

RELACIONES LABORALES, TELETRABAJO Y PROTECCIÓN DE DATOS PERSONALES: una aproximación desde el derecho europeo

LABOR RELATIONS, TELEWORKING AND PROTECTION OF PERSONAL INFORMATION: an approximation since the european law

Álvaro A. Sánchez Bravo*

1 Introducción. Principios de la protección de datos en las relaciones laborales

Muchas actividades realizadas de manera habitual en las relaciones laborales suponen el tratamiento de datos personales de los trabajadores. Cualquier actividad de recogida, utilización o almacenamiento de información personal sobre los trabajadores, mediante procedimientos electrónicos, estará sometido a la normativa reguladora de la legislación sobre protección de datos¹, tanto interna como internacional.

La Unión Europea necesita normas más claras y sencillas para la protección de los datos personales de los trabajadores, que tengan mejor en cuenta la relación entre empresario y trabajador. La existencia de un marco claro y sencillo de principios y normas, aplicable en toda la UE, será positivo para los trabajadores y las empresas.

De esta manera se expresaba ya en 2001, Anna Diamantopoulou, Comisaria Europea responsable de Empleo y Asuntos Sociales, evidenciando la preocupación comunitaria por establecer un marco adecuado para la protección de los datos en el trabajo.

*Doctor en Derecho. Profesor de la Facultad de Derecho, del Instituto Andaluz Interuniversitario de Criminología y Miembro del Grupo de Investigación “Informática, Lógica y Derecho” de la Universidad de Sevilla. Presidente de la Asociación Andaluza de Derecho, Medio Ambiente y Desarrollo Sostenible. Coordinador de Relaciones Internacionales del Instituto Brasileiro de Direito Urbanístico (IBDU). Director del Seminario Hispano-Brasileño de Filosofía del Derecho y Derechos Humanos. Secretario de Universidades e Investigación. Comisión Ejecutiva FETE-UGT Sevilla (2009-2011).

¹En España, Ley Orgánica n. 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y Real Decreto n. 1.720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica n. 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD). En el ámbito de la Unión Europea, Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de los datos personales y a la libre circulación de estos datos.

El porqué de esa preocupación comunitaria parte de la constatación de que, pese al marco general de protección de datos establecido por las Directivas 95/46/CE y 2002/58/CE², se ha evidenciado en los últimos tiempos mutaciones de diversa etiología que es necesario considerar. Fenómenos como el progreso tecnológico (*e-mail* y teletrabajo), la globalización; e incluso, el 11-S³ (control de los trabajadores por motivos de seguridad) han propiciado la necesidad de una reflexión acerca de la protección adecuada de los datos personales de los trabajadores que, partiendo de las regulaciones generales, acoja sus especificidades.

Es por ello muy relevante el establecimiento de unos perfiles, de unos principios fundamentales⁴ que los empresarios deberán tener en cuenta al tratar de los datos personales de los trabajadores.

1. FINALIDAD. Los datos se recogerán con fines determinados, explícitos y legítimos. No podrán ser tratados de manera incompatible con los fines para los que fueron recogidos.

2. TRANSPARENCIA. Los trabajadores, como garantía imprescindible, deben conocer que datos recoge el empresario y cuales las finalidades de tratamiento previstas o ya realizadas.

Para ello debe garantizarse el más amplio ejercicio del derecho de acceso, rectificación y cancelación, en su caso.

3. LEGITIMIDAD. El tratamiento de los datos personales de los trabajadores deberá realizarse de manera legítima. El tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para: la ejecución de un contrato en el que el interesado sea parte; o el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento; o proteger el interés vital del interesado; o el cumplimiento de una misión de interés público, o la satisfacción del interés legítimo perseguido por el responsable del tratamiento.

4. PROPORCIONALIDAD. Los datos deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recogieron y para los que se traten posteriormente. Amén de informar a los trabajadores sobre el tratamiento de sus datos personales, este tratamiento deberá ser leal con los trabajadores.

²Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento automatizado de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), DOCE L 201, 31.7.2002.

³SÁNCHEZ BRAVO, Alvaro. El control de la Red. **Diario La Ley**, 30 de diciembre de 2002.

⁴Dictamen del grupo de Trabajo del artículo 29 sobre el tratamiento de datos personales en el contexto laboral.

5. EXACTITUD Y CONSERVACIÓN DE LOS DATOS. Los datos profesionales deben ser exactos, mostrando la realidad de las relaciones del trabajador. Cuando sea necesario, igualmente deberán ser actualizados. Corresponde a los empleadores a la asunción de las medidas necesarias y razonables para que los datos inexactos o incompletos sean suprimidos y rectificadas.

6. SEGURIDAD. El empleador deberá establecer medidas adecuadas, de carácter organizativo y técnico, en el lugar de trabajo, para garantizar la integridad y seguridad de los datos personales de sus trabajadores. Especial atención deberá prestarse para evitar los supuestos de acceso o difusión no autorizados.

7. FORMACION PROFESIONAL. El personal encargado del tratamiento de datos personales de otros trabajadores deberá tener unos conocimientos suficientes, y proporcionados a su nivel de responsabilidad.

8. CONSENTIMIENTO. Si un empleador debe utilizar datos personales como resultado inevitable y necesario de una relación laboral, sólo podrá verificarlo si cuenta con el consentimiento del trabajador. El consentimiento debe haber sido otorgado de forma totalmente libre y manteniendo integro su derecho de rectificación posterior, sin perjuicios como consecuencia de esta decisión.

9. DERECHO DE ACCESO. Todos los interesados deberán tener el derecho de obtener del responsable del tratamiento: la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos; la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones normativas, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.

10. VIGILANCIA Y CONTROL. Los principios de protección de los datos personales se aplican también a la vigilancia y control de los trabajadores, en lo relativo a uso de correo electrónico, acceso a Internet, cámaras de vigilancia o mecanismos de geolocalización. Estas medidas sólo serán pertinentes si constituyen una respuesta proporcionada del empresario ante riesgos reales, debiendo respetar escrupulosamente el derecho a la vida privada y otros intereses de los trabajadores. Cualquier dato del que se disponga o sea utilizado como instrumento de control deberá ser adecuado, pertinente y no excesivo con relación a los fines que determinan dicho control.

11. TRANSFERENCIA INTERNACIONAL DE DATOS. La transferencia de datos de los trabajadores sólo podrá verificarse si el país de destino garantiza un nivel de protección adecuado.

2 Propuesta para un marco regulatorio de los datos personales en las relaciones laborales

La ausencia de una legislación sectorial especial, contempladora de las especificidades del tratamiento de los datos personales en el ámbito de las relaciones laborales, no sólo crea una situación comprometedora para la seguridad jurídica de trabajadores y empresarios, sino que crea lagunas de interpretación contradictoria, en lo judicial y administrativo, que es preciso considerar. Las legislaciones internas, como la española, han elaborado Guías⁵ y resuelto, a través de la relevante labor de sus Agencias de Protección de Datos, temas concretos y puntuales, pero sin aportar aún una regulación unitaria y plenamente operativa.

Es por ello que, partiendo de la iniciativa desarrollada desde la Unión Europea⁶, pueden apuntarse algunas consideraciones respecto al contenido mínimo de una regulación adecuada en estos ámbitos⁷.

1 Ámbito de aplicación

Respetando el marco de protección general establecido en las normas generales, no puede establecer el principio de la libre circulación de datos laborales, sino precisar, y completar el marco jurídico existente, a fin de asegurar una protección suplementaria de los datos personales de los trabajadores (entendiendo por tal los trabajadores en activo, los ya jubilados y los candidatos a un empleo).

El campo de aplicación deberá cubrir todos los datos, incluidos el sonido y la imagen, independientemente del soporte utilizado para el tratamiento. A tal efecto, la protección incluiría la vigilancia de los trabajadores mediante dispositivos técnicos de cámaras, ordenadores, teléfonos y cualquier otro equipo de comunicación, identificación y localización.

Igualmente debe proteger no sólo los datos personales generados en el transcurso de una relación laboral existente, sino también los recopilados durante el proceso de selección o conservados después de la extinción de la relación laboral

⁵AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS . **Guía:** la protección de datos en las relaciones laborales. 2009. Disponible em: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales.pdf .>

⁶IP/02/1593, Bruselas, 31 de octubre de 2002.

⁷SANCHEZ BRAVO, Álvaro. A proteção dos dados pessoais dos trabalhadores: perspectiva comunitária europeia. **Revista do Tribunal Regional do Trabalho da 15ª Região**. Campinas, n. 30, p. 153-160, 2007.

Los destinatarios de estas medidas no sólo serían el sector público, sino también el sector privado, incluyéndose, si se estimase necesario las agencias de empleo, las ATT y las organizaciones que representan a los trabajadores.

2 Participación de los representantes de los trabajadores

Dada la dimensión colectiva de los derechos de los trabajadores, la participación de sus representantes se evidencia como imprescindible, tanto en la protección de sus intereses, como en la protección de los datos personales.

Es por ello que, como señalamos anteriormente, debe establecerse como principio general la obligación de informar y consultar a los representantes de los trabajadores, antes de y siempre que, se adopten medidas tendentes a la introducción y modificación de sistemas de tratamiento automatizado de datos, de dispositivos técnicos de control y vigilancia de los trabajadores, así como, de cuestionarios o tests de cualquier formato utilizados durante la selección o el periodo de empleo.

3 Principios generales para el tratamiento de datos en el sector de las relaciones laborales

Teniendo presente lo prescrito por la Directiva 95/46/CE en su art. 6, deben establecerse algunas precisiones en el ámbito de las relaciones laborales:

-Los datos personales de los trabajadores no serán objeto de tratamiento más que por motivos directamente relacionados y necesarios para el desarrollo de la prestación laboral.

-Los datos de los trabajadores no podrán ser utilizados más que para los fines previstos inicialmente; con interdicción de tratamientos posteriores incompatibles con dichos fines.

-Los datos personales serán objeto de un tratamiento leal. Ello supone que sean obtenidos directamente del trabajador afectado. Si proceden de terceros deberá informarse al trabajador y obtenerse su consentimiento previo al tratamiento.

- Los trabajadores tienen el derecho al libre acceso a sus datos. Se prohíbe que los empleadores y empresarios soliciten a los candidatos a un empleo o a los trabajadores en activo que ejerciten su derecho de acceso con el objeto de suministrárselos al empleador o empresario. Se intenta con ello que los trabajadores no se vean sometidos al "chantaje", y suministren datos que luego les puedan perjudicar.

-La relevancia que juega el consentimiento del trabajador en las relaciones laborales, en cuanto legitimador del tratamiento de sus datos personales debe matizarse. La relación de dependencia y subordinación, así como la precariedad laboral, hacen que el consentimiento se expanda, amparando situaciones intrusivas en los derechos de los trabajadores, pues se entiende por muchos empleadores que tal consentimiento ampara cualquier control o vigilancia sobre sus empleados.

Es por ello, con buen criterio, no debe estimarse como el único criterio relevante para el tratamiento, sino que lo vincula al cumplimiento de otros principios como los de pertinencia necesidad y proporcionalidad.

-Los datos personales deben ser tratados de manera lícita. En el ámbito laboral, el tratamiento de datos personales no debe tener como objetivo y/o efecto perjudicar ilícitamente al trabajador.

4 Categorías especiales de datos: los datos sensibles

El art. 8.1 de la Directiva 95/46/CE prohíbe el tratamiento de los datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Su apartado 5 prohíbe el tratamiento de datos relativos a las condenas penales.

El tratamiento de los datos sensibles, en su imbricación con los datos laborales, es susceptible de provocar situaciones de discriminación para los trabajadores por referencia a alguna de las categorías de datos mencionadas.

Es por ello, que deben plantearse algunas medidas específicas en este campo. El tratamiento de los datos sensibles de los trabajadores deberá estar prohibido, salvo que, a título excepcional y previa habilitación legal, se establezcan garantías y salvaguardas adecuadas. En este caso, y teniendo en cuenta los principios de determinación y limitación de la finalidad, legitimidad y proporcionalidad, podrá autorizarse un tratamiento de tales datos, sí bien de acuerdo a las siguientes particularidades:

-Los datos relativos a la vida sexual sólo podrán ser objeto de tratamiento cuando sea necesario para la determinación de la responsabilidad de los empleadores en el supuesto de una acusación de acoso sexual.

-Los datos relativos a los antecedentes penales sólo podrán tratarse si fuere necesario respecto a las funciones particulares del empleo en cuestión. En estos casos se prevé el necesario control previo por parte de la autoridad nacional de control, para evitar abusos y extralimitaciones, así como verificar la pertinencia de tal tratamiento.

Por otra parte, se prohíbe la solicitud de un empleador a un trabajador de la relación completa de sus antecedentes penales, sin

precisar previamente los que sean relevantes a efectos de la prestación laboral. El consentimiento del trabajador deviene irrelevante en este supuesto, no amparando estos tratamientos.

-Los datos relativos al origen racial o étnico y las convicciones religiosas y filosóficas sólo serán objeto de tratamiento cuando, previa habilitación legal, tenga por motivo una determinada exigencia profesional, o en caso de medidas de discriminación inversa positiva para favorecer a determinados colectivos, precisamente en atención a su origen racial, étnico o cultural.

5 Datos relativos a la salud

Aunque considerados igualmente como datos sensibles, a tenor de lo preceptuado por el art. 8.1 de la Directiva 95/46, debe dedicarse un apartado específico y concreto a la problemática de los datos relativos a la salud. Igualmente es necesario detenernos en la consideración de los cada vez más generalizados tests de consumo de drogas y alcohol, así como tests genéticos, en el ámbito de las relaciones laborales.

Partiendo del principio general de prohibición del tratamiento de datos relativos a la salud, se prevén, sin embargo, determinadas excepciones justificadas por la protección de los intereses de empleadores y trabajadores en la relación laboral que los une.

Ahora bien, el tratamiento **excepcional** de estos datos sólo podrá verificarse si fuera necesario, bien para comprobar si el trabajador es apto para el desarrollo de las funciones inherentes al puesto de trabajo, bien para adaptar su labor a las normas de seguridad e higiene en su lugar de trabajo; o bien, para comprobar si el trabajador tiene derecho a percibir determinadas prestaciones sociales (jubilaciones, incapacidades, subsidios...).

Respecto a las personas legitimadas para efectuar dicho tratamiento, se restringe a los profesionales de la sanidad o personas sometidas al secreto médico equivalente al de los profesionales sanitarios, siguiendo lo señalado por el punto 3 del art. 8 de la Directiva 95/46/CE.

Los datos relativos a la salud deben ser conservados independientes de cualesquiera otros datos personales. La causa no es sólo la especial incidencia de estos sobre los derechos de los ciudadanos, sino también el acceso indeseado de terceros, ajenos a las laborales sanitarias dentro o fuera de la empresa.

Por último, se restringe taxativamente el acceso del empleador al resultado de las pruebas médicas, limitándose su conocimiento a aquellos datos relevantes a efectos de la adecuación del trabajador al puesto concreto de trabajo.

En lo tocante a los datos relativos a los tests de consumo de drogas y/o alcohol, es evidente la potencialidad lesiva de dichos tests, sobre todo cuando son sistemáticos, generalizados o impuestos sistemáticamente sin motivos concretos.

Ahora bien, debe establecerse una nítida diferenciación entre test de consumo de drogas y de alcohol. Un resultado positivo en este último revela una deficiencia actual en el trabajo; mientras, que el relativo a drogas no evidencia una deficiencia anterior o actual o un riesgo de dependencia, sino únicamente que determinadas drogas han sido consumidas con anterioridad. No obstante, estas diferencias en cuanto a lo relevante de los tests en orden a la carga de la prueba de determinados consumos, desde el punto de vista técnico la iniciativa exige que los mismos sean fiables, precisos y sometidos a rigurosos proceso de control de calidad.

Al igual que en el supuesto de las condenas penales, se estima que el solo consentimiento del trabajador no puede servir como paraguas habilitador para realizar el tratamiento de datos relativos al consumo de drogas y/o alcohol.

Las propuestas en este campo pueden cifrarse en las siguientes propuestas:

-Los datos relativos al consumo de drogas y alcohol sólo podrán ser recogidos y tratados con objeto de determinar si un trabajador es apto para desarrollar su trabajo sin poner en peligro su seguridad o la de otras personas.

-Los tests sistemáticos y generalizados están prohibidos. Se exceptúan los casos en que un control de tal naturaleza está justificado por la naturaleza particular del empleo en que la seguridad es primordial.

-Los tests individuales se autorizan sólo si se puede determinar razonablemente que un trabajador consume drogas o alcohol poniendo en peligro gravemente la seguridad de sus compañeros o del público (sector de transportes, grúas, obras públicas...).

-Los datos derivados de los tests de consumo de drogas y/o alcohol podrán ser utilizados para los tratamientos de deshabituación de dichos consumos.

-Al igual que los datos relativos a la salud, éstos solo podrán ser recogidos y tratados por profesionales de la salud cualificados y sometidos al secreto profesional.

Por otra parte, la genética, y sus múltiples aplicaciones, constituyen hoy una de las manifestaciones más contundentes de la sociedad del Tercer Milenio. Ahora bien, frente a innegables logros, un uso torticero e inadecuado puede producir graves lesiones a los ciudadanos en sus derechos e intereses más íntimos.

Es por ello, que debemos partir de la premisa de que los datos genéticos que manifiesten el estado de salud de una persona deberían gozar de una protección reforzada respecto de los datos relativos a la salud⁸. Y ello es así porque estos datos afectan a temas importantes como el “derecho a no saber” y el “derecho a no dar a conocer” datos tan íntimos de la persona.

Nuevamente, el solo consentimiento del afectado no debe considerarse como elemento habilitador para el tratamiento de dichos datos. Es por ello que para el tratamiento excepcional de estos datos deben adoptarse las garantías adecuadas, y que pueden agruparse en las siguientes:

-El tratamiento de datos genéticos no debe autorizarse más que a título excepcional, con fines de protección de la salud y la seguridad de los trabajadores afectados o de terceros, y siempre en la medida en que esté autorizado por una norma legal nacional que establezca las necesarias garantías.

-Respeto estricto al principio de proporcionalidad. El resultado buscado no puede ser obtenido por otro medio menos intrusivo.

-Debería establecerse una asistencia genética previa (psicológica, médica...).

-Será necesaria una verificación previa por parte de la autoridad nacional de control. Esta verificación deberá tener en cuenta especialmente, como detalla el texto de la iniciativa, las particularidades de cada caso, la calidad de los tests, la pertinencia y fiabilidad de los resultados y la necesidad de buscar un equilibrio entre los siguientes elementos: los derechos de la persona afectada; los intereses manifiestamente predominantes de la sociedad; **y el derecho de no saber**, en caso de enfermedades graves incurables.

6 Actividades de vigilancia y control

La posibilidad de establecer una vigilancia y control sobre los trabajadores en el lugar de trabajo como una de las potestades del empleador, vinculada a cuestiones de eficiencia y productividad, constituye hoy objeto de una viva controversia.

Junto a la disparidad de las legislaciones nacionales (con ausencia de marco regulatorio alguno en muchos Estados⁹), la existencia de dispositivos técnicos avanzados (que incluso utilizan las herramientas tecnológicas de los propios trabajadores, tales como *e-mails*, *Internet*, registro automático de datos, *cookies*, etc.) dibuja un mapa de nebulosa indefinición, fuente de no pocos conflictos.

⁸SÁNCHEZ BRAVO, Álvaro. La protección de los datos genéticos, en derecho y conocimiento. **Anuario Jurídico Sobre la Sociedad de la Información**, v. 3, p. 1-23, 2006.

⁹AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía: Videovigilancia.. 2009. Disponible em: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf>.

Retomando lo señalado en el apartado 2 respecto a la participación de los interlocutores sociales en el diseño de estas políticas, deberán incluirse los siguientes principios:

-Verificación previa por parte de la autoridad nacional de control de toda actividad de control y vigilancia de los trabajadores.

-La vigilancia continua y permanente no debería autorizarse más que por motivos de salud, seguridad, o protección de bienes de la empresa.

-La vigilancia secreta no debe autorizarse salvo que se cumplan las garantías fijadas por las legislaciones protectoras (¿y los países que no tienen legislación interna?), o si puede suponerse razonablemente que se está desarrollando una actividad criminal o cualquier otro acto digno de sanción (¿nos sería más correcta la supervisión judicial, como sucede en otros ámbitos?).

-Los datos personales recogidos con el fin de garantizar la seguridad, el control o el buen funcionamiento de los sistemas de tratamiento no deben utilizarse para controlar de cada trabajador, salvo el de aquéllos de los que depende concretamente el funcionamiento del sistema.

-La evaluación de los rendimientos de los trabajadores y la toma de decisiones basadas en los mismos no deben estar justificadas exclusivamente en los datos recabados en el curso de la vigilancia electrónica.

-Salvo casos excepcionales, se prohíbe la vigilancia sistemática de la utilización del correo electrónico o de *Internet* por parte de los trabajadores. Se podrá efectuar una vigilancia individualizada cuando existan motivos suficientes para suponer que se está cometiendo un delito, cualquier otro acto reprobable o una infracción grave, siempre que no exista otro medio menos lesivo para conseguir el resultado buscado.

-Independientemente que se autorice o no la utilización de herramientas tecnológicas del trabajo con fines privados, el empleador no puede, como principio, acceder al correo electrónico de carácter privado y/o otros ficheros privados, especialmente a aquellos identificados como tales.

-El consentimiento del trabajador no habilita al empleador para derogar el secreto del correo electrónico y ficheros privados, especialmente durante la conclusión del contrato.

7 Teletrabajo y protección de datos

El teletrabajo hace referencia a un variado conjunto de situaciones y de prácticas laborales sometidas a una rápida y constante evolución. Los agentes sociales y laborales envueltos en su aplicación lo consideran como un medio para modernizar la organización laboral en la empresa y organizaciones del sector público, y al mismo tiempo una forma

de cumplir la prestación laboral que permite a los trabajadores conciliar su vida laboral y familiar, atribuyéndoles una mayor autonomía organizativa.

Ahora bien, ello no debe suponer que la flexibilidad y la seguridad se disocien, sino que permita una mejor calidad del empleo, así como el acceso al mercado laboral de personas con discapacidad o con situaciones personales y/o familiares especiales.

Como señala González:

[...] globalmente los autónomos con oficinas en su propia casa, los trabajadores móviles y los trabajadores a distancia ocasionales representan ahora mismo en la Unión Europea un volumen de 10 millones de personas y algunos vaticinan que este número alcanzará los 17 millones en el año 2011. Por otro lado Holanda incentiva fiscalmente el teletrabajo, Alemania ha creado un servicio de asesoramiento y contratación online para teletrabajadores, y Portugal fomenta el uso del teletrabajo para la reinserción social de discapacitados. Sin embargo, a pesar de la rápida expansión del teletrabajo, su regulación a nivel nacional es irregular hasta la fecha. Italia es el único estado miembro con una legislación que abarca los servicios públicos. Irlanda presentó un código de conducta en 1998 y existen convenios colectivos para algunos sectores en determinados países.¹⁰

Para hablar de teletrabajo deben cumplirse dos premisas básicas, en primer lugar, es necesaria el empleo significativo y predominante de equipos informáticos y telecomunicaciones,-esto hace que los puestos de trabajos susceptibles de ser desarrollados bajo este régimen esté relacionados con tareas relativas al tratamiento de la información-, y, en segundo lugar, que el porcentaje de la jornada laboral realizado fuera del centro de trabajo sea relevante. La doctrina lo estima en un tiempo superior o igual al 20%.

El ordenamiento jurídico español no cuenta con una legislación específica en materia de teletrabajo. La única alusión la tenemos en el artículo

¹⁰GONZALEZ, Agustín. **Un acuerdo europeo sobre las condiciones del teletrabajo.** Disponible em: <<http://www.istas.net/pe/articulo.asp?num=19&pag=19&titulo=Un-acuerdo-europeo-sobre-las-condiciones-del-teletrabajo.>>

13 del Estatuto de los Trabajadores¹¹ que regula el “trabajo a domicilio”. Los Convenios Colectivos a falta de una regulación específica deberán delimitar los aspectos más significativos de esta nueva forma de entender el trabajo¹².

La Organización Internacional del Trabajo lo define como “la forma de trabajo efectuada en un lugar alejado de la oficina central o del centro de producción y que implica una nueva tecnología que permite la separación y facilita la comunicación”.

Por su parte, el Acuerdo Marco Europeo sobre Teletrabajo¹³, lo conceptúa como

[...] una forma de organización y/o de realización del trabajo utilizando las tecnologías de la información, en el marco de un contrato o de una relación laboral, en la que un trabajo, que también habría podido realizarse en los locales del empresario, se ejecuta habitualmente fuera de esos locales.

El precitado Acuerdo establece regulaciones claves para garantizar la correcta aplicación de las normas laborales, dado el carácter específico del teletrabajo:

¹¹**Artículo 13.** Contrato de trabajo a domicilio. 1. Tendrá la consideración de contrato de trabajo a domicilio aquél en que la prestación de la actividad laboral se realice en el domicilio del trabajador o en el lugar libremente elegido por éste y sin vigilancia del empresario. 2. El contrato se formalizará por escrito con el visado de la Oficina de Empleo, donde quedará depositado un ejemplar, en el que conste el lugar en el que se realice la prestación laboral, a fin de que puedan exigirse las necesarias medidas de higiene y seguridad que se determinen. 3. El salario, cualquiera que sea la forma de su fijación, será, como mínimo, igual al de un trabajador de categoría profesional equivalente en el sector económico de que se trate. 4. Todo empresario que ocupe trabajadores a domicilio deberá poner a disposición de éstos un documento de control de la actividad laboral que realicen, en el que debe consignarse el nombre del trabajador, la clase y cantidad de trabajo, cantidad de materias primas entregadas, tarifas acordadas para la fijación del salario, entrega y recepción de objetos elaborados y cuantos otros aspectos de la relación laboral interesen a las partes. 5. Los trabajadores a domicilio podrán ejercer los derechos de representación colectiva conforme a lo previsto en la presente Ley, salvo que se trate de un grupo familiar.

¹²Disponível em: <<http://appcalia.com/ArchivosNoticias/Art%C3%ADculo%20Publicado%20en%20Capital%20Humano.pdf>>.

¹³La Confederación Europea de Sindicatos (CES), la Unión de Confederaciones de la Industria y de Empresarios de Europa (UNICE) / la Unión Europea del Artesanado y de la Pequeña y Mediana Empresa (UNICE/UEAPME) y el Centro Europeo de la Empresa Pública (CEEP) han firmado, el 14 de mayo de 2002, un acuerdo marco sobre el teletrabajo a fin de dar más seguridad a los teletrabajadores por cuenta ajena en la UE. Este acuerdo es especialmente importante, ya que se trata del primer acuerdo europeo establecido por los propios interlocutores sociales. El objeto del acuerdo es elaborar un marco general a escala europea para las condiciones laborales de los teletrabajadores y compaginar las necesidades de flexibilidad y seguridad comunes a los empresarios y los trabajadores. El acuerdo otorga a estos últimos la misma protección global que a los trabajadores que ejercen sus actividades en los locales de la empresa.. Disponível em: <http://europa.eu/legislation_summaries/employment_and_social_policy/employment_rights_and_work_organisation/c10131_es.htm>.

• **El carácter temporal del teletrabajo:** El teletrabajo es voluntario para el trabajador y el empresario de que se trate. El teletrabajo puede formar parte de la descripción inicial del trabajador o es posible aceptarlo voluntariamente después. En ambos casos, y con arreglo a la Directiva 91/533/CEE¹⁴, el empresario facilita al teletrabajador la información escrita pertinente.

• **Las condiciones de empleo:** los teletrabajadores tienen los mismos derechos que los trabajadores similares que realizan su tarea en los locales de la empresa. Esos derechos están garantizados por la legislación y los convenios colectivos aplicables. Podrían ser necesarios acuerdos específicos para tener en cuenta las peculiaridades del teletrabajo.

• **El ámbito de la vida privada:** el empresario debe respetar la vida privada del teletrabajador. Si existe un medio de vigilancia, deberá ser proporcionado al objetivo e introducirse con arreglo a la Directiva 90/270/CEE¹⁵ relativa a las pantallas de visualización.

• **Los equipos para la actividad:** por lo general, el empresario deberá facilitar, instalar y encargarse del mantenimiento de los equipos necesarios para el teletrabajo regular, salvo si el teletrabajador utiliza su propio equipo. El empresario ha de hacerse cargo, con arreglo a la legislación nacional y a los convenios colectivos, de los costes derivados de la pérdida o el deterioro de los equipos y de los datos utilizados por el teletrabajador.

• **La salud y la seguridad:** el empresario es responsable de la salud y la seguridad profesional del teletrabajador con arreglo a la Directiva 89/391/CEE¹⁶ y a las directivas específicas, las legislaciones nacionales y los convenios colectivos pertinentes. Para comprobar la correcta aplicación de las disposiciones aplicables en materia de salud y seguridad, el empresario, los representantes de los trabajadores y/o las autoridades competentes tendrán acceso al lugar del teletrabajo, dentro de los límites establecidos en las legislaciones y los convenios colectivos nacionales. Si el teletrabajador realiza su tarea en su domicilio, para poder acceder al mismo serán necesarias una notificación previa y el acuerdo del teletrabajador. El teletrabajador podrá solicitar una visita de inspección.

¹⁴Directiva 91/533/CEE del Consejo, de 14 de octubre de 1991, relativa a la obligación del empresario de informar al trabajador acerca de las condiciones aplicables al contrato de trabajo o a la relación laboral, DO L 288. 18.10.1991.

¹⁵Directiva 90/270/CEE, del Consejo, de 29 de mayo de 1990, referente a las disposiciones mínimas de seguridad y de salud relativas al trabajo con equipos que incluyen pantallas de visualización (quinta Directiva específica con arreglo al apartado 1 del artículo 16 de la Directiva 89/391/CEE) DO L 156. 21.6.1990.

¹⁶Directiva 89/391/CEE del Consejo, de 12 de junio de 1989, relativa a la aplicación de medidas para promover la mejora de la seguridad y de la salud de los trabajadores en el trabajo. DO L 183. 29.6.1989. Directiva 2007/30/CE del Parlamento Europeo y del Consejo, de 20 de junio de 2007, por la que se modifica la Directiva 89/391/CEE del Consejo, sus directivas específicas y las Directivas 83/477/CEE, 91/383/CEE, 92/29/CEE y 94/33/CE del Consejo, a fin de simplificar y racionalizar los informes sobre su aplicación práctica (Texto pertinente a efectos del EEE). DO L 165. 27.6.2007

• **La organización del trabajo:** en el marco de la legislación, de los convenios colectivos y de las normas laborales aplicables, corresponde al teletrabajador gestionar la organización de su tiempo de trabajo. La carga de trabajo y los criterios de resultados del teletrabajador son equivalentes a los de los trabajadores similares que realizan su tarea en los locales del empresario.

• **La formación de los teletrabajadores:** los teletrabajadores tienen el mismo acceso a la formación y a las posibilidades de carrera profesional que trabajadores similares que realizan su tarea en los locales del empresario, y están sujetos a las mismas políticas de evaluación que los demás trabajadores. Los teletrabajadores recibirán una formación apropiada, centrada en los equipos técnicos puestos a su disposición y en las características de esa forma de organización del trabajo.

• **Los derechos colectivos de los teletrabajadores:** los teletrabajadores tienen los mismos derechos colectivos que los trabajadores que realizan su tarea en los locales de la empresa. No deberá obstaculizarse la comunicación con los representantes de los trabajadores.

En lo relativo a **la protección de los datos personales**, corresponde al empresario adoptar las medidas necesarias para garantizar la protección de los datos utilizados y procesados por el teletrabajador para fines profesionales. El empresario informará al teletrabajador de toda restricción en lo que respecta a la utilización de los equipos y a las sanciones en caso de incumplimiento.

Lógicamente la normativa reguladora de la protección de datos personales es plenamente aplicable a los teletrabajadores. Si bien, y dada la ausencia física del trabajador del local de trabajo, cobrarán especial importancia las relativas al control de su actividad y/o del tiempo de trabajo.

El artículo 20.3 del Estatuto de los Trabajadores establece que “el empresario podrá adoptar las medidas de vigilancia y control que estime más oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales...”.

Como ha señalado la Agencia Española de Protección de Datos:

[...] cuando para el desarrollo de la función empresarial se utilizan las tecnologías de la información, las posibilidades de repercusión en los derechos de los trabajadores se multiplican. 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 del uso de ordenadores-, o los controles sobre la ubicación física del trabajador mediante localización.¹⁷

En casi todos estos supuestos se tratan datos personales, por lo que es necesario cumplir los principios de protección de datos.

En España, la Sentencia del Tribunal Supremo de 26 de septiembre de 2007, dictada en un Recurso para la Unificación de Doctrina, viene a confirmar la obligación de informar al trabajador sobre las reglas de uso del ordenador y los controles que sobre los mismos efectuará el empresario, dentro del poder que le confiere el artículo 20.3 del Estatuto de los trabajadores, así el fundamento jurídico cuarto señala que:

CUARTO.- El control del uso del ordenador facilitado al trabajador por el empresario no se regula por el artículo 18 del Estatuto de los Trabajadores, sino por el artículo 20.3 del Estatuto de los Trabajadores y a este precepto hay que estar con las matizaciones que a continuación han de realizarse. La primera se refiere a los límites de ese control y en esta materia el propio precepto citado remite a un ejercicio de las facultades de vigilancia y control que guarde 'en su adopción y aplicación la consideración debida' a la dignidad del trabajador, lo que también remite al respeto a la intimidad en los términos a los que ya se ha hecho referencia al examinar las sentencias del Tribunal Constitucional 98 y 186/2000. En este punto es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos

¹⁷AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **Guía:** La protección de datos en las relaciones laborales. 2009. Disponible em: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales.pdf>

para esa utilización y para garantizar la permanencia del servicio. **Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.**¹⁸ De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado 'una expectativa razonable de intimidad' en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos. (Sentencia de la Sala de lo Social del Tribunal Supremo de 26 de septiembre de 2007).

Por su parte, el control de llamadas es lícito siempre y cuando se sea proporcionado y se controlen exclusivamente las llamadas de carácter profesional. En todo caso, el trabajador deberá siempre estar informado de la existencia de este control.

En cuanto a la instalación de videocámaras, solo sería lícito en los supuestos en que fuese necesario para asegurar los bienes de la empresa. En aquellos supuestos en los que el control pudiese ser ejercido por un medio menos invasivo, se optaría por esta opción. En caso contrario, las videocámaras deberían ser instaladas en lugares donde no se desarrolle vida familiar y la conexión debería ser realizada durante las horas en las que se está trabajando.

De otra parte, en el seno del Grupo de Berlín¹⁹, se ha abordado la problemática derivada del uso de las nuevas tecnologías de la información y las telecomunicaciones dentro del lugar de trabajo caracterizada, al menos potencialmente, por la indudable generación de información acerca de los trabajadores.

¹⁸El subrayado es nuestro.

¹⁹GRUPO DE TELECOMUNICACIONES DE BERLÍN. **International Working Group on Data Protection in Telecommunications: IWGDPT**. Este grupo se creó en 1983, a iniciativa de la autoridad de protección de datos del Länder de Berlín, donde tiene su sede, y lo novedoso, frente a otros grupos de trabajo es que agrupa junto a representantes de las

En su documento “Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales”, el Grupo analiza los riesgos inherentes al control y vigilancia de los empleados a través de las modernas Tecnologías de la Información y de las Comunicaciones, que suponen en muchas ocasiones una intrusión en su privacidad.

La protección de los datos personales de los trabajadores tanto “en el lugar de trabajo”, como en su propio domicilio, a consecuencia de la extensión del denominado “Teletrabajo”, justificaron que el Grupo se definiera mediante el dictado de una serie de Recomendaciones, dirigidas a establecer los requisitos y condiciones necesarios que deberían ser respetados en la recogida de datos a través de los dispositivos propios de las nuevas tecnologías.

En dicho documento se “informa” sobre los métodos de recogida de datos más comunes utilizados en el seno de las organizaciones empresariales, tales como los dispositivos magnetofónicos, audio-visuales, transmisores de infrarrojos, identificadores de datos biométricos, dispositivos de videovigilancia, y comunicaciones electrónicas, alertando sobre los riesgos y perjuicios que el uso desviado de dichos medios puede ocasionar al trabajador.

8 Referências

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **Guía:** La protección de datos en las relaciones laborales. 2009. Disponível em: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales.pdf>

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **Guía:** Videovigilancia. 2009. Disponível em: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf>

GONZALEZ, Agustín. **Un acuerdo europeo sobre las condiciones del teletrabajo.** Disponível em: <<http://www.istas.net/pe/articulo.asp?num=19&pag=19&titulo=Un-acuerdo-europeo-sobre-las-condiciones-del-teletrabajo.>>

GRUPO DE TELECOMUNICACIONES DE BERLÍN. **International Working Group on Data Protection in Telecommunications: IWGDPT**

autoridades de control de un gran número de Estados, a representantes de organizaciones internacionales públicas y privadas, y a representantes de los sectores industriales implicados. Es un foro de trabajo abierto que pretende debatir sobre las implicaciones del uso de las telecomunicaciones en la esfera privada de los individuos, anticipándose a los problemas que se plantean en la práctica. Disponível em: GRUPO DE TELECOMUNICACIONES DE BERLÍN. **International Working Group on Data Protection in Telecommunications: IWGDPT.** Disponível em: <https://www.agpd.es/portalwebAGPD/internacional/Europa/grupos_de_trabajo_y_cooperacion/index-ides-idphp.php>

Disponível em: <https://www.agpd.es/portalwebAGPD/internacional/Europa/grupos_de_trabajo_y_cooperacion/index-ides-idphp.php .>

SÁNCHEZ BRAVO, Álvaro. A proteção dos dados pessoais dos trabalhadores: perspectiva comunitária europeia. **Revista do Tribunal Regional do Trabalho da 15ª Região. Campinas**, n. 30, p. 153-160, 2007.

SÁNCHEZ BRAVO, Álvaro. La protección de los datos genéticos, en derecho y conocimiento. **Anuario Jurídico Sobre la Sociedad de la Información**, v. 3, p. 1-23, 2006.

SÁNCHEZ BRAVO, Álvaro. El control de la Red. **Diario La Ley**, 30 de diciembre de 2002.