# Efectos de la Protección de Datos de Carácter Personal en la Gestión de Recursos Humanos

**Simón Mesanza Legarda**
**Secretario General de la Agencia Vasca de Protección de Datos**

**Junio 2007**

## Sumario

**Página**

# I. El DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

| | |
|---|---|
| ***Es un DERECHO FUNDAMENTAL que nace con el desarrollo de las nuevas tecnologías de la información*** | • *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".(**Art. 18.4 CE)*<br>• *A partir del artículo 18.4 de la Constitución y de la jurisprudencia del Tribunal Constitucional, se ha configurado el derecho a la protección de datos de carácter personal como un **derecho fundamental,** diferenciado del derecho al honor y a la intimidad.*<br>• *Diferenciar la esfera íntima (derecho a la intimidad) de la privada (derecho a la protección de datos). Binomio **intimidad privacidad** ("aspectos más recónditos de la personalidad"-cualquier dato relativo a una persona que lo identifique).*<br>• ***Art. 8 Carta de Derechos Fundamentales de la Unión Europea**. Niza 7 diciembre 2000. "toda persona tiene derecho a la protección de los datos de carácter personal que lo conciernan".* |
| ***Consiste en*** | • Proteger los datos que identifican o permiten identificar a una persona.<br>• Asegurarse que la persona **sepa, consienta y pueda disponer** de sus datos y del uso que se hace de ellos. |
| ***Respecto del cual, las administraciones y empresas tendrán en cuenta*** | • Que **los datos personales pertenecen a las personas a** las que se refieren y sólo ellas pueden decidir sobre los mismos, **y no a los diferentes servicios o departamentos que los utilizan**.<br>• Que sólo se podrán utilizar respetando en todo caso la normativa sobre protección de datos de carácter personal. |

# II. UN ACERCAMIENTO A LA CUESTIÓN A TRAVÉS DE LA PARADOJA

## II.1. TECNOLOGÍA Y TRABAJO

| **Época de grandes avances tecnológicos** | **Incremento de amenazas para los derechos de los trabajadores** |
|---|---|

| **Antes** | **Ahora** |
|---|---|
| Procesos de más desgaste físico | Como el trabajo es "menos físico" se pueden acelerar los procesos |
| Concepto estricto de subordinación | Se relativiza la subordinación. Se tiende a confundir vida laboral y vida privada |
| Trabajo localizado | Descentralización productiva y "deslocalización" |
| Control "físico" y visual | El "ojo electrónico": control más tecnológico: videovigilancia, seguimiento actuaciones en Internet o correo electrónico |
| Control periférico, discontinuo y parcial | Control centralizado, en cada instante, y que puede dejar rastro permanente en la máquina |
| Selección por sistemas tradicionales | Selección por perfiles de personalidad, e incluso por datos genéticos |

El riesgo de esta nueva sociedad ligada al mundo de la tecnología nos puede conducir al **TRABAJADOR TRANSPARENTE**, ese trabajador, o, lo que es más grave, ese potencial trabajador, conocido, evidente en su actuación presente y en su actuación futura. La planificación será perfecta, no habrá espacio para la improvisación, nuestras vidas (también nuestra vida privada) serán transparentes.

## II.2. DERECHOS CONCURRENTES. LIBERTAD DE EMPRESA FRENTE A PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

| **Derecho a la libertad de empresa** | **Derecho fundamental a la protección de datos personales** |
|---|---|
| Es una facultad (la principal) del empresario | Es un derecho fundamental del trabajador |
| **Art. 38 CE.** Establece la libertad de empresa. Habla de productividad y planificación. Viene a facultar al empresario para velar por el buen hacer de su empresa y a ejercer un control sobre sus herramientas de trabajo puestas a disposición del empleado | |
| **Art. 20.3 ET** *el empresario podrá adoptar las medidas más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales guardando, en su adopción y aplicación, la consideración debida a su dignidad humana* | |

STC **129/1989, de 17 de Julio…"***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 éstos 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*"

STC **99/1994** "*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"*

## II.3. LA PROTECCIÓN DE DATOS Y LA SOCIEDAD O CUANDO PARECE QUE EL DERECHO SE ADELANTA A LA REALIDAD SOCIAL

| **Hay normativa suficiente en materia de protección de datos** | **Esta vez parece que el derecho se ha adelantado a la realidad social** |
|---|---|
| Existe una legislación europea, estatal y en 3 CCAA | Un gran número de ciudadanos desconocen la existencia del derecho |
| Existen leyes en tres comunidades autónomas. Empiezan a incluirse referencias al derecho en los estatutos de autonomía de nueva generación | Ni las administraciones, ni las empresas, han incorporado a sus culturas de gestión la protección de datos. |
| Se han creado autoridades de control en el Estado y en las Comunidades autónomas de Cataluña, Madrid y País Vasco | Falta de sensibilización social sobre la cuestión |

## II.4. DOS VISIONES DE LA PROTECCIÓN DE DATOS: UNA OPORTUNIDAD O UNA AMENAZA

| **La protección de datos de carácter personal es una oportunidad para mejorar los procesos organizativos dentro de la Administración o la Empresa** | **Es más burocracia para las Administraciones** |
|---|---|
| Como Administración o empresa me permite reinventar mis procesos de planificación | Complica mis procesos al incluir nuevos puestos especializados en la organización |
| Contribuye a la mejora de la organización porque me hace re-estudiar mis circuitos de información | Hace los procesos más largos y más farragosos |

# III. LOS DATOS PERSONALES RELACIONADOS CON LOS RRHH

| | |
|---|---|
| ***LOPD. Art. 3.*** | *"Cualquier información concerniente a personas físicas identificadas o identificables"* |
| ***Grupo del Art. 29. Recomendación 1/2001 sobre datos de evaluación de los trabajadores*** | *"Todo tipo de información sobre una persona física identificada o identificable tal como los datos relacionados con su identidad física, fisiológica, o psíquica, económica, cultural o social"* |

| **FICHEROS Y DATOS MÁS UTILIZADOS RELACIONADOS CON EL ÁMBITO DE LOS RRHH** | |
|---|---|
| ***Fichero RRHH*** | • Personales (apellidos, nombre, DNI, Domicilio), de estado civil, número de hijos,…<br>• Relativos a la vida laboral/profesional. Puestos desempeñados.<br>• De titulaciones, académicos y de formación. Cursos recibidos e impartidos<br>• Administrativos: relación de empleo, situación administrativa, datos de la selección, datos de provisión<br>• De licencias y permisos con fechas de disfrute |
| ***Ficheros de Seguridad social y/o económicos*** | • Retribuciones<br>• Retenciones impuestos<br>• Cotizaciones a SS<br>• Número de hijos<br>• Afiliación sindical y descuento de cuota sindical<br>• Discapacidades de hijos<br>• Obligación de pagar pensión por resolución judicial<br>• Estado civil<br>• Número de hijos<br>• Número de cuenta de entidad bancaria<br>• Número de días de baja<br>• Si ha sido enfermedad común o profesional |

| | |
|---|---|
| ***Servicios Médicos (datos especialmente protegidos)*** | • Ficheros de salud laboral<br>• Datos de distintas revisiones médicas<br>• Datos aportados voluntariamente para su utilización en prevención y vigilancia<br>• Discapacidades del propio trabajador |
| ***Otros datos o ficheros personales relacionados con las nuevas tecnologías en el trabajo*** | • Datos biométricos<br>• Datos de videovigilancia<br>• Datos de vigilancia del correo electrónico<br>• Datos de vigilancia de acceso a Internet<br>• Datos relacionados con el teletrabajo<br>• Datos genéticos<br>• Datos relacionados con el RFID |

# IV. SUJETOS O AGENTES QUE INTERVIENEN EN EL TRATAMIENTO DE DATOS PERSONALES DE LOS RRHH

| | |
|---|---|
| ***Sujetos*** | • *Los empleados públicos, trabajadores o candidatos.*<br>• *Los becarios y alumnos en prácticas.*<br>• *El Responsable del fichero.*<br>• *Los trabajadores de RRHH como gestores de los datos de los ficheros.*<br>• *El personal sanitario encargado de la Seguridad y Salud Laboral.*<br>• *Encargados de tratamiento. Especial referencia a empresas que se encarguen de la vigilancia de la salud o de la selección de personal*<br>• *Los Sindicatos y los represantes de los trabajadores.*<br>• *Otras administraciones receptoras de datos por mandato legal (Hacienda, Seguridad Social,…)* |

# V. Obligaciones de las Administraciones y su personal

## *V.1. Antes de recoger datos personales, es necesario…*

| | |
|---|---|
| ***Crear el fichero y publicarlo en el Boletín***<br>Art.20 LOPD | La creación del fichero corresponde al responsable del fichero mediante disposición de carácter general, que ha de ser publicada en el Boletín Oficial del Territorio Histórico.<br><br>Las disposiciones de creación o de modificación de ficheros deberán indicar:<br>➢ La finalidad y los usos del fichero.<br>➢ Las personas de las que se obtendrán datos.<br>➢ El procedimiento de recogida de los datos.<br>➢ La estructura básica del fichero.<br>➢ La descripción de los tipos de datos.<br>➢ Las cesiones de datos de carácter personal.<br>➢ Las transferencias de datos a países terceros.<br>➢ La Administración *o algún órgano de la misma* como responsable del fichero.<br>➢ El servicio, sección, unidad, órgano o cargo donde se puede ejercitar los derechos de acceso, rectificación, cancelación y oposición.<br>➢ El nivel de seguridad y las medidas de seguridad aplicables. |
| *Declararlo en la AVPD para su inscripción en el Registro de Protección de Datos de Euskadi*<br>**Art.18-2**<br>**Ley 2/2004** | • Una vez publicada en el Boletín del Territorio Histórico la disposición de creación, se notificará a la Agencia Vasca de Protección de Datos para su **inscripción en el Registro de Protección de Datos (**vale también para la AEPD**)**<br>• A través de la página Web de la AVPD (www.avpd.es) existe la posibilidad de obtener un **programa de auto declaración**, así como instrucciones para cumplimentar los formularios.<br>• Asimismo, en la misma página, en el **Registro de Protección de Datos de Euskadi** se podrán consultar las características de los ficheros creados y declarados por las Administraciones. |

## *V.2. En la recogida de datos personales*

| | |
|---|---|
| ***Formas de obtener la información*** | • **En función del origen**<br>➢ Del propio trabajador<br>➢ De fuentes accesibles al público<br>➢ De terceras empresas encargadas del tratamiento<br>• **En función del proceso**<br>➢ Procesos selectivos o de creación de bolsas<br>➢ Procesos provisorios<br>➢ Procesos de gestión ordinarios: licencias y permisos, situaciones administrativas, control horario, salud laboral, formación, … |
| *Informar*<br>**Art.5 LOPD** | • **El empleado** al que se soliciten datos personales deberá ser **previamente informado** de la existencia del fichero, de su finalidad, de eventuales cesionarios, del responsable y de la posibilidad y ante quién puede ejercer sus derechos.<br>• **Cuándo informar.** Cuando se solicita información verbal o por escrito.<br>• **Cómo informar.** La cláusula informativa debe aparecer en el contrato de trabajo. Se debe incluir también en anexos que modifiquen las condiciones y las resoluciones referentes a situaciones administrativas donde se recaben datos de carácter personal. |

| | |
|---|---|
| **Solicitar el consentimiento de la persona**<br>*Art.6 LOPD* | • *El tratamiento de los datos de carácter personal requerirá el **consentimiento** inequívoco de la persona afectada, salvo que la ley disponga otra cosa. Así, según el artículo **6.2. LOPD** no será preciso el consentimiento cuando:*<br>➢ *Los datos se recojan para el ejercicio de las funciones propias de la Administración en el ámbito de sus competencias.*<br>➢ ***Se refieran a una relación** negocial, **laboral o administrativa** y sean necesarios para su mantenimiento o cumplimiento.*<br>➢ *Su tratamiento tenga por finalidad proteger un interés vital de la persona interesada.*<br>➢ *Los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por la Administración o por el de tercera persona a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales de la persona interesada.*<br>• ***Informe 8/2001 del Grupo del Artículo 29**, apartado 10*<br>➢ *el consentimiento del trabajador debe ser otorgando con total independencia y libertad*<br>➢ *cuando sea necesario el consentimiento de un trabajador y de su negativa a prestarlo se deriven perjuicios reales o potenciales para el interesado, el consentimiento no será válido aunque se satisfagan los artículos 7 y 8 ya que dicho consentimiento no ha sido prestado libremente.* |
| ***Respetar el principio de calidad***<br>Art.4 LOPD | • Los datos solicitados serán **adecuados, pertinentes y no excesivos** en relación con la finalidad de la actividad laboral para la que se hayan obtenido.<br>• Los datos de carácter personal objeto de tratamiento **no podrán usarse para finalidades incompatibles** con aquellas para las que hubieran sido recogidos.<br>**STS 11/1998 de 13 de enero** CASO RENFE estableció claramente la imposibilidad de utilización desviada de una dato para un fin distinto (dato de afiliación sindical para descuento de huelga)<br>• Los datos podrán utilizarse después de un tratamiento con fines históricos, estadísticos o científicos.<br>• Serán **exactos y puestos al día**, de forma que respondan con veracidad a la situación actual de las personas afectadas. Durante la vida del fichero la administración tiene que respetar siempre la finalidad para la cual fueron recabados y mantenerlos actualizados. |

| | |
|---|---|
| *Mostrar una especial atención en la recogida de datos especialmente protegidos*<br>**Arts.7 y 8 LOPD** | • **Los datos de carácter personal que se refieran a la vida sexual, salud u origen racial** de las personas sólo serán recabados, tratados y cedidos cuando por razones de interés público así lo establezca una ley o la persona interesada consienta expresamente.<br>• Respecto a los **datos personales relativos a la salud**, el personal al servicio de la administración o empresa directamente relacionado con la salud de las personas podrá tratar los datos de carácter personal relativos a la salud de las personas, de acuerdo con lo dispuesto en la normativa vigente en materia de sanidad y de protección de la salud y prevención de riesgos laborales.<br>• El tratamiento de **datos relativos a ideología, religión, creencias y afiliación sindical,** requiere el consentimiento expreso y por escrito de la persona interesada. |

| ***V.3. Durante el tratamiento y utilización de los datos por la organización responsable o un encargado de tratamiento*** | |
|---|---|
| ***Facilitar a las personas el ejercicio de sus derechos*** | • Las administraciones o empresas deben facilitar a las personas el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición y, en su caso, el de impugnación de valoraciones (**Arts. 15 a 19 LOPD**)<br>• Es recomendable establecer modelos y procedimientos para hacer posible el ejercicio del derecho |
| *Realizar un contrato por escrito con encargados de tratamientos*<br>**Art.12-2 LOPD** | • Supuestos más frecuentes de encargo de tratamiento en la gestión de RRHH :<br>➢ Gestión de Seguridad y Salud Laboral<br>➢ Gestión de Sistemas Selectivos o Provisorios<br>➢ Desarrollo y mantenimiento de aplicativos informáticos relacionados con la gestión de RRHH<br>➢ Formación<br>➢ Envío de documentación (empresas de mailing)<br>➢ Elaboración de la nómina por asesorías externas<br>➢ Entidades financieras para coordinar el pago de nómina<br>• Cuando se realice a la Administración o empresa la prestación de un servicio en virtud del cual posibilite el acceso a datos personales de los que es responsable, habrá de formalizarse un contrato por escrito, conforme a lo establecido en el artículo 12 LOPD, concretándose expresamente :<br>➢ Qué datos o categorías de datos se facilitan a la empresa contratada.<br>➢ Cómo deben tratarse lo datos.<br>➢ Obligaciones de la empresa adjudicataria |

## *V.4. Cuando cedan, comuniquen o faciliten la salida de los datos recabados*

| | |
|---|---|
| ***Supuestos más frecuentes de cesiones de datos de RRHH*** | • Cesión a Administraciones Públicas<br>➢ Administración tributaria<br>➢ Administración de la Seguridad Social<br>➢ Otras entidades de Función Pública o RRHH<br>➢ A otros órganos administrativos<br>• Cesión a Ministerio Fiscal, Jueces o Tribunales<br>• Cesión a entidades bancarias para el pago de la nómina<br>• Cesión a organizaciones sindicales<br>• Traslado de referencias de personal |
| ***Supuestos más frecuentes de difusión y publicidad datos de RRHH*** | • Publicidad y difusión de resultados de procesos selectivos y provisorios<br>• Difusión de directorios telefónicos<br>• Difusión de directorios de Internet |
| *Cumplir estrictamente el deber de secreto profesional*<br>**Art. 10 LOPD**<br>**Art. 53-12 EEP**<br>**Art. 95-2 e) EEP** | • Toda persona empleada que intervenga en cualquier fase del tratamiento de los datos de carácter personal de ficheros de la Administración está obligada al **secreto profesional** respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar su relación con la Administración.<br>• El incumplimiento del deber de secreto será sancionado de conformidad con lo previsto en la legislación vigente y traerá consigo, en su caso, las responsabilidades penales, disciplinarias y, ante terceros, que la misma establece. |

| | |
|---|---|
| **Solicitar el consentimiento de la persona cuyos datos se quieren ceder**<br>*Art. 11 LOPD* | • *Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a otra administración, empresa o a una tercera persona para el cumplimiento de fines directamente relacionados con las funciones legítimas de la Administración y/o empresa y de quien los ha solicitado, con el previo consentimiento de la persona interesada.*<br>• *El consentimiento no será preciso:*<br>➢ *Si la cesión está autorizada en una ley.*<br>➢ *Si son datos de fuentes accesibles al público.*<br>➢ *Si el tratamiento responde 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.*<br>➢ *Si la comunicación que deba efectuarse tiene por destinatario:*<br>▪ *El Defensor del Pueblo o el Ararteko.*<br>▪ *El Ministerio Fiscal o los Jueces o Tribunales.*<br>▪ *El Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas, o el Tribunal Vasco de Cuentas Públicas.*<br>➢ *Si la cesión se produce entre administraciones públicas y tiene por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.*<br>➢ *Si la cesión de datos de carácter personal relativos a la salud es necesaria para solucionar una urgencia o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.* |

## V.5. En todo momento, adoptar las medidas técnicas y organizativas que garanticen la seguridad de los datos (Art. 9 LOPD)

| | | | |
|---|---|---|---|
| | - Nivel básico: ficheros con datos de carácter personal.<br>- Nivel medio: ficheros con datos relativos a infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por el art. 29 de la LOPD (inf. de servicios de solvencia y crédito).<br>- Nivel alto: ficheros con datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas. | | |
| *DOCUMENTO DE SEGURIDAD* | - Implanta la normativa de seguridad especificando el ámbito de aplicación, las funciones y obligaciones de personal y los procedimientos existentes en la organización.<br>- Se debe mantener actualizado en lo referente a la normativa y la organización. | - Identificación del responsable de seguridad (1 o varios)<br>- Control periódico del cumplimiento del documento.<br>- Medidas a adoptar en caso de reutilización o desecho de soportes. | |
| *PERSONAL* | - Funciones y obligaciones claramente definidas y documentadas.<br>- Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento. | - | - |
| *REGISTRO DE INCIDENCIAS* | - Registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados. | - Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente.<br>- Autorización por escrito del responsable del fichero para ejecutar procedimientos de recuperación de datos. | |
| *IDENTIFICACIÓN Y AUTENTICACIÓN* | - Relación actualizada de usuarios y accesos autorizados.<br>- Procedimientos de gestión de contraseñas periodicidad con que se cambian.<br>- Caducidad de contraseñas y almacenamiento ininteligible de las mismas. | - Se establecerá el mecanismo que permita la identificación de todo usuario y la verificación de que está autorizado.<br>- Límite de intentos reiterados de acceso no autorizado. | |
| *CONTROL DE ACCESO* | - Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones.<br>- Existirán mecanismos que aseguren lo anterior y que gestionen la concesión de permisos de acceso sólo por personal autorizado en el Documento de Seguridad. | - Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información. | |
| *GESTIÓN DE SOPORTES* | - Identificar el tipo de información que contienen.<br>- Inventario.<br>- Almacenamiento con acceso restringido<br>- Salida de soportes autorizada por el responsable del fichero. | - Registro de entrada y salida de soportes.<br>- Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado.<br>- Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento. | - Cifrado de datos en la distribución de soportes. |
| *COPIAS DE RESPALDO Y RECUPERACIÓN* | - Existirá un procedimiento de copias de respaldo y recuperación de datos.<br>- Garantiza la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción.<br>- Copia de respaldo, al menos semanal. | - | - Copia de respaldo y de los procedimientos de recuperación en lugar diferente del que se encuentren los equipos. |
| *RESPONSABLE DE SEGURIDAD* | - | - Encargado de coordinar y controlar las medidas del documento.<br>- No supone delegación de responsabilidad por parte del responsable del fichero. | |
| *PRUEBAS CON DATOS REALES* | - | - Solo con datos reales si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado. | |
| *AUDITORIA* | - | - Al menos cada dos años, interna o externa.<br>- Dará lugar a un informe de auditoría que es analizado por el responsable de seguridad. | |
| *REGISTRO DE ACCESOS* | - | - | - Registrar datos de cada acceso.<br>- Conservación 2 años.<br>- Informe mensual del responsable de seguridad. |
| *TELECOMUNICACIONES* | - | - | - Transmisión de datos cifrada. |

Nuevo Proyecto de Reglamento de desarrollo de la LOPD contempla considerar a todos los ficheros de nómina como de nivel básico

| ***V.6. Al finalizar el tratamiento*** | |
|---|---|
| *Cancelar los datos*<br>**Art. 4.5 LOPD** | • Finalizada la relación se tendrá que proceder a su bloqueo hasta que finalice el plazo de prescripción de acciones judiciales y, posteriormente, a su cancelación |

# VI. Algunas cuestiones del máximo interés

## *VI.1. La protección de datos de carácter personal y los sindicatos y representantes de los trabajadores*

| | |
|---|---|
| ***Necesidad sindical*** | • El **art. 63 ET** establece que *"el comité de empresa es el órgano representativo y colegiado del conjunto de los trabajadores en la empresa o centro de trabajo para la defensa de sus intereses"*<br>• El **art. 7 CE** determina que "*Los Sindicatos… contribuyen a la defensa y promoción de los intereses económicos y sociales que le son propios".*<br>• El **art. 10.3 LOLS** otorga a los delegados sindicales las mismas garantías si no forman parte del Comité.<br>• La **STS de Justicia de la CAPV de 16 de Mayo de 2006** ratifica la posición de las Secciones Sindicales como asimilada a la de los representantes de los trabajadores<br>• Necesidad de diferenciar entre<br>➢ Representacíon de trabajadores de la empresa y<br>Comités de empresa (laborales)<br>Delegados de personal y Juntas de Personal (funcionarios Art. 39 Estatuto del Empleado Público)<br>➢ Representación de trabajadores afiliados<br>Secciones Sindicales y Delegados sindicales<br>• Los sindicatos tienen necesidad de datos personales para el desarrollo de sus funciones: identificativos, laborales, administrativos, económicos,…<br>• Interés de la Recomendación 17/2006 de APDCM |
| *¿Existe cesión de datos?* | • Las Juntas de Personal, los Delegados y el Comité **no forman parte de la empresa**, porque no existe vinculación jerárquica o de tutela con el responsable del fichero.<br>• Estamos ante un supuesto de **cesión de datos** |

| | |
|---|---|
| **Concurrencia de derechos** | • *Concurren el derecho a la protección de datos de carácter personal (**art. 18.4 CE** y su desarrollo jurisprudencial y por LO), el principio de libertad sindical y garantía de los derechos de los trabajadores (**art. 28 CE**) y el de Libertad de Empresa (**art. 38 CE**)*<br>• *Los derechos fundamentales no son absolutos sino que están sometidos a límites*<br>• *Según la **STC 292/2000 de 30 de Noviembre** el "derecho a la protección de datos personales no es ilimitado y sus límites hay que encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la constitución". Los limites:*<br>➢ *Tienen que estar establecidos por ley (53,1 y 81 de CE)*<br>➢ *Tienen que responder a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos*<br>➢ *Tienen que respetar el contenido esencial del derecho fundamental a la protección de datos personales* |
| ***No necesidad de consentimiento para cesión de datos a sindicatos*** | • Excepción artículo **11 LOPD**: cuando norma con rango de ley establezca la posibilidad de entrega o manejo de datos. El **Art. 64 ET** establece las competencias del Comité de Empresa:<br>➢ Ser informados trimestralmente de las situación de la entidad en su sector económico<br>➢ Recibir copia básica de los contratos<br>➢ Funciones de información económica sobre la marcha de la empresa. Conocer balance, cuenta de resultados, memoria y documentos de la sociedad.<br>➢ Emitir Informe previo sobre:<br>❖ Reestructuración plantillas<br>❖ Reducciones de jornada<br>❖ Traslado de instalaciones<br>❖ Planes de formación<br>❖ Implantación de sistemas de organización y control de trabajo<br>❖ Funciones de vigilancia del cumplimiento por parte del empresario de la normativa laboral, de ss y de seguridad e higiene<br>➢ Emitir informe sobre absorción, fusión o modificación de estatus de la empresa<br>➢ Incidencia del empleo en la empresa<br>• En muchos casos es suficiente con dar información general disociada, sin necesidad de dar datos personales |

| | |
|---|---|
| ***Cesión de datos para elecciones sindicales*** | • El Censo de electores se deberá trasladar a los miembros de las mesas electorales<br>• Las mesas harán público el censo<br>• Los datos del listado: Apellidos, nombre, fecha de nacimiento.<br>• **Informe CN 29/2006 de la AVPD**<br>• Sistemas de difusión: tablones de anuncios, intranet. En ningún caso páginas Web en abierto.<br>• Aun cuando **NO** se contempla expresamente la cesión a los sindicatos, algunos interpretan que es necesaria para poder realizar la campaña sindical. En el supuesto que se admitiera, el principio de calidad implicaría que los Sindicatos no podrían utilizarlo para finalidades distintas a la campaña electoral y deberían cancelar la información una vez finalizado el proceso |
| *Cuestión controvertida respecto de la Cesión de datos salariales y del complemento de productividad* | • **STC de 22 abril 1993** avala el acceso a datos salariales<br>• **STSCM de 6 Julio 1995**, establece que los representantes no tienen derecho a recibir información sobre masa salarial del trabajador<br>• El art. **23-3c de Ley 30/1984** Y el **80 de la LFPV** establecía que el Complemento de Productividad debía ser conocido por representantes de trabajadores o por organizaciones sindicales y por el resto de los trabajadores. Ha desaparecido en el estatuto del empleado público<br>• **Informe CN11/2005 de la APVD**. Aquellos artículos se referían al conocimiento público de las retribuciones de los funcionarios, pero no autorizaban la cesión de datos retributivos individualizados. |

| | |
|---|---|
| ***Cesión de datos de RPT con información agregada de los trabajadores*** | • *El **art. 74** (que parece sustituir al antiguo 15 de la Ley 30/1984, no específicamente derogado) **del Estatuto del Empleado Público** contempla que "Las Administraciones Públicas estructurarán su organización a través de relaciones de puestos de trabajo u otros instrumentos organizativos similares que comprenderán, al menos, la denominación de los puestos, los grupos de clasificación profesional, los cuerpos o escalas, en su caso, a que estén adscritos, los sistemas de provisión y las retribuciones complementarias. Dichos instrumentos serán públicos."*<br>• *La RPT contiene características de los puestos de trabajo y no información agregada de los titulares de los mismos*<br>• *Para informar de los titulares de los puestos y de sus datos personales (apellidos, nombre, DNI, lugar de trabajo) será necesario el consentimiento previo de los trabajadores.*<br>• *Algunos discrepan y consideran que para que los representantes de los trabajadores puedan cumplir la función encomendada por el **art. 64 ET** y por otra normativa sectorial de INFORMAR a los trabajadores de las cuestiones que tengan repercusión en las relaciones laborales es necesario que conozcan estos datos. En este supuesto será necesario decidir en función de cada petición para armonizar derechos.*<br>• ***Informe CN3/2007 de la APVD**.* |
| ***Cesión de datos relativos a bajas, absentismo laboral y régimen disciplinario*** | • El **art. 39.2 c de LPRL** autoriza la cesión a los delegados de prevención del Comité de Seguridad e Higiene de un listado de nombres y accidentes<br>• El Comité de Empresa tiene derecho a conocer el nivel de absentismo, pero puede hacerse a través de datos disociados, o sea a través de estadísticas, sin necesidad de facilitar datos personales<br>• El a**rt. 64 1 7 del ET** establece la necesidad de informar a los representantes de los trabajadores sobre las sanciones por faltas graves, sin necesidad de tener el consentimiento del expedientado. |
| *Cesión de datos de cotizaciones a SS y cuota sindical* | • Obligación legar de cumplimentar los datos TC1 y TC2 a TGSS<br>• Es necesario hacer público el listado con la relación nominal de los trabajadores<br>• Existe la posibilidad de sustituirla por su traslado a los representantes de los trabajadores<br>• Según el **art. 11.2. LOLS** existe la posibilidad de descontar la cuota sindical a petición del sindicato. En este supuesto será necesario el consentimiento expreso y por escrito porque se trata de un dato sensible |

| | |
|---|---|
| **Posibilidad de obviar el consentimiento en el Convenio Colectivo o Acuerdo de Condiciones laborales** | • *El **art. 37.1 CE** establece que la ley garantizará el derecho a la negociación colectiva laboral entre los representantes de los trabajadores y empresarios, y determina la fuerza vinculante de los convenios y **el ET, entre los arts. 82 a 92,** concreta que aquella es la expresión del acuerdo libremente adoptado entre el empresario y los representantes de los trabajadores*<br>• *Los Convenio y Acuerdos obligan a todos los empresarios y trabajadores dentro de su ámbito de aplicación y de su periodo de vigencia*<br>• *Según **STC 28/1992,** el hecho de que el convenio se incardine en el sistema de fuentes no le impide someterse a las normas de mayor rango jerárquico, entre ellas la ley y ha de someterse a los derechos fundamentales reconocidos en nuestra constitución, también al derecho a la protección de datos personales.*<br>• *Según **STC 58/1995** el convenio es un tipo de norma que rige las relaciones individuales de trabajo "sin necesitar el complemento de voluntades individuales"*<br>• *El Convenio Colectivo **no puede tener como contenido materias que no le son propias***<br>• *Las partes que lo negocian no tienen libertad absoluta para delimitar su contenido*<br>• *Está orientado a mejorar los derechos de los trabajadores, no a empeorarlo*<br>• *Por tanto **no existe la posibilidad de que en convenio se recoja una autorización al responsable del fichero para comunicar a los representantes de los trabajadores y organizaciones sindicales datos personales de los trabajadores sin su consentimiento** y sin que exista previsión legal al respecto*<br>• *Cuestión diferente es si por vía negocial se les puede hacer partícipes de grupos de trabajo o de gestión que tengan acceso a información de datos de carácter personal, y si en estos grupos ha de trabajarse con información de datos personales o disociada* |
| *Cómo se ceden los datos* | • Deben establecerse procedimientos para solicitarlos, justificando su necesidad para el cumplimento de algunas de sus atribuciones legales<br>• No deben realizarse transferencias de datos sin que se especifique la finalidad de su tratamiento |

| | |
|---|---|
| **Uso de los datos por los representantes de los trabajadores** | • *No podrán usarse para finalidad distinta que garantizar el cumplimiento de las obligaciones del empresario y de los derechos del trabajador.*<br>• *Los que los reciben deberán guardar el debido sigilo profesional (art. 10.3.1 LOLS, en relación con el art. 65.2 ET y art. 10, párrafo 2, de la Ley 9/1987, de 12 de junio, de órganos de representación, determinación de las condiciones de trabajo y participación del personal al servicio de las Administraciones públicas)*<br>• *Algunos consideran que cuando tengan los datos son responsables de ficheros según el **11.5 LOPD** y por tanto tienen que cumplir las obligaciones, medidas de seguridad, no comunicar datos a terceras personas sin consentimiento y deben facilitar a los trabajadores los derechos de acceso, rectificación y cancelación* |

## *VI.2. Datos relacionados con la salud laboral*

| | |
|---|---|
| ***En qué consiste la prevención de riesgos laborales*** | • Regulación en la **Ley 31/1995**, de 8 de noviembre, de Prevención de Riesgos Laborales. Existe un informe de la AEPD 434/2004 que aclara bastante la cuestión<br>• La prevención de riesgos trata de concretar el número de accidentes, su intensidad, los días de baja, los trabajadores sensibles a riesgos<br>• Sujetos: Servicios de prevención, delegados de prevención, empresario, los responsables de RRHH, los representantes de los trabajadores<br>• La Administración o el empresario tienen la obligación de constituir un servicio de prevención que se responsabilice de las actividades de prevención y de la protección de riesgos<br>• Como consecuencia de su actividad, el personal sanitario de los servicios de prevención o las mutuas a quienes se haya encargado el servicio deben acceder a datos especialmente protegidos |
| ***Posibilidad de recoger datos especialmente protegidos*** | • **Art. 7.3 LOPD** cuando por razones de interés general lo disponga una ley o lo consienta expresamente el afectado. Viene establecido en la LPRL.<br>• **Art. 7.6 LOPD** cuando resulte necesario para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamientos médicos o para la gestión de servicios sanitario<br>• En el supuesto de que las acciones de vigilancia de la salud sean voluntarias será necesaria la obtención del consentimiento del trabajador por parte del empresario para el tratamiento de sus datos de salud |
| *Sujetos que pueden acceder a los datos* | • Profesional sanitario sujeto a secreto profesional<br>• El propio trabajador **art. 22.3 LPRL**.<br>• A datos especialmente protegidos no tendrán acceso: el empresario, la dirección de RRHH (aunque tenga la competencia de vigilancia de la salud) ni el personal administrativo (si no es profesional sanitario)<br>• El **art. 39.2 c de LPRL** autoriza la cesión a los delegados de prevención del Comité de Seguridad e Higiene de un listado de nombres y accidentes |

| | |
|---|---|
| **Externalización de los servicios relacionados con la salud laboral** | • *Las Mutuas o empresas que tienen encomendado el servicio tienen la condición de encargados de tratamiento*<br>• *Es necesario firmar con ellas un contrato por escrito tal y como establece el artículo 12 LOPD*<br>• *Las Mutuas no pueden comunicar información médica a la empresa o administración (sí a su servicio médico) sino sólo el informe de aptitud psicofísica del trabajador. Los informes médicos han de ser comunicados únicamente al trabajador.*<br>• *Es responsabilidad de la mutua garantizar la confidencialidad y seguridad en las comunicaciones con los trabajadores* |
| ***Recomendación (89) 2 del Consejo de Europa*** | Recoge consideración sobre trato leal y legitimo de los datos de los trabajadores<br>• necesidad de consentimiento expreso para realizar pruebas análisis o procedimientos destinados a evaluar el carácter o la personalidad.<br>• derecho del afectado a conocer el resultado<br>• sólo podrá realizar exámenes o preguntar por salud a trabajadores o candidatos con el fin de determinar<br>o aptitud para el puesto<br>o cubrir necesidades de medicina preventiva<br>o conceder prestaciones sociales<br>• sólo puede recoger esos datos personal sujeto normas de secreto médico y se recomienda que se registren separados de los demás |
| ***Problema de incluir datos médicos en los ficheros de RRHH o de Nóminas*** | • Los datos que pueden tener los ficheros de RRHH relacionados con la baja: fechas de alta y baja médica, si se trata de enfermedad común, enfermedad profesional o accidente de trabajo.<br>• **Los datos relacionados con la baja pero relativos a la salud (diagnóstico médico, tratamientos, enfermedades, otros comentarios) no deben estar en el fichero** y sólo deben manejarse por el departamento que tenga la competencia en materia de personal.<br>• En las administraciones o empresas la responsabilidad de los reconocimientos médicos suele ser de los Responsables de RRHH y puede producirse la mala práctica de que la información clínica se archive junto a la laboral.<br>• **STC 202/1999**, de 8 de Noviembre un fichero relativo a control de absentismo laboral no puede mantener también información clínica de los trabajadores. |

## VI.3. Especial debilidad del trabajador en la cesión de datos durante la fase de colocación

| | |
|---|---|
| ***La fase de selección de trabajadores es especialmente relevante*** | • El empresario y la administración tienen derecho a contratar y/o seleccionar trabajadores aptos<br>• Existe un riesgo evidente para el trabajador, por su especial debilidad en esa fase de la relación, en la que puede existir un riesgo claro de que se hagan perfiles de personalidad del candidato |
| ***Existencia de prácticas inadecuadas*** | • Existen prácticas que violan la intimidad antes de la propia existencia de la relación laboral. En situaciones de elevado desempleo se acaban realizando preguntas impropias e incluso humillantes |
| ***Consentimiento previo*** | • Será necesario el consentimiento previo del candidato cuando se le soliciten datos.<br>• La aceptación de participación en el proceso supone un consentimiento inequívoco |
| ***Qué datos se han de solicitar*** | • Los necesarios para evaluar la aptitud de los candidatos<br>• Han de solicitarse al propio candidato<br>• Sólo podrán consultarse fuentes ajenas con el consentimiento del interesado<br>• Sólo se podrán realizar exámenes o preguntar por salud a los candidatos con el fin de determinar la aptitud para el puesto |
| ***Conservación de los datos*** | • Deben cancelarse los datos de los candidatos.<br>• Si se conservan, deben suprimirse a petición del interesado<br>• Sólo deberán conservarse para atender posibles recursos |
| ***Cesión de datos*** | • Sólo se podrán ceder si existe el consentimiento expreso del candidato<br>• Cesión de datos de bolsas entre diferentes administraciones. Debe haberse dado el consentimiento.<br>• Conveniencia de establecer sistemas y procedimientos regulados para el traslado de “referencias”. En este momento se hace de manera absolutamente informal. |
| ***Intervención de empresas ajenas que realizan el proceso*** | • Son encargados del tratamiento<br>• Es necesario firmar con ellas un contrato por escrito tal y como establece el artículo 12 LOPD |

| | |
|---|---|
| ***Intervención de empresas de colocación*** | • El RD 735/1995 regula la comunicación de datos a Agencias de colocación e INEM |
| *A considerar* | • OIT/96/29 7 octubre 1996 Repertorio de recomendaciones prácticas sobre la protección de datos personales de los trabajadores<br>• Recomendación (89) 2 del Consejo de Europa |

## *VI.4. Control de la utilización del correo electrónico*

| | |
|---|---|
| ***Uso del correo electrónico*** | • El correo electrónico es una herramienta de trabajo eficaz que simplifica el trabajo, ahorra tiempo, papel, permite una comunicación inmediata,…<br>• Está generalizándose en el funcionamiento de las comunicaciones entre las diferentes administraciones y empresas y entre estas y sus clientes<br>• Puede utilizarse adecuadamente o deslealmente: introducción de virus, robo de información de la empresa y-con matices- uso particular |
| ***Protección jurídica*** | • El **art. 18.3 CE** garantiza el secreto de comunicaciones, en especial, las postales, telegráficas y telefónicas. Entre ellas se encuentra el correo electrónico<br>• La **LO 10/1995, de 23 de Noviembre, del Código Penal** tipifica como delito su vulneración (art. 197.1)<br>• La AEPD lo considera dato de carácter personal y entiende necesario que el mismo esté amparado por el régimen establecido en la LOPD para proteger el derecho a la privacidad consagrado en el artículo 18.4 |
| ***Control*** | • Existen técnicas para controlar y acceder a todo el correo electrónico, tanto a datos de envío y recepción como a su propio contenido.<br>• No se puede usar indiscriminadamente esta herramienta por el empresario o la Administración |
| ***Consideraciones respecto del control por el empresario del uso del correo electrónico por sus trabajadores*** | • Necesidad de control. Sólo si no hay otros métodos que se entrometan menos en la vida privada<br>• Finalidad. Los datos se recogerán con fines determinados, explícitos y legítimos<br>• Transparencia. El control secreto del uso del ce por el empresario está prohibido (excepto en algunos estados miembros)<br>• Legitimidad<br>• Proporcionalidad. Los datos recogidos deben ser adecuados pertinentes y no excesivos<br>• Exactitud y conservación. Los datos deben ser precisos, actualizarse y no conservarse más allá de lo necesario<br>• Seguridad. Deberán aplicarse medidas técnicas y organizativas adecuadas para proteger los datos, protección contra los virus, análisis del tráfico, etc. |

| | |
|---|---|
| ***Soluciones posibles*** | • Acuerdos donde se establezcan protocolos de actuación para el uso de ce<br>• Para ello, parece necesario que el trabajador manifieste la renuncia exclusiva a la titularidad de la cuenta o el consentimiento expreso, para convertir la intromisión del empresario en legítima |
| ***Otra cuestión: uso del correo electrónico con fines sindicales*** | • La LO 11/1985 de Libertad Sindical y el art. 81 del ET establece el derecho de información sindical, que se traduce en que la empresa debe poner a disposición de los trabajadores un TABLÓN DE ANUNCIOS<br>• Ahora existe una nueva realidad: correo electrónico, intranet o listas de distribución que facilitan la comunicación entre los representantes sindicales y los trabajadores afiliados<br>• **La STC de 7 de noviembre 2005** "*sobre el empresario pesa el deber de mantener al sindicato en el goce pacífico de los instrumentos aptos para su acción sindical siempre que tales medios existan, su utilización no perjudique a la finalidad para la que fueron creados por la empresa y se respeten sus límites y reglas de uso que a continuación enunciaremos:*<br>➢ *no perturbar la actividad normal de la empresa.*<br>➢ *no perjudicar el uso específico del correo electrónico como herramienta de trabajo ni pretenderse que prevalezca el interés del uso sindical, conciliar ambos intereses, pero si conflicto prevalece su uso como herramienta de trabajo*<br>➢ *no podrá ocasionar gravámenes adicionales para el empleador, significativamente, la asunción de mayores costes.*<br>• Por tanto, las empresas no están obligadas a dotarse de esa infraestructura informática para uso sindical. |
| *Implicación de la ley que se dicte en cumplimiento de la Directiva 2006/24 de Comunicaciones electrónicas* | • Los operadores de comunicaciones están obligados a conservar durante un periodo de tiempo datos relativos al origen y destino de la comunicación (direcciones IP).<br>• Problema que se puede suscitar en administraciones y empresas donde para envío al exterior o la entrada se utilizan proxys si no se conservan los logs de conexión. ¿Tendrán que conservar los datos relativos a los envíos y recepciones realizados por sus trabajadores? |

## *VI.5. Control de la utilización de Internet*

| | |
|---|---|
| ***Uso de Internet*** | • Internet es una herramienta de trabajo eficaz que simplifica el trabajo, ahorra tiempo, papel y permite búsquedas de información y documentación inmediatas<br>• Está generalizándose como herramienta de trabajo entre las diferentes administraciones y empresas<br>• Puede utilizarse adecuadamente o deslealmente: para uso particular, accediendo a páginas de contenidos lúdicos, relacionados con el ocio, páginas de contenido sexual o realizarse descargas inadecuadas o, incluso, contrarias a la ley |
| ***Principio*** | • Es el empresario quién autoriza el acceso y, en su caso, ejerce el control sobre el acceso a Internet de sus trabajadores |
| ***Criterios*** | • Jurisprudencia contradictoria<br>• Grupo del art. 29 realizó las siguientes consideraciones sobre la cuestión:<br>➢ La prevención debería primar sobre la detección<br>➢ Toda medida de control debe ser proporcionada con relación al riesgo que corre el empresario<br>➢ En el análisis de la utilización de Internet por los trabajadores, los empleadores deberían evitar sacar conclusiones precipitadas por problemas de motores de búsqueda, vínculos hipertextuales engañosos, pancartas publicitarias ambiguas, etc. |
| ***Consideraciones respecto del control por el empresario del acceso a Internet de sus trabajadores*** | • Necesidad de control. Sólo si no hay otros métodos que se entrometan menos en la vida privada<br>• Finalidad. Los datos se recogerán con fines determinados, explícitos y legítimos<br>• Transparencia. El control secreto del acceso a internet por el empresario está prohibido (excepto en algunos estados miembros)<br>• Legitimidad<br>• Proporcionalidad. Los datos recogidos deben ser adecuados pertinentes y no excesivos<br>• Exactitud y conservación. Los datos deben ser precisos, actualiz*arse* y no conservarse más allá de lo necesario<br>• Seguridad. Deberán aplicarse medidas técnicas y organizativas adecuadas para proteger los datos, protección contra los virus, análisis del tráfico |

| | |
|---|---|
| ***Soluciones posibles*** | • el Grupo art. 29 considera que la prohibición absoluta de la utilización de Internet para fines privados, podría considerarse inaplicable y un tanto irrealista, ya que no se tendría en cuenta el apoyo que Internet puede brindar a los trabajadores en su vida diaria<br>• Necesidad de establecer equilibrio entre potestad el empresario para ejercer el control y el derecho a la intimidad por la vía de establecer políticas:<br>➢ sobre las condiciones en que se autoriza su utilización<br>➢ los sistemas instalados para impedir el acceso a algunos sitios o para detectar posibles utilizaciones abusivas<br>➢ el papel de los representantes de los trabajadores en ese control |
| *Implicación de la ley que se dicte en cumplimiento de la Directiva 2006/24 de Comunicaciones electrónicas* | • Los operadores de comunicaciones están obligados a conservar durante un periodo de tiempo datos relativos al origen y destino de la comunicación (direcciones IP).<br>• Problema que se puede suscitar en administraciones y empresas donde para envío al exterior o la entrada se utilizan proxys si no se conservan los logs de conexión. ¿Tendrán que conservar los datos relativos a los envíos y recepciones realizados por sus trabajadores? |

## *VI.6. Uso de videovigilancia en el trabajo*

| | |
|---|---|
| ***Marco legal*** | • Inexistencia de regulación específica para usos no policiales.<br>• **Instrucción 1/2006 de la Agencia Española de Protección de Datos**<br>• Quizás sea necesaria una regulación mediante ley de los usos no policiales como desarrollo específico de los derechos al honor y al intimidad y a la protección de datos personales<br>• Inexistencia de regulación específica en el ámbito laboral<br>• El **art. 20.3 ET** determina que "*el empresario podrá adoptar las medidas que estime oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso*"<br>• **LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen** considera intromisiones ilegítimas *"el emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas" así como la " utilización de aparatos para escucha…para el conocimiento de la vida intima de las personas o de manifestaciones o cartas privadas …"*<br>• El art. **197.1 del Código Pena**l penaliza al que, sin consentimiento, utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen para descubrir los secretos o vulnerar la intimidad del otro. |
| ***Realidad*** | • Generalización de la videovigilancia en el trabajo a través de<br>➢ Circuitos cerrados de televisión<br>➢ Cámaras de videovigilancia sin grabación<br>➢ Cámaras de videovigilancia con grabación bien en formato de cintas de vídeo o en discos duros<br>• Finalidades diversas: seguridad, información al exterior, control del proceso productivo y del trabajador, etc. |

| | |
|---|---|
| *Diferente jurisprudencia* | • La **STC186/2000 de 10 de julio** establece la posible legitimidad de la aplicación de medios audiovisuales como control de la actividad laboral, pero para determinarla estudia los siguientes parámetros:<br>➢ El lugar del centro donde se colocan,<br>➢ La utilización de forma indiscriminada y masiva<br>➢ Si son sistemas visibles<br>➢ La finalidad real perseguida<br>➢ La existencia de razones de seguridad<br>• Reiterada jurisprudencia, para determinar que los controles que puedan establecer los empleadores en uso de su derecho a controlar la actividad de los trabajadores serán lícitos mientras no produzcan resultados inconstitucionales, es necesario analizar en cada caso la medida adoptada para ver si cumple:<br>➢ Juicio de idoneidad<br>➢ Juicio de necesidad<br>➢ Juicio de proporcionalidad en sentido estricto<br>• Algunas sentencias han establecido que :<br>➢ el control aleatorio de llamadas de operadores en empresas de tele marketing no viola la intimidad (los trabajadores disponen de teléfonos no controlados en salas de descanso)<br>➢ el control mediante cámaras de cajas registradoras en un economato no viola la intimidad<br>➢ si viola el derecho poner en un casino además de cámaras micrófonos que graban todas las conversaciones |

## *VI.7. Utilización de datos biométricos*

| | |
|---|---|
| ***Qué son datos biométricos*** | • Rasgos fisiológicos o del comportamiento de una persona<br>➢ fisiológicos: parte de las anatomía, huella dactilar, rostro, retina, etc.<br>➢ del comportamiento: acciones como voz o firma<br>• Son por tanto datos personales |
| ***Nueva realidad*** | • Implantación progresiva de sistemas de control de acceso y presencia de los empleados basados en datos biométricos: huella digital, iris, contorno de manos, etc. |
| *Desde la óptica de protección de datos personales* | • NO se requiere consentimiento cuando forma parte de una relación laboral y sea necesaria para su mantenimiento<br>• Para algunos, el problema estaría en su consideración como datos de salud que exigiría el consentimiento expreso, pero en general se interpreta que no son datos de salud<br>• Debería aplicarse el juicio de idoneidad y necesidad y establecer que respetan el principio de calidad si son racionales (adecuación de medios al fin) y razonables (su uso se corresponde con un bien constitucionalmente garantizado) y proporcionados<br>• Varias sentencias del **T Superior de Cantabria (a modo de ejemplo las de 23 de Enero de 2003 y la de 21 febrero 2003)**, establecen la legitimidad del control horario de funcionarios a través del control de contorno de manos. Mucho más recientemente el **Auto del TC 57/07** inadmite el recurso de amparo frente a esa sentencia |

### *VI.8. Enunciando otras cuestiones especialmente relevantes*

- **Control de listados de llamadas telefónicas**
- **Uso de directorios de correo electrónico y telefónicos**
- **Necesaria coexistencia del derecho a la protección de datos y del derecho del ciudadano a que el funcionario, al que se dirige o con el que realiza una gestión, se identifique**
- **Problemas diferenciados que se suscitan en colectivos específicos de funcionarios en áreas de actividad basadas en la actividad personal: sanidad, educación, policía y bienestar social**
- **Localización de trabajadores mediante geolocalización y técnica RFID**
- **Establecimiento de canales de denuncia de irregularidades en el seno de las empresas. Implicaciones ley Sarbanes Oxley.**

# VII. PROPUESTAS REALIZADAS POR ALGUNAS INSTITUCIONES O COLECTIVOS

| | |
|---|---|
| ***Comisión europea***<br>***Agenda Social para 2005*** | • *Contemplaba una iniciativa para la protección de datos personales de los trabajadores.*<br>• *No se ha traducido en ninguna propuesta firme* |
| ***Comisión de Libertades e Informática (CLI)***<br>***Propuestas a grupos parlamentarios*** | • Introducir la figura del delegado de protección de Datos en empresas y administraciones, con la función de velar por la aplicación de esta normativa en el entorno laboral. Apoyar al empleado en sus derechos y obligaciones<br>• Participación de los Sindicatos en el Consejo Consultivo de la AEPD (sustituyendo a representantes de CCAA)<br>• Modificar<br>➢ Art. 4 de ET sobre utilización de aparatos audiovisuales en locales no abiertos al público en centros de trabajo<br>➢ Art. 5 sobre utilización de instrumentos tecnológicos por los trabajadores, permitiendo un uso moderado y proporcionado de éstos para fines personales, siempre que no afecte a su rendimiento profesional o laboral. Preservación reservada de sus datos<br>➢ Art. 22 de la LPRL, referente a datos relativos a la vigilancia de la salud, que no podrán ser usados con fines discriminatorios ni en perjuicio del trabajador ni utilizados con fines distintos.<br>➢ Art. 3 de la LOLS, considerando que el delegado sindical podrá asistir a las reuniones de los comités de empresa o de los órganos que se establezcan en materia de vigilancia electrónica y de protección de datos de carácter personal en el sentido de equilibrar acuerdos de empleado-empresa |

## VIII. A MODO DE CONCLUSIÓN O MIS 10 DESEOS

| | |
|---|---|
| ***Siempre atentos*** | • *Las nuevas tecnologías son una gran oportunidad, pero también pueden constituir una amenaza*<br>• *No debemos ser paranoicos, pero si cuidadosos a la hora de incorporarlas* |
| ***En casa del herrero cuchara de palo*** | • En la protección de datos de carácter personal no debemos olvidarnos de nuestros propios empleados |
| ***En el medio está la virtud*** | • Cuando hay varios derechos objeto de protección tendremos que evaluar, valorar y ponderar su justa forma de aplicación<br>• Es necesaria una cuidada ponderación de los derechos y los bienes en juego. No se debe confundir la finalidad legítima de control del empleador con la licitud de los medios a emplear |
| ***¿Me siento seguro?*** | • Existe una necesidad de integración entre la normativa laboral y la normativa de protección de datos de carácter personal, que algunos entienden se debe solventar con regulaciones adicionales<br>• Mientras no se den esa regulaciones son las Agencias y los Tribunales los que establecerán las líneas a seguir<br>• Las nuevas regulaciones en otras materias relacionadas deberían tener en cuenta este nuevo derecho<br>• También cabe la posibilidad de que se produzcan autorregulaciones a través de la negociación colectiva, fundamentalmente en lo relativo a la utilización del correo electrónico e Internet y su control por el empresario y la participación en ese control de lo representantes de los trabajadores |

| | |
|---|---|
| ***¿Ojos que no ven, corazón que no siente?*** | • Debemos adaptar los procedimientos de gestión para que cuando en grupos de trabajo, comisiones y órganos se acceda a datos de carácter personal, sobre todo si son sensibles, la información se estudie, siempre que sea posible, de forma disociada.<br>• Cuando en vía negocial se acuerde la participación sindical habrá que contemplar procedimientos de este tipo |
| ***Marcando el campo de juego*** | • Hay que establecer procedimientos tanto para la petición de información como para la cesión de la misma, incluso en los supuestos de cesiones a sindicatos y otras amparadas en la ley (qué se pide, para qué se pide, se cumpliría el objetivo con información disociada, se informa que se ceden datos personales y se recuerda el deber de secreto,…) |
| ***El guerrero del antifaz*** | • Es interesante analizar la implantación del delegado de datos personales en las administraciones o empresas que superaran un determinado número de trabajadores<br>• Encarece el coste de la estructura y ¿puede mantener la independencia?<br>• Algunos países han estudiado soluciones de este tipo, frente a la formalista de la necesidad de declarar ficheros. En aquellos casos se ocupa no sólo de lo referente a los datos personales de los trabajadores de la empresa, sino de cualquier tipo de dato personal tratado por la empresa |
| ***¿El que más guarda, sabe más?*** | • No se justifican los hiper-registros que acumulan y duplican la información<br>• ¿Tienen sentido Registros Generales de personal con datos no disociados? Parece lógico que los datos personales reales sólo estén en poder de las administraciones responsables<br>• No es admisible duplicar o triplicar expedientes con originales o copias en papel en diferentes niveles administrativos. |

| | |
|---|---|
| ***Administración organizada, vale por dos*** | • En la medida en que documentemos adecuadamente los procesos de gestión en RRHH, nos adelantaremos a los problemas y a las situaciones conflictivas<br>• Es necesario asimismo que al estudiar estos procesos incorporemos criterios de gestión documental<br>• Qué datos pedimos, donde los guardamos, qué medidas de seguridad adoptamos, cuándo los actualizamos, cuándo los destruimos, de qué manera los destruimos |
| ***Enseñar al que no sabe*** | • Es necesario especializar a los que trabajan en RRHH para que conozcan y apliquen de manera adecuada la normativa<br>• También parece conveniente una cierta adecuación y especialización de los representantes de los trabajadores |

# IX. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y NUEVO ESTATUTO DEL EMPLEADO PÚBLICO

- *Se echan en falta referencias específicas, como las hay a otros temas, como si la ley se hubiera hecho "a espaldas" de este nuevo derecho*

| | |
|---|---|
| Art. 14<br>**Derechos individuales** | • No mención específica<br>• 14 h) "*Al respeto de su intimidad, orientación sexual, propia imagen y dignidad en el trabajo, especialmente frente al acoso sexual y por razón de sexo, moral y laboral.*<br>*i) A la no discriminación por razón de nacimiento, origen racial o étnico, género, sexo u orientación sexual, religión o convicciones, opinión, discapacidad, edad cualquier otra condición o circunstancia personal o social.*<br>*A los demás derechos reconocidos por el ordenamiento jurídico.* |
| Art. 37<br>**Exclusión de la obligación de negociación** | *La regulación del ejercicio de los derechos de los ciudadanos y de los usuarios de los servicios públicos, así como el procedimiento de formación de los actos y disposiciones administrativas, queda excluida del ámbito negocial* |
| Art. 37<br>**Sigilo profesional** | *Cada uno de los miembros de la Junta de Personal y ésta como órgano colegiado, así como los Delegados de Personal, en su caso, observarán sigilo profesional en todo lo referente a los asuntos en que la Administración señale expresamente el carácter reservado, aún después de expirar su mandato. En todo caso, ningún documento reservado entregado por la Administración podrá ser utilizado fuera del estricto ámbito de la Administración para fines distintos de los que motivaron su entrega.* |
| Art. 53-4<br>**Principios éticos** | *4. Su conducta se basará en el respeto de los derechos fundamentales y libertades públicas, evitando toda actuación que pueda producir discriminación alguna por razón de nacimiento, origen racial o étnico, género, sexo, orientación sexual, religión o convicciones, opinión, discapacidad, edad o cualquier otra condición o circunstancia personal o social.* |
| Art. 82<br>**Movilidad por violencia de género** | **E***n las actuaciones y procedimientos relacionados con la violencia de género, se protegerá la intimidad de las víctimas, en especial, sus datos personales, los de sus descendientes y las de cualquier persona que esté bajo su guarda o custodia.* |
| **Art. 95-2**<br>**Faltas muy graves** | *e) La publicación o utilización indebida de la documentación o información a que tengan o hayan tenido acceso por razón de su cargo o función.* |

# ANEXOI. NORMATIVA DE REFERENCIA

## Anexo 3. 1. Marco normativo en materia de protección de datos

- **LEGISLACIÓN COMUNITARIA**
  - Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de Octubre de 1995, relativa a la protección de las personas físicas en que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
  - Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01)
    - Artículo 8
  - Proyecto de Constitución para Europa (DOUEC de 16 de Diciembre de 2004)
    - Artículo I-51
- **CONSTITUCIÓN**
  - Constitución Española de 27 de Diciembre de 1978.
    - Artículo 18
- **LEGISLACIÓN ESTATAL**
  - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
  - 4.2. Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
  - Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal

  En trámite nuevo Proyecto de Real Decreto 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

- **NORMATIVA AUTONÓMICA CAPV**

    - Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos (BOPV 4 de marzo de 2204)
    - Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos. (BOPV 16 de noviembre de 2005)
    - Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos. (BOPV 9 de noviembre de 2005)
    - Resolución de 21 de julio de 2005, del Director de la Agencia Vasca de Protección de Datos, por la que se establecen los modelos normalizados y los medios por los que debe procederse a la solicitud de las inscripciones de creación, modificación o supresión de ficheros en el Registro de Protección de Datos de la Agencia Vasca de Protección de Datos. (BOPV 31 de agosto de 2005)
    - Resolución de 28 de noviembre de 2005, del Director de la Agencia Vasca de Protección de Datos por la que se desarrolla la estructura orgánica de la Agencia Vasca de Protección de Datos. (BOPV 29 de diciembre de 2005)

## Anexo 3. 2. Marco normativo en materia laboral

- Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical
- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales
- Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
- Convenios colectivos

## Anexo 3. 3. Marco normativo en materia de función pública

- Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.
- Ley 6/1989, de 6 de Julio, de la Función Pública Vasca. y sus diversas modificaciones
- Decreto 190/2004, de 13 de octubre, por el que se aprueba el Reglamento de provisión de puestos de trabajo del personal funcionario de las Administraciones Públicas Vascas.

- Decreto 339/2001, de 11 de noviembre, por el que se aprueba el Reglamento de Situaciones Administrativas del personal funcionario de las Administraciones Públicas Vascas.
- Acuerdos de condiciones de trabajo

## ANEXOII. BIBLIOGRAFÍA


- Buenas Prácticas en Protección de Datos. Pedro Serrera Cobos. Fundación DINTEL. 2007.
- La protección de datos de carácter personal en los centros de trabajo. Antonio Farriols y Solá (Director y Coordinador). Comisión de Libertades e Informática y CINCA. 2006.
- Relaciones Laborales y Nuevas Tecnologías. Salvador Rey Guantes (Director) y Manuel Luque Parra (Coordinador). La Ley. 2005. En especial Capítulo VI El control empresarial del uso de las nuevas tecnologías en la empresa por Daniel Martínez Fons y Capítulo IX El derecho a la protección de datos en la relación laboral por Antonio José Valverde Asensio.
- El tratamiento por la empresa de Datos Personales de los Trabajadores. Análisis del estado de la cuestión. Rodrigo Tascón López. THOMSON-CIVITAS y Agencia de Protección de Datos de la Comunidad de Madrid. 2005
- Datos Personales y Administración Pública. Emilio Guichot. THOMSON-CIVITAS y Agencia de Protección de Datos de la Comunidad de Madrid. 2005
- Manual de Protección de Datos para las Administraciones Públicas THOMSON-CIVITAS y Agencia de Protección de Datos de la Comunidad de Madrid. 2003

# ANEXOIII. INFORMES Y RESOLUCIONES DE LA AGENCIA VASCA DE PROTECCIÓN DE DATOS RELACIONADOS

| ***Referencia*** | ***Contenido*** |
|---|---|
| CN 02/2005 | Cesión a sindicatos de datos personales para preparar recurso casación |
| CN 11/2005 | Cesión a un particular de datos retributivos de funcionarios |
| CN 12/2005 | Información de los derechos arco en fichero de asuntos sociales de un Ayuntamiento |
| CN 16/2005 | Cesión por HABE a un Departamento de relación de asistentes y aprovechamiento a cursos de euskera |
| CN 17/2005 | Cesión datos tributarios a tribunales y otros órganos de la Administración |
| CN 22/2006 | Implantación de sistemas de videovigilancia en zona de trabajo |
| CN 29/2006 | Inclusión de la fecha de nacimiento en el censo para elecciones sindicales |
| CN 30/2006 | Utilización de información de la Web del Ayuntamiento para noticia aparecida en el periódico |
| CN 31/2006 | Información representantes sindicales de un Departamento |
| CN 3/2007 | Información a representantes sindicales de un Ayuntamiento |
| PI 4/2005 | Falta leve a administración por no informar de la colocación de videocámaras en lugar de trabajo |
| **PI 3/2006** | Falta leve a administración por incumplir el deber de secreto al facilitar datos |