aplica a los datos personales incluidos en soportes no informáticos cuando puedan ser objeto de tratamiento.

El elemento determinante para identificar un fichero o un tratamiento no automatizado sometido a la legislación sobre protección de datos reside en que se trate de información estructurada en la que resulte posible recuperar los registros relativos a un individuo determinado.

Pues bien, para que una actuación manual sobre datos personales (recogida, , grabación, conservación, elaboración, modificación, bloqueo…)tenga la consideración de "tratamiento de datos personales" sujeto al

---

17 WWW.AEPD.ES –informe 78/2008

18 Guía de las relaciones Laborales "www.AEPD.es

sistema de protección de la LOPD, es necesario que dichos datos estén contenidos o destinados a ser incluidos en un fichero, esto es, un conjunto estructurado u organizado de datos con arreglo a criterios determinados. Si no es así, el tratamiento manual de datos personales quedará fuera del ámbito de aplicación de la ley.

La LOPD establece el deber de notificar los ficheros.

"Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal, lo notificará previamente a la AEPD" donde se ubica el Registro General de datos. Para iniciar la inscripción inicial del fichero y, en su caso, la posterior modificación o supresión de la inscripción, se encuentra disponible el formulario electrónico "NOTA"[19]

5.3 CANCELACIÓN Y BLOQUEO DE DATOS

Cuando cesa la finalidad o cuando motivada y justificadamente se solicita por el afectado hay que proceder a cancelar los datos. La cancelación se da en dos etapas:

1. El bloqueo, con el fin de impedir su tratamiento, excepto para su puesta 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,
2. Transcurrido ese plazo deberá procederse a la supresión de los datos (art. 5.b, LOPD)

Es imprescindible mantener la calidad de los datos pues sino implicaría infracción de carácter grave, de acuerdo con lo dispuesto en el artículo 44.3, f de la LOPD.

6. RECURSOS HUMANOS Y PROTECCION DE DATOS DEL EMPLEADO

6.1 SELECCIÓN DE PERSONAL

El deber de información del art. 5 LOPD forma parte del contenido esencial del derecho a la protección de datos. Este carácter esencial lo posee tanto en el caso de la recogida de datos personales que requiera consentimiento, como en el supuesto de que no lo requiera.

El artículo 5 de la LOPD, viene a establecer un deber impuesto a los responsables de los tratamientos de datos, por lo que será necesario informar al afectado del tratamiento de sus datos de carácter personal (informe de la AEPD 60/2004).

"1. Los interesados a los que se soliciten datos personales, deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

[19] NOTA: Aprobado mediante Resolución de la AEPD de12 de Julio de 2006 (BOE 181 de 18 de Julio)

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

El primer tratamiento de datos personales puede producirse cuando el futuro trabajador sea un simple candidato a un puesto. Por todo ello, es conveniente, que cuando los recursos lo permitan, la empresa debe disponer de impresos de modelos para la formalización del currículo y de un procedimiento de formalización y entrega de los mismos por los candidatos, ya que ello permite informar adecuadamente, establecer las medidas de seguridad, etc.

No debe olvidarse que el Reglamento de desarrollo de la LOPD indica que el deber de información deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

En casos de grupos de empresa o de cualquier otra fórmula de colaboración empresarial, debe tenerse en cuenta que la cesión de datos contenidos en el currículo, o del propio documento debe contar con el consentimiento del candidato (PS/00239/2007)[20]

Así lo demuestra el Procedimiento Sancionador 00239/2007 de la Agencia de Protección de Datos por el cual D. M. M presenta denuncia contra MANAGMENT HOTERLO PIÑERO, S.L. En el citado proceso dicha empresa cedió el currículo a BAHIA PRINCIPE CLUB RESORTS. El Director de la Agencia de Protección de Datos, acabó resolviendo "En el presente procedimiento, se imputa a Management Hotelero Piñero S. L, infracción del deber del 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 consentidos por los titulares de los mismos. "El deber del 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 tanto 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 solo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento".

Y acaba resolviendo imponiendo una multa de 60.101,21 Euros, por infracción del artículo 10 de la LOPD, tipificada como grave en el artículo 44.3 g) de dicha norma, de conformidad con lo establecido en el 45.2 y 4 de la citada Ley Orgánica.

6.2 *CONTRATACIÓN DEL TRABAJADOR Y LOS DATOS ESPECIALMENTE PROTEGIDOS*

El contrato de trabajo es un medio adecuado para informar al trabajador respecto al tratamiento que se realizará respecto a sus datos.

No debe confundirse la información con la manifestación del consentimiento. Por ello, el contrato de trabajo constituye un medio adecuado para ofrecer información sobre los tratamientos directamente relacionados con la prestación laboral.

[20] WWW.AEPD.ES-PS/329/2007

No exime el deber de información sobre todos aquellos nuevos tratamientos de datos personales que la empresa decida realizar con carácter posterior a la relación laboral. (AEPD).

Los datos que por su naturaleza religiosa o ideológica o bien por pertenecer al carácter más íntimo de la persona tienen que protegerse especialmente**.** La LOPD exige una serie de garantías adicionales.

Para que un empresario pueda incorporar a su fichero de datos protegidos información sobre la salud del trabajador, habrá de contar con un servicio de prevención de riesgos laborales y un servicio médico; el reconocimiento sanitario deberá llevarse a cabo siempre y cuando sea necesario para el desempeño de su trabajo. En cuanto al conocimiento de esos datos por los responsables de la gestión de personal se limitarán al APTO o NO APTO. Y en cuanto a las medidas de seguridad se debe aplicar el nivel alto.

Se requiere un consentimiento expreso y por escrito del afectado cuando se vayan a tratar datos de carácter personal que revelen la *ideología, afiliación sindical, religión y creencias.*

La Audiencia Nacional ha señalado en su *Sentencia, de 24 de marzo de 2006,* que «Por consentimiento expreso hemos de entender aquel que se obtiene de una declaración clara e inequívoca, por parte del interesado, que acepta o rechaza la cesión y uso de sus datos mediante la expresión de su voluntad de forma que permita su constancia y prueba indubitada. La existencia de consentimiento expreso, referido a la cesión y uso de estos datos especialmente sensibles no debe admitir duda ni entenderse o interpretarse en varios sentidos, o poder dar ocasión a juicios diversos».

Por otro lado, el artículo 7.4 de la LOPD prohíbe la creación de ficheros que tengan la finalidad exclusiva de almacenar datos personales que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

El resto de tratamientos, es decir, cuando no se pretenda tratar datos considerados como *especialmente protegidos* del artículo 7 de la LOPD (ideología, afiliación sindical, religión y creencias, salud, origen racial y vida sexual), se encuadrarían dentro de la regla general —del artículo 6 de la LOPD—no siendo necesario que esa recogida del consentimiento se realice de forma *expresa*, o de forma *expresa y por escrito.*[21]

6.3 WHISTLEBLOWING

Se le plantea a la AEPD si el sistema interno de denuncia o whistleblowing que pretende implantar es conforme con la LOPD. La Agencia considera que no se requiere el consentimiento de los trabajadores para el tratamiento de sus datos personales en los procedimientos de denuncias internas, siempre que exista pleno conocimiento de la existencia de estos procedimientos por parte de aquellos, y tales procedimientos se refieran a cuestiones que tengan efectiva implicación en la relación laboral.

[21] Javier Álvarez Hernando-extracto del libro “Guía práctica sobre protección de datos – Cuestiones y Formularios”.

La Ley 15/1999 es aplicable tanto a los tratamientos automatizados de datos como a los no automatizados, por lo que las recepciones de denuncias a partir de personaciones del denunciante ante responsable de la empresa también quedarían bajo el ámbito de aplicación de la LOPD.

El sistema de denuncias se ha de limitar a aquellos relacionados con hechos o actuaciones que tengan una efectiva implicación en la relación laboral. Se deberá concretar qué acciones deberán ser objeto de denuncia y especificar las normas, tanto internas de la empresa como leyes normativas o códigos éticos, a los que las mismas se refieran.

La Agencia advierte que se ha de evitar toda denuncia anónima y que el denunciado no ha de poder conocer los datos del denunciante.

La persona denunciada deberá ser informada del registro de los datos relativos a su persona, de la entidad responsable del programa de denuncia de irregularidades, de los hechos de los que se le acusa, de los departamentos y servicios que podrían recibir el informe dentro de su propia sociedad o en otras entidades o sociedades del grupo del que forma parte su sociedad y de cómo ejercer sus derechos de acceso y rectificación.[22]

Deberán implantarse las correspondientes medidas de seguridad en relación con los datos que se establecen en el Real Decreto 994/1999 de 11 de junio que aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Todos los datos tratados deberán eliminarse en el plazo de seis meses desde la finalización de la investigación de los hechos alegados en el informe interno de la empresa.

Por último, la Agencia exige que se le notifique el tratamiento de los datos a fin de obtener su inscripción en el Registro General de Protección de Datos.

6.4 CONTRATACION DE SEGUROS DE VIDA Y PLANES DE PENSIONES

En muchas ocasiones las empresas, y los grupos de empresas, constituyen seguros de vida y planes de pensiones en beneficio de sus empleados, bien de modo voluntario, bien en virtud de lo pactado en un Convenio Colectivo. Debe tenerse en cuenta que:

1. Los tratamientos de datos que resulten necesarios para la contratación de este tipo de productos se encontrarán legitimados, ya sea por el consentimiento del trabajador, ya sea por la existencia de la relación laboral.
2. La empresa puede realizar distintos tipos de tratamientos:
    a) La cesión de los datos de identificación y contacto del trabajador a la empresa aseguradora o la gestora del Plan de Pensiones.

[22] Revista Actualidad Jurídica-Abogado Uría Menéndez

b) La recogida de datos vinculados al contrato a celebrar para su traslado a la aseguradora o gestora del plan de pensiones.[23]

La fórmula de la recogida de datos por la empresa aseguradora es la más recomendable desde el punto de vista de protección de datos.

Sea cual sea el tratamiento que realice la empresa es imprescindible la información al trabajador como así lo dispone el art. 5 de la LOPD,[24]

6.5 EXTERNALIZACIÓN DE NÓMINAS

En la actualidad, muchos negocios prefieren externalizar parte de sus servicios a ciertas compañías especializadas en un determinado aspecto normalmente técnico. Así, el aspecto informático lo depositan en manos de empresas especializadas en este ámbito.

Esto conlleva un traslado de archivos y datos que contienen información personal bastante importante, y respecto a esto hay que llevar una política adecuada para cumplir con los requerimientos de nuestro Ordenamiento Jurídico.

Estos servicios especializados se conocen como "outsourcing" que traducido literalmente sería "externalización" en su acepción castellana. En el "outsourcing" más amplio, una empresa se involucra con otra para conseguir un fin común, en una especie de "joint venture" pero sin la creación de una nueva empresa.

La Ley afirma que "la realización de tratamiento por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Una vez terminada su relación con la gestaría o la empresa, dichos datos deben ser destruidos, o devueltos al responsable de su empresa, incluyendo todos los documentos donde hubiere algún dato de carácter personal.

Ante la posibilidad de que la empresa gestora realice un incumplimiento contractual en esta materia, el apartado 4 del articulo 12 dice: "En el caso de que el encargado del tratamiento destine los datos a otra finalidad, incumpliendo las estipulaciones del contrato, será considerado responsable también del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.. Además de un incumplimiento contractual por el que se pueden pedir las lógicas indemnizaciones, el responsable (el que ha manejado los datos en la gestoría, estará sometido al régimen sancionados de la LOPD. [25]

---

[23] WWW.AEPD.ES GUIA DE LAS RELACIONES LABORALES

[24] Guía práctica de la Protección de Datos: Cuestiones y Formularios. LEX NOVA ISBN 978 84 9898 353.1

[25] Alfonso Villahermosa Iglesias –Especialista en Economía y Derecho de la Tecnología Digital

Igualmente, cesiones de datos temporales, pueden encuadrarse dentro del supuesto del artículo 11 "comunicación de datos". Como regla general, se pide el consentimiento del afectado para que se produzca esta comunicación. En dicho artículo, se afirma que dicho consentimiento no será efectivo cuando:

- La cesión haya sido autorizada por ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público.
- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas.
- Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

El responsable del fichero es la persona "dueña" de los datos, el Encargado del Tratamiento es quien realiza el servicio. Tanto unos como otros deben estar perfectamente identificados en el Documento de Seguridad.

Quien efectúa el tratamiento para el responsable se obliga a prestarlo en el nivel de calidad pertinente, observar confidencialidad y tomar las medidas adecuadas para garantizar la seguridad de la información.

El encargado del tratamiento es un tercero que trata los datos personales siguiendo las instrucciones del responsable si bien no bajo la dependencia o autoridad del mismo desde el punto de vista laboral (esto es importante, ya que si no, nos encontraríamos en la órbita del artículo 12). No es un empleado del responsable, le presta sus servicios al amparo de un contrato cuyos requisitos básicos aparecen diseñados por la Ley.

Es claro que si el Encargado del tratamiento incumple las obligaciones – por ejemplo- destinando los datos a otra finalidad distinta, dicho Encargado será considerado responsable.

7. LOS CONTROLES EMPRESARIALES

El uso de de facultades específicas atribuidas a la empresa en el Estatuto de los Trabajadores, otorgan la posibilidad al empresario de desarrollar un control al trabajador en el desarrollo de la prestación laboral.

De este modo el empresario podrá adoptar las medidas que estime oportunas de control y vigilancia, guardando en su adopción y aplicación, la consideración debida a su dignidad humana

Se podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por este para justificar su falta de asistencia mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dicho reconocimiento podrá determinar la suspensión de los derechos económicos que puedan existir a cargo del empresario (art. 20.3 y 4 ET.)

7.1 CONTROLES BASADOS EN EL USO DE TECNOLOGIAS DE LA INFORMACIÓN

Pueden citarse entre otros, los controles biométricos como la huella digital, la videovigilancia, los controles sobre el ordenador –como las revisiones, el análisis o la monitorización remota, la indexación de la navegación por Internet, o la revisión y monitorización del correo electrónico y/o el uso de ordenadores, o los controles sobre ubicación física del trabajador mediante geolocalización.

En la mayor parte de estos supuestos existe tratamiento de datos personales y, en consecuencia es necesario cumplir con los principios de protección de datos. La Agencia Española de Protección de Datos y la jurisprudencia de los tribunales han venido indicando distintos supuestos en los que tales tratamientos son admisibles y las condiciones para su realización.[26]

El principio de proporcionalidad es el factor primordial que se debe adecuar al control empresarial que se lleve a cabo, respetando en todo momento los derechos fundamentales que asisten al trabajador.

Es esencial la información al trabajador especialmente cuando se adopten medidas restrictivas en el uso de Internet y/o Correo Electrónico, describiendo de forma exacta y concreta la utilización de dichos medios de comunicación de la empresa con fines personales o privados.

7.2 VIDEO-VIGILANCIA EN EL TRABAJO

El incremento que últimamente están experimentando las instalaciones de sistemas de cámara y videocámaras con fines de vigilancia, ha generado numerosas dudas en lo relativo al tratamiento de las imágenes que ello implica Todo esto hace necesario que, en ejercicio de la competencia que le atribuye el artículo 37.1.c de la LOPD, la AEPD dicte una instrucción para adecuar los tratamientos de imágenes con fines de vigilancia a los principios de la Ley Orgánica y garantizar los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos.

[26] AEPD – Guía de la Protección de Datos en las Relaciones Laborales.

El marco en que se mueve la presente instrucción es claro. La seguridad y vigilancia elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático.

Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la LOPD y el artículo 1.4 del Real Decreto 1332/1994 de 20 de junio que considera como dato de carácter personal la información gráfica o fotográfica.[27]

Los bienes jurídicos afectados son: Intimidad, honor y la propia imagen

La imagen de una persona, en la medida que es identificable o susceptible de ser identificada es considerada, dato de carácter personal.

En el ámbito de la video-vigilancia, deben aplicarse los principios sobre protección de datos siempre que se utilicen medios técnicos para grabar, captar, tratar o almacenar y reproducir imágenes de personas identificables, ya sea en tiempo real o en diferido.

Así, cuando se instalen sistemas de video-vigilancia donde puedan aparecer personas identificables, deben observar lo dispuesto en la legislación de protección de datos y de las circulares e instrucciones de la AEPD.

Las personas expuestas a la video-vigilancia deben de ser informadas de modo expreso, previo e inequívoco respecto a la colocación de los equipos, la zona que se monitoriza, el responsable de la instalación y las acciones que se puedan llevar a cabo por los individuos cuyas imágenes sean tratadas. (AEPD)

La reciente STC 29/2013, de 11 de febrero (recurso de amparo núm. 10522/2009 resuelve un asunto de este tipo y declara una doctrina que sujeta el ejercicio de las facultades del empresario del empresario al cumplimiento del deber de información previa a los trabajadores acerca del contenido y objetivo específicos de la correspondiente medida de vigilancia y control.[28]

El recurso lo interpuso el Sr. Fraile, un trabajador de la Universidad de Sevilla, que había sido sancionado con la suspensión temporal de empleo u sueldo por incumplir injustificada y reiteradamente su jornada laboral. En prueba de la infracción, la Universidad que desde hacia tiempo sospechaba que el Sr. Fraile no cumplía con su horario laboral, decidió servirse de las cámaras de video-vigilancia que tenia instaladas en los accesos al recinto universitario para controlar el acceso a sus campus y centros. Dos de estas cámaras apuntaban al acceso directo del despacho del Sr. Fraile. Hay que decir que la Universidad de Sevilla disponía de la autorización administrativa concedida por la AEPD y que la existencia de las citadas cámaras estaba debidamente advertida mediante los oportunos carteles informativos.

En su demanda de amparo el Sr. Fraile insistió en que la utilización no consentida ni previamente conocida de las imágenes grabadas en las cámaras de seguridad, vulneró su derecho a la protección de datos de carácter personal (art.18.4 CE).

---

[27] Instrucción 1/2006, de 8 de Noviembre, de la AEPD sobre el tratamiento de datos personales, con fines de Vigilancia a través de sistemas de cámaras o videocámaras.

[28] Miguel Casino Rubio-Profesor Titular derecho Administrativo de la universidad Carlos III de Madrid

El Tribunal Constitucional, responde afirmativamente y, en consecuencia declara que cuando el empresario pretenda valerse de las grabaciones captadas por la cámara de seguridad para fines de control laboral debe previamente informar a los trabajadores de esa posibilidad.

La STC 186/2000 enjuicia por su parte el caso de una empresa que, ante la sospecha de la existencia de irregularidades en su economato motivas por la existencia de un llamativo descuadre, decidió instalar un circuito cerrado de televisión para controlar la actividad laboral de tres de sus cajeros. Las cintas de video grabadas revelaron que uno de ellos realizó de forma reiterada maniobras en el cobro de artículos a los clientes del economato, sustrayendo diferentes cantidades de la caja. Por este motivo, fue expedientado y finalmente despedido de la empresa.

Tras agotar sin éxito las vía judicial laboral, el trabajador acudió en vía de amparo al Tribunal Constitucional para denunciar que ese tipo de control laboral vulneró su derecho a la intimidad personal y a la propia imagen (art. 18.1 CE).

En esta ocasión el Tribunal Constitucional, denegó el amparo solicitado, afirmando que la intimidad del recurrente no resulta agredida por el mero hecho de filmar como desempeñaba las tareas encomendadas en su puesto de trabajo., sino que se trataba de obtener la actuación profesional del trabajador, pretensión justificada por la circunstancia de haberse hallado irregularidades en su actuación profesional.

7.3 CONTROL DEL CORREO ELECTRÓNICO POR PARTE DEL EMPRESARIO

¿Qué procedimiento debe seguirse en cuanto al uso de correos electrónicos de los trabajadores por parte de las empresas según la LOPD? A esta pregunta responde el Informe Jurídico 047/2008 de la AEPD.

Para poder acceder a esta información, resulta necesario que exista legitimación para dicho tratamiento de datos, y el artículo 6.1 de la LOPD dispone que “El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga lo contrario”, no obstante el tratamiento de los datos correspondientes a los trabajadores, cuando el mismo se efectúa en el ámbito de la relación laboral, debe señalarse que el artículo 6.2 de la LOPD exceptúa la obligación de recabar el consentimiento de los afectados, en los supuestos en que “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.

No obstante, el Estatuto de los Trabajadores aprobado por Real Decreto Legislativo 1/1995 de 24 de Marzo, establece en su artículo 20.3 que “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 derechos 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.

En virtud de lo expuesto, podemos entender que existe legitimación para filtrar el contenido del correo electrónico de los empleados, pero siempre que se trate de una cuenta de correos proporcionada por la empresa para el desarrollo de sus funciones laborales y siempre que se haya informado previamente a los trabajadores sobre dicho filtrado y los medios que se van a utilizar.[29]

Especial eco informativo, ha tenido en los medios de comunicación por el interés que en el ámbito socio-laboral suscita la sentencia dictada el 7 de Octubre por el Tribunal Constitucional en el recurso de amparo 2.907/2011. En la citada sentencia se establecen los límites que los derechos fundamentales al secreto de las comunicaciones (art. 18.3 de la Constitución Española) y a la intimidad personal (art. 18 CE) imponen a las empresas en el control y vigilancia del uso que sus trabajadores hacen del correo electrónico corporativo.

El interés suscitado se explica porque, como explica el Tribunal Constitucional, la decisión de fondo tiene una especial trascendencia que, según la doctrina de anteriores sentencias, se da cuando en el momento de admitirse a trámite un recurso plantee un problema o una faceta de un derecho fundamental susceptible de amparo sobre el que no haya doctrina constitucional. Y aunque la materia ya se había abordado en la anterior sentencia del TC 241/2012 de 17 de Diciembre, no concurren en ellas "las peculiaridades del actual recurso".

El caso del que trae antecedente la sentencia es el de un trabajador de una empresa del sector químico que valiéndose de la cuenta del correo electrónico corporativa, transmitió y reveló a terceras personas información industrial confidencial, y al que la empresa despidió tras comprobar tales hechos y su autoría mediante la intercepción y extracción ante notario y por un técnico informático del contenido de sus mensajes SMS y mails remitidos desde el móvil y el portátil corporativos, que confirmaron las previas sospechas de una conducta irregular.

La defensa del trabajador alego en el juicio por despido que dicho registro y acceso al correo electrónico del trabajador constituía una intromisión ilegítima y no autorizada por este en la esfera de los referidos derechos fundamentales. Y que la apuesta a disposición de la cuenta de correo electrónico, se hizo sin comunicarle un protocolo de reglas de uso de dicha herramienta informática,

El Tribunal Constitucional deniega el amparo solicitado por el trabajador. Y en la razón de su decisión pesa esencialmente la circunstancia de que en el convenio colectivo de trabajo aplicable en el sector, el XV Convenio de la Industria Química, se establece el exclusivo uso profesional del correo electrónico propiedad de la empresa y, además, se tipifica como falta laboral su utilización para fines distintos al trabajo.

El razonamiento del TC quedaría incompleto sin añadir que en el caso comentad consideró que el registro y control empresarial obedecía a un fin legítimo (la protección de secretos de la empresa, ante la existencia de sospechas fundadas de un comportamiento irregular del trabajador) y que era una medida proporcionada por idónea (para verificar la irregularidad sospechada), por necesaria (el acceso al contenido de los mensajes era necesario para probar tanto aquella conducta irregular, como para adoptar la sanción disciplinaria, sin que hubiera bastado para ello con solo identificar al remitente y al destinatario sin acceder al contenido), y por equilibrada (el contenido de los mensajes no incluía datos relativos a la vida privada del trabajador, de modo que

[29] Publicado por Jesús Pérez Serna un Viernes, enero 15th 2010 –I-SPY

el interés empresarial en ejercer sus facultades de control debe prevalecer pues no sacrifica contenidos de privacidad con carácter personal o familiar).

La sentencia subraya que el Pleno del Tribunal ha señalado como elemento caracterizador de la definición constitucional del art. 18.4 CE, , el derecho del afectado a ser informado de quien posee los datos personales y con que fin (FJ 7)[30]

De cualquier forma, se llega ala conclusión de que la libertad informática, cubre un radio mas amplio que el que por su parte proporciona el art. 18.1 CE

Naturalmente con su STC 292/2000, ha dado paso al reconocimiento de un derecho constitucional autónomo a la protección de datos

7.4 EL ABSENTISMO LABORAL – CONTROLES

El Estatuto de los Trabajadores en su artículo 20.4 establece: "El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por este para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo del 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.

En innumerables ocasiones, el empresario según las facultades que le reconoce la legislación vigente, para obtener un control más eficaz del absentismo laboral elabora bases de datos relativos a la salud de los trabajadores y en concreto del diagnóstico médico, prescindiendo del consentimiento de estos. En este sentido, sería conveniente saber que proceder al almacenamiento de datos no es una facultad que le sea otorgada por la normativa actual.

Así lo indica el Tribunal Constitucional en su sentencia 202/1999 de 8 de Noviembre donde ordena la destrucción de los datos contenidos en un fichero enclavado en un Banco. Resalta el TC "*que a la vista del contenido del fichero, resulta convenir que su mantenimiento no se dirige a la preservación de la salud de los trabajadores, sino al control del absentismo laboral. Consecuentemente, la creación y actualización del fichero….no puede ampararse en la existencia de un interés general…ni tampoco en lo dispuesto en los arts. 22 y 23 de la PRL, habida cuenta de que en el fichero en cuestión no se reflejan los resultados arrojados por la vigilancia periódica –y consentida por los afectados-del estado de salud de los trabajadores en función de los riesgos inherentes a su actividad laboral, sino tan sólo la relación de periodos de suspensión de la relación jurídico-laboral dimanantes de una situación de incapacidad del trabajador*".

[30] Escrito el 17 de Diciembre, 2013 por Ramón Valls

Consiguientemente hemos de deducir que el tratamiento y conservación del diagnóstico médico en una base de datos creada al efecto por el empresario para control del absentismo-sin consentimiento expreso del afectado, incumple la garantía que para la protección de los derechos fundamentales se contiene en el art. 53 de la Constitución.

Por otra parte, 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 revista la solución de consideración idónea, necesaria y proporcionada para la consecución del fin, en este caso el absentismo laboral.[31]

En este sentido se ha pronunciado la Audiencia Nacional en dos importantes Sentencias de 26 de septiembre y 12 de Abril de 2002, cuando en esta última analizó el tratamiento de datos de salud para el control del absentismo laboral.

En la citada sentencia de 26 de Septiembre de 2002, señaló que "siendo así que es regla general la exigencia del consentimiento inequívoco del afectado para el tratamiento de datos de carácter personal (artículo 6.1 Ley Orgánica 15/99) y sabemos que el legislador ha querido reforzar esta exigencia cuando se trata de datos especialmente protegidos (artículo 7.2 y 7.3) las excepciones a dicha norma general, como la prevista en el artículo 7.6 deben ser interpretadas de modo estricto sin que quede admitir otros casos de dispensa del consentimiento distintos al, que aparece expresamente contemplado en la norma".

Del mismo modo la mencionada Sentencia de 12 de Abril de 2002 sobre el tratamiento de datos de salud en un proceso del absentismo laboral, señala lo siguiente:

"A la luz de estos preceptos, y en concepto del art. 7.6 de la LOPD, el fundamento de la excepción de la necesidad del consentimiento en el tratamiento de datos relativos a la salud, se encuentra en la prevención, diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.[32]

Pues bien, en nuestro caso, el tratamiento de datos personales relativos a la salud efectuada por loa entidad recurrente, no se realizaron con esa finalidad, sino en virtud de un contrato suscrito con el Departamento cuyo objeto era controlar el absentismo del personal que prestaba sus servicios en este organismo. Y para ello (…) crea un fichero en el que registra los datos de diagnóstico médico de cada trabajador que utiliza como medio para elaborar un informe que remitirá a dicho Departamento, para que este pueda controlar el absentismo laboral.

La prestación del servicio médico realizado por los facultativos de (…) no tiene por objeto ni la mejora, ni la prevención de la salud de las personas a quienes examina y cuyos datos incorpora al fichero, es decir no realiza una prestación necesaria para su salud, ni tampoco para el tratamiento médico a que pudieran estar sometidos, ni para la investigación científica o el desarrollo de la medicina, sino que la prestación

[31] José Malpartida Morano y Ricardo y Ricardo Pradas Montilla –Boletín de la Facultad de Derecho nº 18,201-Empresas y Protección de Datos de Carácter General.

[32] Revista Jurídica de Castilla y León Nº 12- 49- Abril 2007

únicamente está al servicio de los intereses del arrendador que, a través de ese mecanismo, pretende evitar el absentismo en el trabajo.

Por tanto no puede hablarse de prestación de servicios médicos en los términos exigidos por la Ley, sino de otro tipo de prestación de servicios, no amparada en el art. 7.6 de la LOPD, para cuyo tratamiento informatizado precisa el consentimiento del afectado.

Los datos pueden recogerse para su tratamiento siempre que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas explícitas y legítimas para las que se hayan obtenido, de modo que existe una sutil distinción entre "finalidad de la recogida" y "finalidad del tratamiento", pues la recogida solo puede hacerse con fines determinados, explícitos y legítimo, y el tratamiento posterior.[33]

8. RELACIONES CON LOS SINDICATOS Y PROTECCIÓN DE DATOS

Sabido es que en el contenido del art. 28.1 CE se integra la vertiente funcional del derecho a la libertad sindical, es decir, el derecho de los sindicatos a ejercer aquellas actividades dirigidas a la protección y promoción de los intereses de los trabajadores y a desplegar los medios de acción necesarios para que pueda cumplir las funciones que constitucionalmente les corresponde[34] Es evidente que las organizaciones sindicales para desarrollar sus funciones de promoción de los intereses de los trabajadores en consonancia con los nuevos tiempos, tienen que readaptar continuamente sus estructuras y, en este sentido, puede decirse, como no podía ser de otra manera, que asumir las ventajas derivadas de las nuevas tecnologías supone un paso esencial e imprescindible a la hora de retener informaciones personales de los sujetos representados, siendo el propio sindicato el responsable del fichero.[35]

Será responsable del tratamiento de datos en el tablón de anuncios y por tanto de las informaciones publicadas en el mismo, aquel órgano u organización que decida sobre su uso y finalidad y sitúe materialmente la información en el.

Es fundamental que los tablones sindicales online se sitúen en la intranet de la empresa, nunca en Internet.

Debe tener se cuenta el principio de calidad desde el punto de vista de la proporcionalidad de los tratamientos y de la finalidad de los mismos.[36]

[33] Álvaro Canales Gil –50 Revista Jurídica de Castilla y León nº 12-Abril 2007
[34] STC. 40/1985 de 13 de Marzo
[35] SUSANA RODRIGUEZ ESCANCIANO. Libertad Sindical. Nuevas Tecnologías
[36] Guía de la Protección de Datos en las Relaciones Laborales. AEPD

8.1 ACCESO A DATOS POR EL COMITÉ DE EMPRESA

Al Comité de Empresa y a los representantes sindicales el Estatuto de los trabajadores atribuye unas facultades amplias pero no ilimitadas. El art. 64 del E.T. establece que el Comité de Empresa, tendrá derecho a ser informado de todas las sanciones importantes por faltas muy graves y a recibir la capia básica de los contratos y la notificación de las prórrogas y de las denuncias correspondientes a los mismos en el plazo de diez días siguientes a que tuvieran lugar.

En todo caso, los datos que se cedan por parte de la empresa serán los estrictamente necesarios que el Estatuto de los Trabajadores establece para el cumplimiento de su función, exigiéndoles el deber de sigilo y confidencialidad durante la duración de su mandato y una vez que haya expirado el mismo; asimismo no podrán utilizar esos datos para fines distintos de los que motivaron su entrega.

8.2 CESIONES DE DATOS PERSONALES A SINDICATOS

Cuando el trabajador solicite que el cobro de la cuota sindical se realice en el pago de la nómina, deben darse las condiciones que establece el art. 7.2 LPD en cuanto a la cesión de datos se refiere.

La empresa debe disponer de modelos o impresos de solicitud en los que el trabajador autorice de modo expreso y por escrito el tratamiento. Asimismo la empresa debe limitar el uso de estos datos a la finalidad para la que se han recabado: como la cuota y transferir las cantidades a la organización sindical.

El empresario nunca podrá usar ese dato conocido respecto de la afiliación, proporcionado a los exclusivos efectos de practicar el descuento de la cuota sindical, para otras finalidades claramente incompatibles, tales como la retención de haberes de los afiliados por presunta participación en una huelga convocada por el sindicato, pues como ha señalado el Tribunal Constitucional lesionaría el derecho de libertad sindical consagrado en el art. 28 CE.

Así lo ha manifestado el TC en la sentencia 11/1998 de 13 de enero cuando concedió el recurso de amparo a un trabajador de RENFE, cuando le descontaron de sus haberes lo correspondiente a una huelga en la que no había participado con el agravante únicamente de su afiliación CCOO, situación de la que el empresario tenía noticia por su descuento en nómina de la cuota sindical.

Dice el TC en su FJ 6:

Según el art. 178.2 LP.L., «En el acto del juicio, una vez constatada la concurrencia de indicios de que se ha producido violación de la libertad sindical, corresponderá al demandado la aportación de una justificación

objetiva y razonable, suficientemente probada, de las medidas adoptadas y de su proporcionalidad»; en el sentido de que, concurriendo en el caso los indicios de vulneración del derecho a la libertad sindical (descuento salarial por el mero hecho de afiliación a uno de los Sindicatos convocantes de la huelga), debía el órgano jurisdiccional del orden social haber exigido a la demandada RENFE, de conformidad con el precepto trascrito, que aportase al proceso laboral una justificación objetiva y razonable, ajena a la actitud discriminatoria antisindical, que respaldase el hecho del descuento salarial llevado a efecto.

El empleador quedará en una situación incómoda en la que chocan, aparentemente, dos valores constitucionales: de un lado, la libertad sindical reconocida en el art. 28 CE, que exige en muchos casos la cooperación del empresario para el más fácil y sencillo cumplimiento de los fines a que está encaminada y, de otro, el derecho a la protección de datos (autodeterminación informativa) derivado del art. 18.4 CE que exige de la empresa discreción y protección de las informaciones relativas a los trabajadores que emplea.

Igualmente, como en el caso anterior, el mayor problema que en la práctica se plantea respecto a los tratamientos de datos personales a realizar por los sindicatos y representaciones de los trabajadores, viene dado por determinar cuándo pueden hacer uso legítimo de los mismos en el desempeño de sus funciones que constitucionalmente tienen asignadas en los arts. 7 y 28 CE, arts. y título II ET.

9. PREVENCIÓN DE RIESGOS LABORALES Y LA PROTECCIÓN DE DATOS

La Ley 31/1995 de 8 de Noviembre de Prevención de Riesgos Laborales y sus normas de desarrollo imponen a la empresa la realización de un conjunto de actividades cuyo fin último es evitar a disminuir los riesgos derivados del trabajo. Para esta tarea resulta necesario tratar datos personales de los trabajadores.

En principio, el tratamiento de datos personales en materia de prevención de riesgos, se encuentra legitimado por la existencia de una relación contractual cuyo cumplimiento, desarrollo y control, lo hace necesario (art. 6.2 LOPD).

“El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes a su trabajo”.

“Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento (…) (art. 21.1 de la Ley 31/1995 de 8 de Noviembre de Prevención de Riesgos Laborales).”

No obstante, esta vigilancia puede ser obligatoria conforme al artículo 21.1 de la Ley de Prevención de Riesgos Laborales, previo informe de los representantes de los trabajadores en supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa[37]

[37] WWW.AEPD.ES Guía de la Protección de Datos en las Relaciones Laborales

Ello se proyecta sobre la protección de datos del modo siguiente:

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 será responsable del fichero que se genere para la gestión de la prevención. Los accesos a los datos de salud serán plenos para el servicio sanitario y limitados para la gerencia, que deber únicamente los conceptos "APTO" o "NO APTO".

Las empresas que actúan como servicio de prevención ajenos tienen la v consideración de responsables del tratamiento (Informe 0299/2009)[38]

El nivel de seguridad que será alto en todos aquellos casos que incluyan datos de salud con identificación precisa de las enfermedades, traumatismos, etc. , o si se gestionan históricos de salud laboral.

La historia clínica del trabajador debe regirse, además de lo previsto en la LOPD, por los principios de la Ley 41/2002.

El empresario ostenta un cierto poder sancionador sobre el trabajador (más propio del derecho público) aunque a su vez tiene obligaciones de especial importancia para con dicho trabajador: entre otras, el deber de protegerle de forma efectiva frente a los riesgos laborales. Es en este contexto en el que deben enmarcarse los reconocimientos médicos en el ámbito laboral. Así lo ha interpretado el Tribunal Constitucional en su comentadísima sentencia 196/2004 de 15 de Noviembre (STC 196/04), criticada por excesivamente tuitiva por una parte de la doctrina y alabada por su claridad y contundencia por otra. En este caso el alto Tribunal otorga el amparo a una trabajadora que prestaba servicios en facturación y equipajes de un aeropuerto, cuyo contrato de trabajo temporal, subsiguiente a otros también de duración determinada, fue extinguido por no superación de periodo de prueba, tras la realización de un reconocimiento médico en el que fue calificada como NO APTA por los servicios médicos de la empresa. Se le había detectado a la trabajadora un coeficiente de cannabis de 292ng/ml, muy superior al 50 ng/ml recogido en el protocolo elaborado por la empresa como máximo permitido para la contratación de un trabajador de su categoría profesional. Ciertamente la trabajadora prestó su consentimiento a la realización del reconocimiento médico, aunque en ningún momento se le informó de que en los análisis médicos se examinará el posible consumo de estupefacientes. La sentencia 196/04 otorga el amparo a la trabajadora estimando la vulneración de su derecho fundamental a la intimidad,

El Tribunal Constitucional, recupera el concepto de "consentimiento informado de la Ley 41/2002de 14 de Noviembre.

Finalmente, debe señalarse que todas las cuestiones planteadas por el Tribunal Constitucional parten de la confidencialidad de los datos médicos obtenidos a los que solo tendrá acceso el personal médico y las autoridades sanitarias que lleven a cabo la vigilancia de la salud. El empresario solo será informado de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño de su puesto de trabajo.[39]

[38] AEPD – Informe 0299/2009
[39] Actualidad Jurídica Uría Menéndez / 13-2006

10. ESTADISTICA DE LA EVOLUCION DE LA PROTECCION DE DATOS EN LA EMPRESA

El Instituto Nacional de Tecnologías de la Comunicación INTECO, ha elaborado una encuesta sobre protección de datos en las empresas españolas (pequeñas y medianas empresas) con el objetivo de establecer un diagnóstico de la percepción del cumplimiento de la normativa vigente en materia de protección de datos personales.

El estudio sobre la protección de datos en las empresas españolas tiene por objetivo establecer un diagnóstico de la percepción de cumplimiento de la normativa vigente en matera de protección e datos personales por parte de la pequeña y mediana empresa española en 2012.

Para ello, se ha realizado una encuesta a los responsables de seguridad de 1.109 empresas españolas de menos de 250 empleados repartidas por todo territorio nacional. Los resultados de la encuesta han sido sometidos a la consideración de un grupo de expertos, cuyas aportaciones han sido esenciales para la comprensión de la situación del sector empresarial español.

Se exponen a continuación los puntos clave del análisis

EXISTENCA DE FICHEROS

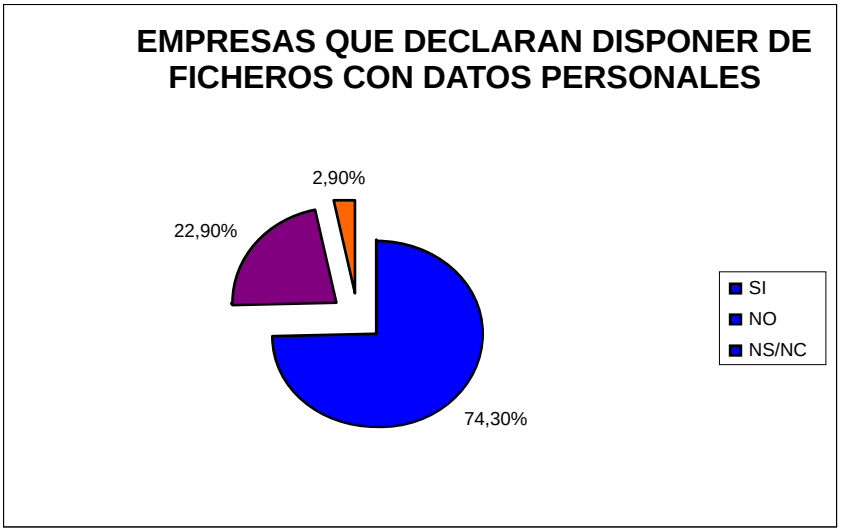
Las pequeñas y medinas empresas españolas trabajan habitualmente con ficheros de datos personales, especialmente las de mayor tamaño. Los ficheros más frecuentes son los de clientes y proveedores y los datos personales recogidos en ellos son datos de identificación y detalles de contacto.[40]

DISPOSICION DE FICHEROS DE DATOS DE CARÁCTER PERSONAL

- ***el 74,3 % de las empresas declara disponer de ficheros de datos de carácter personal***
- ***buena parte de las medianas y pequeñas empresas disponen de estos ficheros, mientras que en las microempresas se registra un porcentaje menor.***
- ***los expertos indican que prácticamente la totalidad de las empresas disponen de este fichero.***

[40] Estudio elaborado por INTECO-INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN.

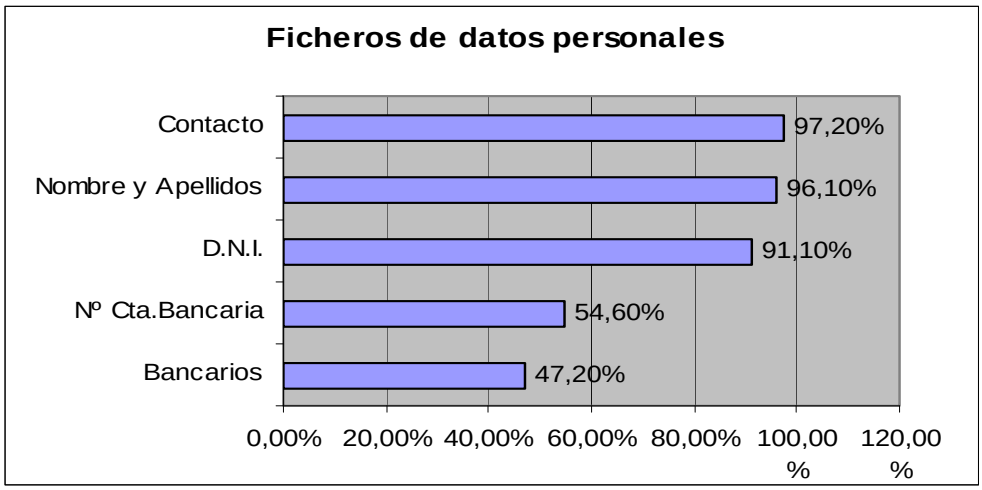
EMPRESAS QUE DECLARAN DISPONER DE FICHEROS CON DATOS PERSONALES



Fuente: INTECO

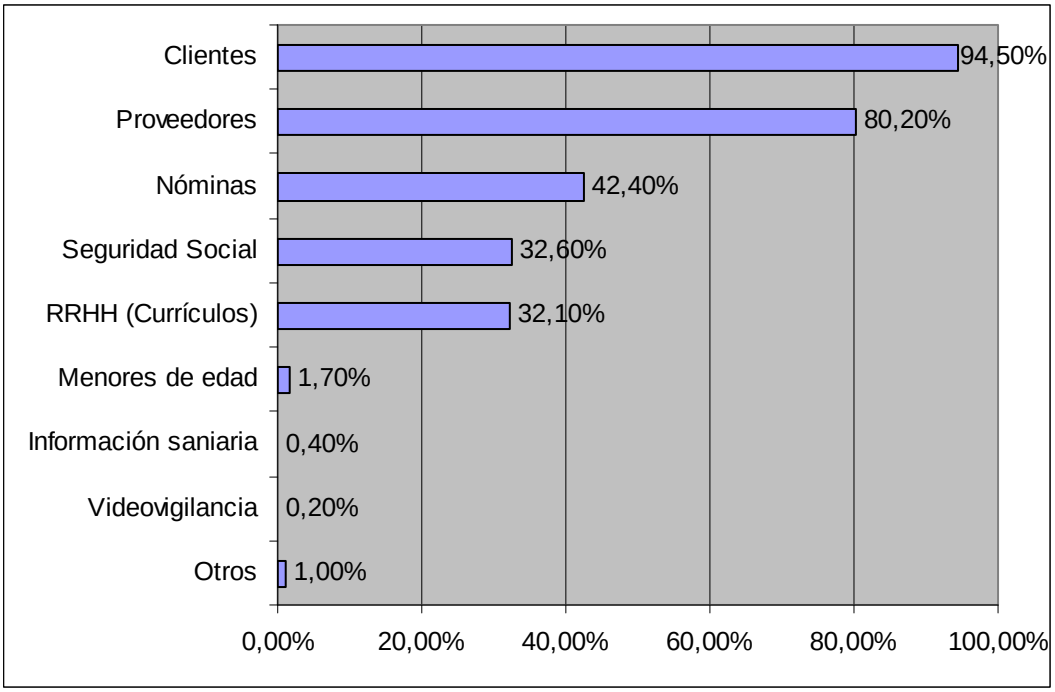
Las empresas españolas trabajan habitualmente con ficheros con datos personales (3 de cada 4) siendo los ficheros mas frecuentes los de clientes y proveedores (94,5 % y 80,2 %, respectivamente. Otros ficheros usados con frecuencia son los de nóminas, los archivos para seguridad social y los currículos de candidatos.

DATOS PRESENTES EN LA TOTALIDAD DE FICHEROS



Fuente: INTECO

FICHEROS HABITUALES: CLIENTES Y PROVEEDORES



Fuente INTECO

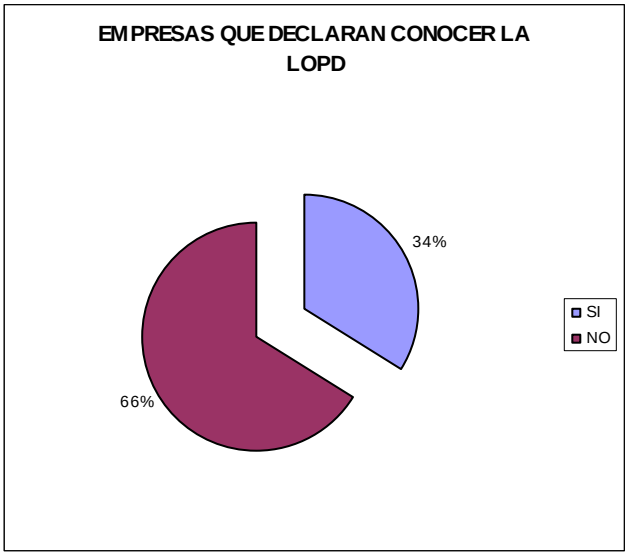
Entre las empresas que disponen de ficheros con datos personales, la gran mayoría dice utilizar ficheros de clientes y proveedores. Otro tipo de ficheros utilizados con menor frecuencia son los de nóminas, seguridad social y currículos.

CONOCIMIENTO DE LA NORMATIVA SOBRE PROTECCION DE DATOS

La práctica generalidad del colectivo de pequeñas y medianas empresas españolas conoce la LOPD y es consciente de su sujeción a la misma. Hay muchas más empresas conocedoras de la protección de datos en 2012 que en 2008, gracias a la intensa labor divulgativa de las autoridades de protección de datos.

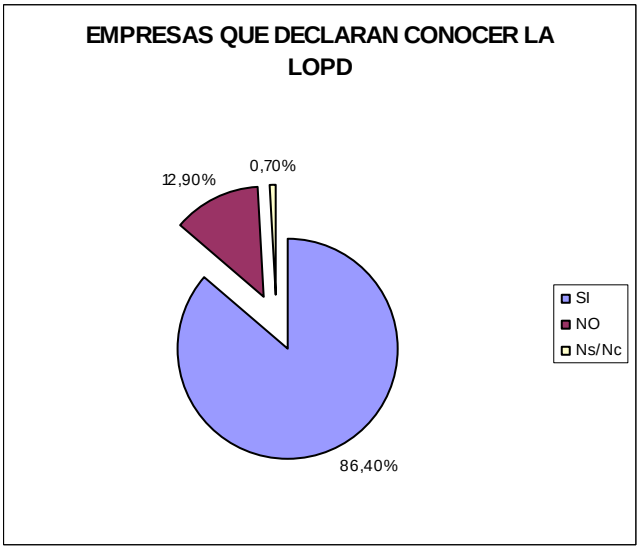
Desde 2008 a 2012, la evolución del grado de conocimiento de las empresas en materia de LOPD ha crecido sustancialmente, aumentando en más de 50 puntos.

AÑO 2008



Fuente; INTECO

AÑO 2012



Fuente INTECO

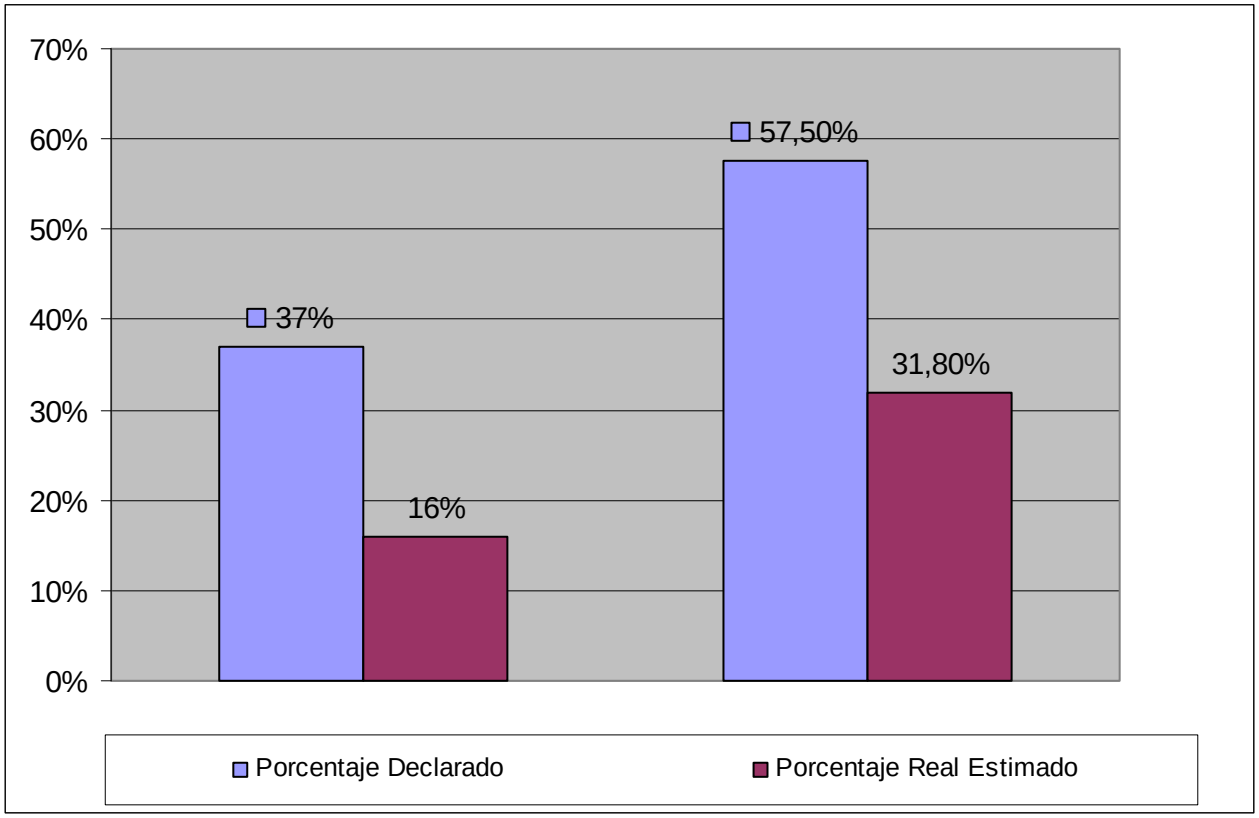
PERCEPCION DE ADOPCIÓN DE LAS OBLIGACIONES SOBRE PROTECCIÓN DE DATOS

Solo la mitad de las pequeñas y medianas empresas españolas manifiesta cumplir con todas las obligaciones que contempla la normativa española sobre protección de datos. No obstante, el grupo de expertos considera que el nivel de cumplimiento real de la LOPD es, en la mayoría de los casos, inferior al manifestado en la encuesta.

El 57,5 % de las empresas españolas con ficheros de datos de carácter personal afirma haber realizado la inscripción de los mismos en el registro General de Protección de Datos.

No obstante, poniendo en relación el número de entidades de titularidad privada que han registrado ficheros ante la AEPD con el total de empresas existentes en España, la estimación de INTECO es que sólo un 31,8% de las empresas españolas habría inscrito sus ficheros en la Agencia Española de Protección de Datos.

EMPRESAS QUE DECLARAN HABER INSCRITO FICHEROS EN LA AEPD Y CONTRASTE CON EL PORCENTAJE REAL ESTIMADO.2008-2012



Fuente: INTECO

DATOS DE LA AEPD RELATIVOS AL MES DE MAYO DE 2014

La divulgación que la AEPD ha realizado a lo largo de estos años ha sido realmente eficaz y se ven reflejados en los datos de la Agencia del mes de mayo. Solamente hago incidencia en ficheros inscritos de titularidad privada y de las empresas de Castila y León.

FICHEROS INSCRITOS EN EL RGPD DE CASTILLA Y LEON

	MAYO-2008	***MAYO 2012***	***MAYO 2014***
AVILA	3.976	161	9.618
BURGOS	9.736	198	23.579
LEON	11.636	275	31.508
PALENCIA	4.463	197	12.693
SALAMANCA	7.503	168	20.179
SEGOVIA	4.640	409	13.574
SORIA	2.567	53	7.230
VALLADOLID	12.384	387	34.873
ZAMORA	3.682	91	11.888

Resulta muy gratificante ver la evolución obtenida desde los años 2008 -2012 -2014, que será una garantía para poder cumplir con los requisitos exigidos en su conjunto, cuando se haga realidad la nueva normativa de la Unión Europea.

11. JURISPRUDENCIA DE LA UNION EUROPEA EN MATERIA DE PROTECCION DE DATOS

En 1981 se aprobó el Convenio nº 108 del Consejo, sobre la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal, primera norma europea que marcó las pautas del modelo común de protección de datos

Sobre la base de los principios aportados por el Convenio mencionado, fue aprobada en el ámbito comunitario la Directiva 95/46 CE del Parlamento y del Consejo de 24 de Octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La Directiva sienta las bases para lograr la coordinación de las legislaciones nacionales aplicables en materia de protección de datos en aras a garantizar la libre circulación de tales datos entre los Estados Miembros.

Los principios de protección de los derechos y libertades de las personas, y concretamente, del respeto a la intimidad, que se contienen en la directiva, vienen a ampliar los del Convenio, y así se desprende del Considerando 11 de la misma.

La directiva establece los principios y requisitos procedímentales que deberán considerarse exigencia mínima para que la protección sea adecuada. Hablamos de dos tipos de principios: los que se tendrán en cuenta en el momento de recoger los datos y los que se tendrán en cuenta durante el tratamiento o procesamiento de los datos.[41]

La Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos es, sin duda, la más importante.

Establece en su art. 25.1 que los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento, únicamente podrán efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones del derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

El artículo 25 de la Directiva en sus apartados 3 y 6, establece mecanismo de coordinación para asegurar el cumplimiento del nivel de protección adecuado.

En efecto, los Estados miembros y la Comisión se informarán recíprocamente de los casos en que un tercer país no garantiza un nivel adecuado de protección.

Así lo dispone el art. 44.4 c) en el que califica como infracción muy grave la transferencia a países que no proporcionen un nivel equiparable, sin autorización del Director de la Agencia española de Protección de Datos[42].

Pero evidentemente el mundo tecnológico avanza a pasos de gigante y hay que adaptar las normativas a los nuevos tiempos; así lo ha entendido el Parlamento Europeo que ya ha respaldado un nuevo paquete legislativo que adapta la norma europea de 1995 sobre protección de datos al mundo de Internet y las nuevas tecnologías.

Se busca reforzar el control de las personas sobre sus datos, armonizando el nivel de protección en toda la U.E.

La normativa incide fundamentalmente sobre las empresas, pero también acerca de las políticas de los Estados.

La protección de datos convenientemente protegida, debería ser una práctica habitual y no sólo una reacción ante nuevos cambios legislativos.

Para Ignacio Chico, Director de Iron Mountain España, las empresas están preocupadas y confusas por como gestionar sus datos, cumpliendo a la vez con la legislación vigente.

Este nuevo proyecto que se convertirá en el nuevo Reglamento Europeo de Protección de Datos debe de recibirse cono una llamada de atención para las empresas y aprovechar el tiempo para revisar y

[41] UOC –Universidad Oberta de Cataluña
ELISENDA BRU –Licenciada en Derecho
Revista de lo Estudios de Derecho y Ciencia Política de la UOC
ISSN 1699-8154 / Fecha de Consulta 20/05/2014

[42] MIGUELVIZCAINO CALDERÓN-Comentarios a la Ley Orgánica de Protección de Datos.
Civitas Ediciones S.L.-ISBN 84-470-1607-2

reforzar sus políticas de gestión de la información con el fin de situarse en posición adecuada para cumplir completamente con los cambios legislativos antes deque entren en vigor.

Los puntos esenciales son los siguientes:

1. Derecho al olvido La Comisión Europea defiende que los ciudadanos puedan solicitar que sus datos sean borrados si no desean que los siga procesando.
2. Consentimiento explicito La Comisión Europea propone que una empresa pueda procesar información personal solo si antes ha obtenido el permiso de la persona afectada. Tal permiso puede ser retirado en cualquier momento.
3. Transparencia, empresas y autoridades públicas, entre otros puntos también importantes.

Las empresas y las autoridades públicas deberían explicar con claridad sus políticas de protección de datos y disponer de un responsable si cuentan con al menos 250 empleados, según la propuesta de la Comisión Europea.

Según un estudio de Iron Mountain un 36 % de las medianas empresas en Europa y un 22% en España, admiten estar almacenando toda la documentación, independientemente de las directrices de conservación de documentos, solo por si la necesitan alguna vez. Más de la mitad de las empresas europeas (54%) creen que los requisitos para la protección de datos están cambiando tan rápidamente que nunca serán capaces de mantenerse actualizadas.

Esta revisión de la Unión Europea ha de ser un recordatorio para que estas empresas sean conscientes de que una legislación más dura esta a punto de hacerse realidad.

La nueva normativa afecta directamente a los temas relacionados con el permiso, la notificación de una brecha de datos y las consiguientes sanciones – hasta un 5% de la facturación global -, lo que significa un cambio drástico respecto a legislación vigente. Las empresas que fracasen en dar una solución a estos datos ahora, no solo corren el riesgo de tener que afrontar cuantiosas multas en el futuro próximo, sino también tendría que enfrentarse a serios daños para su reputación, lo que haría peligrar la retención de sus clientes.[43]

A continuación se establece en la tabla siguiente, un análisis comparativo de la legislación sobre protección de datos de cinco países europeos Alemania. Francia, Italia, Suecia y España. En ella se observa que España cuenta con el régimen sancionador mas duro de toda la Unión Europea y ello puede colocar a las empresas españolas en una situación de desigualdad frente a otras competidoras europeas.

La nueva legislación europea pretende eliminar las diferencias que separan los niveles de protección en los Estados Miembros para no obstaculizar el ejercicio desde una serie de actividades económicas a escala Europea. [44]

---

[43] www.Legaltoday.Com/Noticias

[44] UOC –Universidad Oberta de Cataluña
ELISENDA BRU –Licenciada en Derecho
Revista de lo Estudios de Derecho y Ciencia Política de la UOC

DETALLE DE LAS LEYES SOBRE PROTECCIÓN DE DATOS DE LO PAISES DE ALEMANIA, FRANCIA, ITALIA, Y SUECIA ADEMÁS DE ESPAÑA.
ESTA COMPARACCIÓN NOS DA UNA APROXIMACIÓN DE CÓMO SE HA IMPLANTADO EN LOS DIFERENTES ESTADOS LA DIRECTIVA 95/46, QUE DEJA UNA PUERTA ABIERTA NO SOLO AL TIPO DESANCIONES QUE PUEDAN PREVEERSE, SINO TABIEN AL SECTOR JURIDICO EN EL QUE PUEDEN INTEGRARSE.

PAIS	*LEY DE PROTECCIÓN DE DATOS*		*CODIGO PENAL*
ESPAÑA	*Arts. 44-45* *Infracciones leves 601,01 a 60.101,21 E.* *Infracciones graves: 60.101,21 a 300.506,05 E.* *Infracciones muy graves: 300.506,05 a 601.012,10 E.*		*1 a 4 años prisión+multa de 12 a 24 meses-tipo básico (Art.197.2 CP)* *2 a 5 años prisión - tipo agravado* *3 a 5 años prisión - tipo agravado encargado o responsable* *4 a 7 años prisión - tipo hiperagravado*
ALEMANIA	*párrafo 43* *Multa de 25.564 a 255.645 .*	*párrafo 44* *Hasta 2 años de cárcel o multa por las conductas del párrafo 43 realizadas con ánimo de lucro o con intención de perjudicar a un tercero*	*Párrafo 202a* *Espionaje e datos. Pena de prisión o multa no superior a 3 años*
FRANCIA	*art. 45 a 47* *Primera infracción multa no superior a 150.000 E.* *Infracción reiterada: multa no superior a 300.000 E.*		*Arts. 226-16 a 226-24* *Pena de prisión de 5 años+multa de 300.000 E.*
ITALIA	*arts. 161 a 165* *De 500 a 90.000 E.*		
SUECIA	*Multa de 6 meses a 2 años (sistema días multa)*		

Fuente: BRU,ELISENDA (2007) Revista de Internet, Derecho y Política. Nº 5
UOC – ISSN 1699-8154

12. CONCLUSIONES

Es innegable el avance de la tecnología y la trascendencia social e institucional que el derecho a la protección de datos de carácter personal ha adquirido en los últimos tiempos. Pese a ello, se abren grandes dudas e interrogantes en lo que respecta a la privacidad, al tratamiento y recogida de datos, video-vigilancia, Internet y redes sociales, etc. en el entorno laboral, que sin duda se irán resolviendo, con nueva normativa que cristalice la consolidación de una real y efectiva garantía de este derecho fundamental.

La Legislación española surgida para esta protección ha sido a mí entender, correcta y ha apostado por el compromiso de garantizar derechos y establecer exigencias para las posibles vulneraciones que pudieran producirse en el cumplimiento de esos derechos.

Es un camino difícil, sin duda, donde aún queda mucho por hacer. En lo que respecta al mundo empresarial, sobre todo en la pequeña y mediana empresa, hay grandes dudas sobre cómo ejercer esas obligaciones y derechos para gestionar con el rigor necesario el compromiso de consolidación de una cultura en la protección de datos.

Corresponde a los poderes públicos y autoridades competentes en la materia, promover iniciativas y actuaciones para fomentar la efectiva garantía, objetivos estratégicos para fortalecer la calidad del tratamiento de los datos personales.

Harán falta más esfuerzos normativos que secunden a la directiva 95/46 CE. Para acercar las aún distantes leyes de protección de datos de los diferentes Estados Miembros, el Parlamento Europeo ha respaldado un nuevo paquete legislativo que adapta la norma europea de 1995 sobre protección de datos al mundo de Internet y las nuevas tecnologías. Las nuevas reglas buscan reforzar el control de las personas sobre sus datos, armonizando el nivel de protección en toda la UE. Espero que se alcance el objetivo que se han propuesto, para seguir creciendo en calidad y eficacia, con el fin de garantizar a los ciudadanos un equilibrio entre nuevos avances tecnológicos, que sin duda habrá, y seguridad jurídica.

BIBLIOGRAFÍA

- AEPD . Informe 0299/2009. Madrid. Año 2009. WWW.AEPD.ES

- AEPD. Guía de las Relaciones Laborales. Madrid. WWW.AEPD.ES

- BRU, Elisenda. (2007) "*La Protección de Datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad*". En "III Congreso Internet. Derecho y Política (IDP). Revista de Internet, Derecho y Política. Nº 5. UOC – ISSN 1699-8154

- CANALES GIL, Álvaro. Revista Jurídica de Castilla y León. Nº 12. Abril 2007

- INTECO. Instituto Nacional de Tecnologías de la Comunicación. "*Estudio sobre la Protección de Datos en las Empresas Españolas".Octubre. Año 2012.*

- BUISAN GARCIA, Nieves, FERNANDEZ GARCIA, José Antonio, GUERRERO ZAPLANA, José, LESMES SERRANO, Carlos, SANCHEZ CALVO, Lourdes. "*La Ley de Protección de Datos. Análisis y Comentarios a su Jurisprudencia*.LEX NOVA.ISBN 978 84*85012-91-6.

- MALPARTIDA MORANO, José, PRADAS MONTILLA, Ricardo. Boletín de la Facultad de Derecho" nº 18.201. "*Empresas y Protección de Datos de Carácter General".*

- PÉREZ SERNA, Jesús. "*Control del Correo Electrónico*". Publicado en Internet un Viernes, enero 15 th 2010-I-SPY.

- PRODAT. Guía Básica de Protección de Datos de Carácter Personal.

- RODRIGUEZ ESCANCIANO, Susana. Curso: ”*Libertad Sindical. Nuevas Tecnologías*”. Catedrático de Derecho del Trabajo y de la Seguridad Social de la Universidad de León.

- SERRANO PÉREZ, M. Mercedes.”*El Derecho Fundamental a la Protección de Datos. Derecho. Español y Comparado*”. Thomson Civitas 2003.

- URÍA MENÉNDEZ. Abogado. Artículo de la Revista: Actualidad Jurídica/ 13-2006

- VALLS, Ramón. “*Correo Electrónico*”. Escrito 17 Diciembre 2013.

- VIZCAINO CALDERÓN, Miguel.”*Comentarios a la Ley Orgánica de Protección de Datos*. Civitas Ediciones, S.L.-ISBN 84-470-1607-2.