GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS - ARTÍCULO 29

5401/01/ES/Final
WP 55

Documento de trabajo

relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo

Aprobado el 29 de mayo de 2002

Comentarios:

* los capítulos nacionales podrán modificarse posteriormente de acuerdo con las delegaciones nacionales

El Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

La secretaría encargada es la siguiente: Dirección A (Funcionamiento e Impacto del Mercado Interior. Coordinación. Protección de Datos) de la DG Mercado Interior de la Comisión Europea, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Bélgica - Despacho: C100-6/136.

Sitio Internet: www.europa.eu.int/comm/privacy

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[1],

Vistos el artículo 29 y los apartados 1, letra a), y 3 del artículo 30 de dicha Directiva,

Visto su Reglamento interno y, en particular, sus artículos 12 y 14,

Ha aprobado el siguiente documento de trabajo:

[1] Diario Oficial L 281 de 23.11.1995, p. 31, que puede consultarse en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm.

Documento de trabajo del Grupo de Trabajo «Artículo 29»[2] relativo a la vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo

Proyecto de resumen

El presente documento de trabajo completa el dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral[3] y contribuye a la aplicación uniforme de las medidas nacionales adoptadas en el marco de la Directiva 95/46/CE relativa a la protección de datos[4]. No afecta a la aplicación de la legislación nacional en ámbitos vinculados a la protección de los datos.

El Grupo de Trabajo «Artículo 29» ha creado un subgrupo para examinar esta cuestión[5] y ha aprobado un **extenso documento,** disponible en Internet en la siguiente dirección[6]:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

En el presente documento de trabajo, el Grupo de Trabajo «Artículo 29» examina la cuestión de la vigilancia y el control de las comunicaciones electrónicas en el lugar de

---

[2] El Grupo de Trabajo «Artículo 29» es un grupo consultivo independiente compuesto por representantes de las autoridades de los Estados miembros encargadas de la protección de datos, cuya misión es, en particular, examinar todas las cuestiones relativas a la aplicación de las medidas nacionales adoptadas en virtud de la Directiva sobre protección de datos con el fin de contribuir a su aplicación uniforme.

[3] Dictamen adoptado el 13 de septiembre de 2001 y accesible en la siguiente dirección:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf .

Este dictamen incluye un análisis detallado de la aplicación de la Directiva relativa a la protección de datos (en particular, sus artículos 6, 7 y 8) al tratamiento de datos personales en el marco de las actividades profesionales.

[4] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DO L 281 de 23.11.95, p. 31.

[5] Al trabajo de este subgrupo han contribuido las siguientes autoridades de supervisión: AT, BE, DE, ES, FR, IR, IT, NL, UK.

[6] Este documento incluye un anexo en el que figura la legislación sobre protección de datos más pertinente de los Estados miembros con alguna repercusión en las actividades de vigilancia y control de las comunicaciones electrónicas en el lugar de trabajo.

trabajo, o, dicho de otro modo, la vigilancia por el empleador de la utilización del correo electrónico e Internet por los trabajadores.

A la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos sobre el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, otros textos internacionales pertinentes y la Directiva 95/46/CE, el presente documento de trabajo ofrece una orientación y ejemplos concretos sobre lo que constituyen actividades de control legítimas y límites aceptables de la vigilancia de los trabajadores por el empleador. Téngase en cuenta que en algunos Estados miembros la legislación puede prever un nivel de protección más elevado que el que contempla el presente documento de trabajo.

Los trabajadores no dejan su derecho a la vida privada y a la protección de datos cada mañana a la puerta de su lugar de trabajo. Esperan legítimamente encontrar allí un grado de privacidad, ya que en él desarrollan una parte importante de sus relaciones con los demás. Este derecho debe, no obstante, conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con cierta eficacia la empresa, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los trabajadores. Estos derechos e intereses constituyen motivos legítimos que pueden justificar la adopción de medidas adecuadas destinadas a limitar el derecho a la vida privada de los trabajadores. Los casos en que el empleador es víctima de un delito imputable a un trabajador constituyen el ejemplo más claro.

No obstante, para equilibrar los distintos derechos e intereses es preciso tener en cuenta varios principios, en particular, el principio de proporcionalidad. Debe quedar claro que el mero hecho de que una actividad de control o vigilancia se considere útil para proteger el interés del empleador no justifica la intromisión en la vida privada del trabajador. Antes de aplicar en el lugar de trabajo cualquier medida de vigilancia, deben sopesarse una serie de aspectos que se detallan en el presente documento.

En las siguientes preguntas puede resumirse la naturaleza de esta evaluación:

a) ¿Es la actividad de vigilancia transparente para los trabajadores?

b) ¿Es necesaria? ¿No podría el empleador obtener el mismo resultado con métodos tradicionales de supervisión?

c) ¿Garantiza el tratamiento leal de los datos personales de los trabajadores?

d) ¿Es proporcional respecto a las preocupaciones que intenta solventar?

Al centrarse en la aplicación práctica de estos principios, el documento de trabajo proporciona orientación sobre el contenido mínimo de las directrices de las empresas en relación con la utilización del correo electrónico e Internet, que los empleadores y trabajadores pueden tomar como base para una adaptación posterior (habida cuenta de las especificidades de cada empresa, su tamaño y la legislación nacional en ámbitos vinculados a la protección de datos).

Al plantearse la utilización de Internet con fines privados, el Grupo de Trabajo «Artículo 29» considera que la **prevención debería prevalecer sobre la detección;** es decir, que es mejor para el empleador prevenir la utilización abusiva de Internet

que detectarla. En este contexto las soluciones tecnológicas pueden resultar especialmente útiles. Prohibir terminantemente que los trabajadores utilicen Internet con fines privados no parece razonable y no tiene en cuenta la ayuda que Internet puede aportarles en su vida diaria.

El Grupo de Trabajo desearía destacar que es esencial que el empleador informe al trabajador (i) de la presencia, utilización y objetivo de todo equipo y/o aparato de detección activado en su puesto de trabajo, así como (ii) de cualquier abuso de las comunicaciones electrónicas detectado (correo electrónico o Internet), salvo si existen razones imperiosas que justifiquen la continuación de la vigilancia encubierta[7], lo que normalmente no sucede. Puede transmitirse información rápida fácilmente mediante un programa informático, por ej. ventanas de advertencia que avisen al trabajador de que el sistema ha detectado y/o tomado medidas para evitar una utilización ilícita de la red.

Como recomendación práctica, los empleadores pueden considerar la posibilidad de proporcionar a los trabajadores dos cuentas de correo electrónico:

a) una de uso profesional exclusivo, en la que se permitiría un control dentro de los límites del presente documento de trabajo,

b) otra de uso estrictamente privado (o con autorización de utilizar el correo web), que sólo sería objeto de medidas de seguridad y que se controlaría para prevenir abusos en casos excepcionales.

El Grupo de Trabajo «Artículo 29» ha observado divergencias entre las legislaciones nacionales en ámbitos vinculados a la protección de datos, que se refieren principalmente a las excepciones previstas al derecho fundamental al secreto de correspondencia y al alcance y repercusión de la representación y la codecisión colectivas de los trabajadores. No obstante, no ha detectado divergencias entre las legislaciones nacionales en el ámbito de la protección de datos que puedan constituir obstáculos importantes para un enfoque común, por lo que ha redactado el presente documento de trabajo, que se revisará en 2002-2003 a la luz de la experiencia y la evolución en este ámbito.

[7] Los casos de vigilancia encubierta justificada constituyen un buen ejemplo.

1. LA VIGILANCIA EN EL LUGAR DE TRABAJO. UN RETO PARA LA SOCIEDAD.

Últimamente, la cuestión de la vigilancia de los trabajadores ha sido abordada en numerosas ocasiones por los medios de comunicación y es en la actualidad objeto de un debate público en la Comunidad. En efecto, la introducción progresiva en toda la Comunidad del correo electrónico en el lugar de trabajo ha sensibilizado tanto a los empleadores como a sus trabajadores de los riesgos de intromisión en su vida privada en el lugar de trabajo.

Al examinar la cuestión de la vigilancia, conviene tener siempre presente que, si bien los trabajadores tienen derecho a un cierto grado de respeto de la vida privada en el trabajo, este derecho no debe lesionar el derecho del empleador de controlar el funcionamiento de su empresa y de protegerse contra una actuación de los trabajadores susceptible de perjudicar sus intereses legítimos, por ejemplo la responsabilidad del empleador por acciones de sus trabajadores.

Aunque las nuevas tecnologías constituyen un desarrollo positivo de los recursos a disposición de los empleadores, las herramientas de vigilancia electrónica pueden utilizarse para atentar contra los derechos y libertades fundamentales de los trabajadores. Conviene no olvidar que, con la llegada de las tecnologías de la información, es vital que éstos se beneficien de los mismos derechos, ya trabajen en línea o fuera de línea.

Es necesario destacar también que las condiciones laborales han evolucionado, en el sentido de que en la actualidad cada vez es más difícil separar claramente el trabajo de la vida privada. En particular, a medida que se desarrolla la «oficina a domicilio», numerosos trabajadores continúan su trabajo en casa, utilizando la infraestructura informática puesta a su disposición por el empleador para estos u otros fines.

La dignidad humana de un trabajador prima sobre cualquier otra consideración. Al examinar esta cuestión, es importante tenerlo en cuenta, al igual que las consecuencias negativas que este tipo de acciones puede tener en la calidad de la relación de un trabajador con su empleador y en el trabajo propiamente dicho.

Habida cuenta de todos estos factores, no es de extrañar que esta problemática sea objeto de un intenso debate público; por ello es urgente contribuir a una interpretación uniforme de las disposiciones de la Directiva 95/46/CE y de las legislaciones nacionales que la aplican, a la luz de la reciente jurisprudencia del Tribunal Europeo de Derechos Humanos.

El Grupo de Trabajo consideró por tanto que sería útil transmitir la información y las recomendaciones siguientes a los sectores público y privado. Es preciso señalar que el documento de trabajo cubre toda actividad vinculada a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, tanto la vigilancia en tiempo real como el acceso a datos almacenados.

2. INSTRUMENTOS JURÍDICOS INTERNACIONALES

2.1 ARTÍCULOS 8 Y 10 DEL CONVENIO EUROPEO PARA LA PROTECCIÓN DE LOS DERECHOS HUMANOS Y DE LAS LIBERTADES FUNDAMENTALES.

Artículo 8

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Artículo 10

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o e para garantizar la autoridad y la imparcialidad del poder judicial.

Todos los Estados miembros y la Unión Europea deben cumplir las disposiciones del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Estos derechos se han ejercido tradicionalmente de forma vertical (es decir, el individuo frente al Estado) y actualmente se discute hasta qué punto pueden ejercerse horizontalmente (es decir, entre los individuos). No obstante, queda claro que en general estos derechos están presentes.

El Grupo de Trabajo considera por lo tanto que, a la hora de examinar las disposiciones nacionales adoptadas de conformidad con la Directiva 95/46/CE con el fin de contribuir a su aplicación uniforme, es preciso recordar los grandes principios consagrados por la jurisprudencia del Tribunal Europeo de Derechos Humanos en relación con esta disposición y, en particular, en lo que respecta al secreto de correspondencia.

En las sentencias dictadas hasta ahora, el Tribunal ha precisado que la protección de la «vida privada» consagrada por el artículo 8 no se limita al hogar, sino que se aplica también al lugar de trabajo.

El asunto **Niemitz contra Alemania** se refería al registro, por una autoridad pública, de la oficina del demandante. El Gobierno alemán alegó que el artículo 8 no ofrecía protección alguna contra el registro de una oficina, ya que el Convenio establece una clara distinción entre vida privada y domicilio, por una parte, y vida profesional y lugar de trabajo, por otra.

El Tribunal desestimó esta alegación y resolvió del siguiente modo:

«El respeto de la vida privada debe también englobar, hasta cierto punto, el derecho a entablar y desarrollar relaciones con los semejantes. ***Además, ninguna razón de principio permite excluir las actividades profesionales o comerciales del concepto de }vida privada~,*** *puesto que es en el trabajo donde la mayoría de las personas disponen de muchas, o incluso las máximas, oportunidades de relacionarse con el mundo exterior. Un hecho, destacado por la Comisión, lo confirma: no siempre se puede distinguir con claridad entre las actividades que pertenecen al ámbito profesional o laboral de las personas y las que no*[8]*».*

Más concretamente, en el asunto **Halford contra el Reino Unido**, el Tribunal estableció que la interceptación de las llamadas telefónicas efectuadas por los trabajadores desde su puesto de trabajo constituye una violación del artículo 8 del Convenio. Curiosamente, la Sra. Halford tenía a su disposición dos aparatos telefónicos, uno de los cuales estaba reservado para sus comunicaciones privadas. La utilización de estos teléfonos no estaba sometida a restricción alguna ni se le transmitió ninguna orientación a este respecto.

Para la Sra. Halford, la interceptación de sus llamadas telefónicas constituyó una violación del artículo 8 del Convenio. Su empleador, una autoridad pública, consideró en cambio que las llamadas telefónicas realizadas por la Sra. Halford desde su puesto de trabajo no estaban sujetas a la protección del artículo 8, ya que la demandante no podía confiar razonablemente en que se les reconociera carácter privado. En la vista ante el Tribunal, la defensa de la Administración declaró que el empleador debe en principio poder supervisar, sin que los interesados lo sepan de antemano, las llamadas que éstos realizan desde los aparatos que pone a su disposición.

Para el Tribunal, sin embargo, «*se desprende claramente de su jurisprudencia que las llamadas telefónicas que proceden de locales profesionales, al igual que las procedentes del domicilio, pueden incluirse en los conceptos de 'vida privada' y de 'correspondencia' citados en el apartado 1 del artículo 8 [...]*.

No hay pruebas de que a la Sra. Halford se le hubiera avisado, en calidad de usuaria de la red interna de telecomunicaciones, de que las llamadas efectuadas mediante la misma podían ser interceptadas. El Tribunal considera que ella podía razonablemente esperar que se reconociera el carácter privado de este tipo de llamadas [...]»[9].

El concepto de «correspondencia» engloba no sólo las cartas redactadas en papel, sino también otras formas de comunicación electrónica recibidas o enviadas en el lugar de trabajo, como las llamadas telefónicas efectuadas o recibidas en locales profesionales o los

---

[8] 23 de noviembre de 1992, serie A n° 251/B, apartado 29; la negrita es añadida.

[9] 27 de mayo de 1997.

mensajes electrónicos recibidos o enviados en ordenadores puestos a disposición en el lugar de trabajo.

Algunos interpretan la sentencia en el sentido de que parece implicar (aunque no se declare explícitamente) que si el empleador informa previamente al trabajador de que sus comunicaciones pueden interceptarse, el trabajador ya no podrá esperar que se reconozca carácter privado a sus llamadas, con lo que la interceptación no constituirá una violación del artículo 8 del Convenio. El Grupo de Trabajo opina que una advertencia previa al trabajador no basta para justificar una violación de sus derechos en cuanto a protección de datos.

De manera más general, de la jurisprudencia relativa al artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales pueden deducirse los tres principios siguientes:

a) Los trabajadores tienen confianza legítima en que se respetará su vida privada en el lugar de trabajo, confianza que no queda anulada por el hecho de utilizar herramientas de comunicación u otros medios profesionales del empleador.

   Sin embargo, el suministro de información adecuada por el empleador al trabajador puede disminuir esta confianza legítima.

b) El principio general del secreto de correspondencia se aplica a las comunicaciones en el lugar de trabajo, lo que incluye muy probablemente el correo electrónico y los ficheros anexos.

c) El respeto de la vida privada cubre también, hasta cierto punto, el derecho del individuo a entablar y desarrollar relaciones con sus semejantes. El hecho de que estas relaciones se produzcan en gran parte en el lugar de trabajo limita la necesidad legítima del empleador de aplicar medidas de vigilancia.

El artículo 10 es también pertinente, aunque en menor medida, puesto que regula las libertades de expresión e información y destaca el derecho del individuo a recibir y comunicar información e ideas sin injerencia de una autoridad pública. La pertinencia del artículo 10 parece reflejarse en las consideraciones del Tribunal en el asunto Niemitz contra Alemania previamente mencionado. Como afirmó el Tribunal, en el lugar de trabajo las personas desarrollan una parte importante de su relación con el mundo exterior y su derecho a la libertad de expresión desempeña indudablemente un papel en este contexto.

2.2 CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL (STE N° 18)

Abierto a la firma el 28 de enero de 1981, el Convenio fue el primer instrumento internacional legalmente vinculante en el ámbito de la protección de datos. Este Convenio obliga a las partes a adoptar las medidas necesarias en su legislación nacional para aplicar los principios que enuncia con el fin de garantizar el respeto, en su territorio, de los derechos humanos fundamentales de todos los individuos con respecto al tratamiento de los datos de carácter personal[10].

[10] Véase también la Recomendación (89) 2 del Consejo de Europa sobre la protección de los datos de carácter personal utilizados con fines de empleo: http://cm.coe.int/ta/rec/1989/89r2.htm

Otros documentos importantes vinculados al Convenio 108, también pertinentes en este contexto, son los siguientes:

Recomendación (89) 2 del Consejo de Europa sobre la protección de los datos de carácter personal utilizados con fines de empleo[11].

Recomendación (97) 5 del Consejo de Europa sobre la protección de los datos médicos[12].

Recomendación (86) 1 del Consejo de Europa sobre la protección de los datos de carácter personal con fines de seguridad social[13].

Recomendación (95) 4 del Consejo de Europa sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, especialmente en lo que respecta a los servicios telefónicos.

2.3. LA CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

Artículo 7. ***Respeto de la vida privada y familiar***

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8. ***Protección de datos de carácter personal***

1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*

2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*

3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente.*

La Carta de los Derechos Fundamentales de la Unión Europea parece ir en el mismo sentido que el Tribunal Europeo de Derechos Humanos. El concepto de secreto de correspondencia se ha ampliado para convertirse en un concepto de nueva generación: el «secreto de las comunicaciones», con el fin de reconocer a las comunicaciones electrónicas el mismo nivel de protección del que se beneficia el correo tradicional.

---

11 http://cm.coe.int/ta/rec/198 9 /89r2.htm .

12 http://cm.coe.int/ta/rec/1997/97r5.html

13 http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(86)1E.htm

Además, al conferir a la protección de datos una naturaleza claramente diferenciada, el artículo 8 completa la protección prevista por el artículo 7. Ello reviste una importancia singular en el contexto de la vigilancia del correo electrónico.

2.4. OFICINA INTERNACIONAL DEL TRABAJO (OIT)

Repertorio de recomendaciones prácticas de la Oficina Internacional del Trabajo sobre la protección de los datos personales de los trabajadores (1997).

«5. Principios generales

5.1. El tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación de empleo del trabajador.

5.2. En principio, los datos personales deberían utilizarse únicamente con el fin para el cual hayan sido acopiados.

5.3. Cuando los datos personales se exploten con fines distintos de aquéllos para los que fueron recabados, el empleador debería cerciorarse de que no se utilizan de un modo que sea incompatible con esa finalidad inicial y adoptar las medidas necesarias para evitar toda interpretación errada por causa de su aplicación en otro contexto.

5.4. Los datos personales reunidos en función de disposiciones técnicas o de organización que tengan por objeto garantizar la seguridad y el buen funcionamiento de los sistemas automatizados de información no deberían servir para controlar el comportamiento de los trabajadores.

5.5. Las decisiones relativas a un trabajador no deberían basarse exclusivamente en un tratamiento informático de los datos personales que a él se refieran.

5.6. Los datos personales obtenidos por medios de vigilancia electrónica no deberían ser los únicos factores de evaluación profesional del trabajador. (...).

6.14. 1) Cuando los trabajadores sean objeto de medidas de vigilancia, éstos deberían ser informados de antemano de las razones que las motivan, de las horas en que se aplican, de los métodos y técnicas utilizados y de los datos que serán acopiados, y el empleador deberá reducir al mínimo su injerencia en la vida privada de aquéllos.

2) El secreto en materia de vigilancia sólo debería permitirse cuando

a) se realice de conformidad con la legislación nacional; o

b) existan sospechas suficientes de actividad delictiva u otras infracciones graves.

3) La vigilancia continua debería permitirse solamente si lo requieren la salud, la seguridad y la protección de los bienes. (...)

12.2. Los representantes de los trabajadores, cuando los haya, y de conformidad con la legislación y la práctica nacionales, deberían ser informados y consultados:

a) acerca de la instalación o modificación de sistemas automatizados de tratamiento de los datos personales de los trabajadores;

b) antes de la instalación de sistemas de vigilancia electrónica del comportamiento de los trabajadores en el lugar de trabajo; y

c) sobre la finalidad, el contenido, la aplicación y la interpretación de cuestionarios y pruebas relativos a los datos personales de los trabajadores.»

3. VIGILANCIA Y CONTROL DE LAS COMUNICACIONES ELECTRÓNICAS EN EL LUGAR DE TRABAJO EN EL MARCO DE LA DIRECTIVA 95/46/CE

El presente documento de trabajo se basa en una aplicación de los principios enunciados en la Directiva 95/46/CE a la cuestión que nos ocupa, teniendo en cuenta el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que exige el respeto de la correspondencia y de la vida privada.

El empleador dispone de múltiples formas de vigilancia en el lugar de trabajo, cada una de las cuales con su propia problemática. El presente documento examinará dos formas de vigilancia, a las cuales se aplican principios similares: el control del correo electrónico y la vigilancia del acceso a Internet.

El punto de partida es la confirmación de la tesis defendida en el dictamen 8/2001 según el cual la Directiva 95/46/CE se aplica al tratamiento de los datos personales en el contexto profesional como en cualquier otro contexto[14]. Además de la Directiva general 95/46/CE, la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones puede también resultar pertinente. Esta Directiva especifica y completa la Directiva 95/46/CE respecto al tratamiento de los datos personales en el sector de las telecomunicaciones. Además de estar prevista en la Directiva 95/46/CE, la vigilancia por el empleador de las comunicaciones electrónicas, incluidos el correo electrónico y el acceso a Internet, podría también entrar en el ámbito de aplicación de la Directiva 97/66/CE, que actualmente se está examinando en el contexto de la revisión del marco jurídico comunitario en materia de telecomunicaciones. Cuando esta Directiva es aplicable, sus artículos 5 (Confidencialidad de las telecomunicaciones) y 6 (Tráfico y facturación) pueden desempeñar un papel especialmente importante.

3.1 PRINCIPIOS GENERALES APLICABLES A LA VIGILANCIA DEL CORREO ELECTRÓNICO Y LA UTILIZACIÓN DE INTERNET

Los siguientes principios de protección de datos se derivan de la Directiva 95/46/CE y deben respetarse en el tratamiento de los datos personales que implica este tipo de vigilancia. Para que una actividad de control sea legal y se justifique, deben respetarse todos los principios siguientes.

3.1.1. NECESIDAD

Según este principio, el empleador, antes de proceder a este tipo de actividad, debe comprobar si una forma cualquiera de vigilancia es absolutamente necesaria para un objetivo específico. Debería plantearse la posibilidad de utilizar métodos tradicionales de supervisión, que implican una intromisión menor en la vida privada de los trabajadores, y, cuando proceda, aplicarlos antes de recurrir a una forma de vigilancia de las comunicaciones electrónicas.

---

[14] http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48fr.pdf

Sólo en circunstancias excepcionales se considerará necesaria la vigilancia del correo electrónico o de la utilización de Internet de un trabajador. Podría resultar necesario controlar el correo electrónico de un trabajador para obtener una confirmación o una prueba de determinados actos del mismo. En este tipo de actos se incluiría la actividad delictiva de un trabajador que obligara al empleador a defender sus intereses, por ejemplo, cuando es responsable subsidiario de los actos del trabajador. Estas actividades de vigilancia incluirían también la detección de virus y, en general, cualquier actividad realizada por el empleador para garantizar la seguridad del sistema.

Cabe mencionar que la apertura del correo electrónico de un trabajador puede también resultar necesaria por razones distintas del control o la vigilancia, por ejemplo para mantener la correspondencia cuando el trabajador está ausente (por ej. enfermedad o vacaciones) o cuando la correspondencia no puede garantizarse de otra forma (por ej. mediante las funciones de respuesta o desviación automática).

El principio de necesidad significa también que un empleador sólo debe conservar los datos durante el tiempo necesario para el objetivo específico de la actividad de vigilancia.

3.1.2. FINALIDAD

Este principio significa que los datos deben recogerse con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines. En el presente contexto, el principio de «compatibilidad» significa, por ejemplo, que si el tratamiento de los datos se justifica a efectos de seguridad del sistema, estos datos no podrán tratarse posteriormente con otro objetivo, por ejemplo, para supervisar el comportamiento del trabajador.

3.1.3. TRANSPARENCIA

Este principio significa que un empleador debe indicar de forma clara y abierta sus actividades. Dicho de otro modo, el control secreto del correo electrónico por el empleador está prohibido, excepto en los casos en que exista en el Estado miembro una ley que lo autorice en virtud del artículo 13 de la Directiva[15]. Ello puede ocurrir cuando se detecte una actividad delictiva particular (que haga necesaria la obtención de pruebas, y siempre que se cumplan las normas jurídicas y procesales de los Estados miembros) o cuando existan leyes nacionales que autoricen al empleador, previendo las garantías necesarias, a adoptar algunas medidas para detectar infracciones en el lugar de trabajo.

Por otra parte, este principio puede subdividirse en tres aspectos:

3.1.3.1. LA OBLIGACIÓN DE PROPORCIONAR INFORMACIÓN AL INTERESADO

Se trata probablemente del ejemplo más pertinente del principio de transparencia aplicado a la cuestión que nos ocupa. Significa que el empleador debe transmitir a

[15] El artículo 13 de la Directiva permite a los Estados miembros adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en algunos artículos de dicha Directiva, cuando tal limitación constituya una medida necesaria para la salvaguardia de intereses públicos importantes, como la seguridad del Estado, o la prevención, la investigación, la detección y la represión de infracciones penales, o también la protección del interesado o de los derechos y libertades de otras personas.

su personal una declaración clara, precisa y fácilmente accesible de su política relativa a la vigilancia del correo electrónico y la utilización de Internet.

Los trabajadores deben ser informados de manera completa sobre las circunstancias particulares que pueden justificar esta medida excepcional; así como del alcance y el ámbito de aplicación de este control. Esta información debería incluir:

1. La política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales (por ejemplo, períodos y duración de utilización).

2. Los motivos y finalidad de la vigilancia, en su caso. Cuando el empleador autorice a los trabajadores a utilizar los sistemas de comunicación de la empresa con fines personales, las comunicaciones privadas podrán supervisarse en circunstancias muy limitadas, p. ej. para garantizar la seguridad del sistema informático (detección de virus).

3. Información detallada sobre las medidas de vigilancia adoptadas, p. ej. ¿quién? ¿qué? ¿cómo? ¿cuándo?

4. Información detallada sobre los procedimientos de aplicación, precisando cómo y cuándo se informará a los trabajadores en caso de infracción de las directrices internas y de los medios de que disponen para reaccionar en estos casos.

El Grupo de Trabajo desearía destacar aquí que es aconsejable desde un punto de vista práctico que el empleador informe inmediatamente al trabajador de cualquier abuso de las comunicaciones electrónicas detectado, salvo si razones imperiosas justifican la continuación de la vigilancia[16], lo que normalmente no es el caso. Puede transmitirse información rápida fácilmente mediante un programa informático, por ej. ventanas de advertencia que avisen al trabajador de que el sistema ha detectado una utilización ilícita de la red. Un gran número de malentendidos podrían también evitarse de esta manera.

Otro ejemplo del principio de transparencia es la práctica de los empleadores consistente en informar y/o consultar a los representantes de los trabajadores antes de introducir políticas que les conciernan. Cabe destacar que las decisiones relativas a la vigilancia de los trabajadores, en particular, el control de sus comunicaciones electrónicas, están cubiertas por la reciente Directiva 2002/14/CE, siempre que la empresa en cuestión figure en su ámbito de aplicación. En particular, esta Directiva establece la necesidad de informar y consultar a los trabajadores sobre decisiones que puedan implicar cambios importantes en la organización del trabajo o en las relaciones contractuales. La legislación nacional o los convenios colectivos pueden introducir disposiciones más favorables incluso para los trabajadores.

---

[16] En tales casos, por ejemplo, estaría justificada la vigilancia encubierta.

Es posible que los convenios colectivos no sólo obliguen al empleador a informar y consultar a los representantes de los trabajadores antes de instalar sistemas de vigilancia, sino que también supediten esta instalación a su consentimiento previo.

Asimismo, en los convenios colectivos pueden establecerse los límites de la utilización de Internet y del correo electrónico por los trabajadores, así como proporcionarse información detallada sobre el control de esta utilización.

3.1.3.2. LA OBLIGACIÓN DE NOTIFICAR A LAS AUTORIDADES DE SUPERVISIÓN ANTES DE LA APLICACIÓN DE UN TRATAMIENTO TOTAL O PARCIALMENTE AUTOMATIZADO O DE UN CONJUNTO DE TRATAMIENTOS DE ESTE TIPO

Se trata de otro medio de garantizar la transparencia, ya que los trabajadores pueden siempre comprobar en los registros de protección de datos, por ejemplo, qué categorías de datos personales de los trabajadores puede procesar el empleador, con qué finalidad y para qué destinatarios.

3.1.3.3. EL DERECHO DE ACCESO

Un trabajador, así como cualquier otra persona de conformidad con la Directiva[17], tiene derecho a acceder a los datos personales que le conciernen tratados por su empleador y, cuando proceda, a pedir la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular, debido a su carácter incompleto o inexacto.

El acceso de los trabajadores a los archivos del empleador sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos es una herramienta poderosa que los trabajadores pueden utilizar individualmente para garantizar la

---

[17] Artículo 12: Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;

- la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;

- el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.

lealtad y legitimidad de las actividades de vigilancia en el lugar de trabajo. El acceso a los archivos del empleador puede no obstante resultar problemático en circunstancias excepcionales, por ejemplo, el acceso a los datos considerados de evaluación.

El Grupo de Trabajo ya abordó de forma somera esta cuestión[18] y podría proporcionar más orientaciones al respecto a la luz de la experiencia.

3.1.4. LEGITIMIDAD

Este principio significa que una operación de tratamiento de datos sólo puede efectuarse si su finalidad es legítima según lo dispuesto en el artículo 7 de la Directiva y la legislación nacional de transposición. La letra f) del artículo 7 de la Directiva se aplica especialmente a este principio, dado que, para autorizarse en virtud de la Directiva 95/46/CE, el tratamiento de los datos de un trabajador debe ser necesario para la satisfacción del interés legítimo perseguido por el empleador y no perjudicar los derechos fundamentales de los trabajadores.

La necesidad del empleador de proteger su empresa de amenazas importantes, por ejemplo para evitar la transmisión de información confidencial a un competidor, puede considerarse un interés legítimo.

El tratamiento de datos delicados en este contexto es especialmente problemático, ya que el artículo 8 de la Directiva no prevé un equilibrio de intereses según lo dispuesto en la letra f) del artículo 7 de la Directiva. Sin embargo, la letra b) del apartado 2 del artículo 8 hace referencia al tratamiento «necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas».

El tratamiento de datos delicados en relación con las actividades de control y vigilancia es una cuestión espinosa que no sólo es pertinente en un contexto profesional. Se trata en efecto de una cuestión de carácter general sobre la cual el Grupo podría proporcionar orientación en el futuro.

En realidad, a menos que la legislación nacional las autorice específicamente previendo garantías adecuadas, las actividades de vigilancia destinadas directamente al tratamiento de datos delicados relativos a los trabajadores no son legítimas de conformidad con la Directiva 95/46/CE ni tampoco aceptables. No obstante, tampoco parece aceptable impedir o complicar en exceso las actividades de vigilancia (que, en muchos casos no sólo son legales, sino también deseables, como las que tienen por objeto directamente garantizar la seguridad del sistema) por el mero hecho de que sea inevitable el tratamiento de información delicada.

3.1.5. PROPORCIONALIDAD

Según este principio, los datos personales, incluidos los que se utilicen en las actividades de control, deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben. La política de la empresa en este ámbito deberá adaptarse al tipo y grado de riesgo al que se enfrente dicha empresa.

---

[18] Véase la recomendación 1/2001 sobre los datos de evaluación de los trabajadores.

El principio de proporcionalidad excluye por lo tanto el control general de los mensajes electrónicos y de la utilización de Internet de todo el personal, salvo si resulta necesario para garantizar la seguridad del sistema. Si existe una solución que implique una intromisión menor en la vida privada de los trabajadores y que permita lograr el objetivo perseguido, el empleador debería considerar su aplicación (por ejemplo, debería evitar los sistemas que efectúan una vigilancia automática y continua).

Si es posible, el control del correo electrónico debería limitarse a los datos sobre tráfico de los participantes y a la hora de una comunicación más que al contenido, si ello es suficiente para satisfacer las necesidades del empleador. Si el acceso al contenido de los mensajes es indispensable, convendría tener en cuenta el respeto de la vida privada de los destinatarios externos e internos de la organización. Por ejemplo, el empleador no puede obtener el consentimiento de las personas ajenas a la organización que envían mensajes a los miembros de su personal. Del mismo modo, el empleador debería aplicar todos los medios razonables para informar a las personas ajenas a la organización de la existencia de actividades de vigilancia que pudieran afectarlas. Se podría, por ejemplo, insertar avisos de la existencia de sistemas de vigilancia en todos los mensajes salientes de la organización.

La tecnología ofrece al empleador importantes posibilidades de evaluar la utilización del correo electrónico por sus trabajadores, comprobando, por ejemplo, el número de mensajes enviados y recibidos o el formato de los documentos adjuntos; por ello la apertura efectiva de los mensajes electrónicos es desproporcionada. La tecnología puede también utilizarse para garantizar que sean proporcionadas las medidas adoptadas por el empleador para proteger de todo abuso el acceso a Internet autorizado a su personal, utilizando mecanismos de bloqueo más que de vigilancia[19].

Deberían crearse sistemas de tratamiento de las comunicaciones electrónicas para limitar al mínimo estricto la cantidad de datos personales tratados[20].

Por lo que se refiere a la cuestión de la proporcionalidad, debe destacarse que el mecanismo de negociación colectiva puede resultar muy útil para decidir qué acciones son proporcionadas al riesgo que corre el empleador. Es posible alcanzar un acuerdo entre el empleador y los trabajadores sobre la forma de conciliar los intereses de ambas partes.

3.1.6. EXACTITUD Y CONSERVACIÓN DE LOS DATOS

---

[19] Ya existen numerosos ejemplos prácticos de la utilización de estos medios tecnológicos:

- Internet: algunas empresas utilizan un programa informático que puede configurarse para impedir la conexión a categorías predeterminadas de sitios web. Tras consultar la lista global de los sitios web visitados por su personal, el empleador puede decidir añadir algunos sitios a la lista de los bloqueados (eventualmente después de haber informado a los trabajadores de que se bloqueará la conexión con este sitio, salvo si un trabajador le demuestra la necesidad de conectarse).

- Correo electrónico: otras empresas utilizan una función de desviación automática hacia un servidor aislado para todos los mensajes que superan un determinado volumen. Se informa automáticamente al destinatario de que se ha desviado un mensaje sospechoso hacia este servidor, donde puede consultarlo.

[20] Proyecto de Directiva 97/66, considerando 30.

Este principio requiere que todos los datos legítimamente almacenados por un empleador (después de tener en cuenta todos los demás principios enunciados en este capítulo) que incluyan datos procedentes de una cuenta de correo electrónico de un trabajador, de su utilización de Internet o relativos a las mismas deberán ser precisos y actualizarse y no podrán conservarse más tiempo del necesario. Los empleadores deberían especificar un período de conservación de los mensajes electrónicos en sus servidores centrales en función de las necesidades profesionales. Normalmente, es difícil imaginar que pueda justificarse un período de conservación superior a tres meses.

3.1.7. SEGURIDAD

Este principio obliga al empleador a aplicar las medidas técnicas y organizativas adecuadas para proteger todos los datos personales en su poder de toda intromisión exterior. Incluye también el derecho del empleador a proteger su sistema contra los virus y puede implicar el análisis automatizado de los mensajes electrónicos y de los datos relativos al tráfico en la red.

El Grupo de Trabajo opina que, dada la importancia de garantizar la seguridad del sistema, la apertura automatizada de los mensajes electrónicos no debe considerarse una violación del derecho del trabajador a la vida privada, siempre y cuando existan garantías adecuadas. Por ejemplo, los empleadores pueden ahora utilizar tecnologías que responden a sus intereses en términos de seguridad, pero que no violan el derecho de los trabajadores a la vida privada.

El Grupo de Trabajo «Artículo 29» llama la atención sobre el papel del administrador del sistema, un trabajador cuyas responsabilidades en materia de protección de datos son importantes. Es fundamental que el administrador del sistema, así como cualquier persona que tenga acceso a datos personales de los trabajadores durante las operaciones de control, esté sometido a una obligación estricta de secreto profesional respecto a la información confidencial a la que pueda acceder.

4. CONTROL DEL CORREO ELECTRÓNICO

4.1. EL SECRETO DE CORRESPONDENCIA

Tal como se ha explicado anteriormente en el presente documento de trabajo, el Grupo de Trabajo considera que las situaciones en línea y fuera de línea no deben tratarse de manera diferente sin motivo y que, por lo tanto, los mensajes electrónicos deben beneficiarse de la misma protección de los derechos fundamentales que el correo tradicional[21]. La jurisprudencia del Tribunal Europeo de Derechos Humanos ha proporcionado orientación sobre la aplicación del principio del secreto de correspondencia en una sociedad democrática. No obstante, los ordenamientos jurídicos de los Estados miembros interpretan este principio de manera ligeramente diferente, en particular, desde el punto de vista de su ámbito de aplicación a las comunicaciones profesionales, tanto por lo que se refiere a su contenido como a los datos relativos al tráfico. Desde el punto de vista de la protección de datos, este principio tiene consecuencias importantes al considerar el grado de intromisión tolerable en el correo electrónico de los trabajadores.

El Grupo de Trabajo «Artículo 29» opina que las comunicaciones electrónicas que proceden de locales profesionales pueden estar cubiertas por los conceptos de «vida privada» y de «correspondencia» según lo dispuesto en el apartado 1 del artículo 8 del Convenio europeo. Hay poco margen de interpretación a este respecto, puesto que el Tribunal ya reguló claramente la cuestión en el asunto **Halford contra el Reino Unido mencionado más arriba.**

Lo que queda por examinar, y se presta de hecho a cierto margen de interpretación, es en qué medida pueden permitirse excepciones o restricciones a este principio, sobre todo cuando entra en conflicto con derechos y libertades de otros que también son protegidos por el Convenio (por ej. los intereses legítimos del empleador). **En cualquier caso, el secreto de las comunicaciones y de la correspondencia no depende de la ubicación y la propiedad de los medios electrónicos utilizados, según se establece en constituciones y principios jurídicos fundamentales.**

El Grupo de Trabajo «Artículo 29» desearía, sin embargo, recordar que no se trata de un problema específico del tratamiento de los datos de carácter personal en el contexto profesional, sino de un problema general que se deriva del hecho de que las legislaciones y reglamentos sobre protección de datos no se aplican en abstracto. Se supone que los derechos relativos a la protección de datos se aplican a distintos sistemas jurídicos, con otras leyes vigentes que prevén otros derechos y obligaciones para los individuos (por ej.

---

[21] Una de las primeras recomendaciones formuladas por el Grupo de Trabajo, la Recomendación 3/97 «Anonimato en Internet», ya precisaba que las situaciones en línea y fuera de línea debían tratarse de manera idéntica.

Véase http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp6es.pdf

El documento del Grupo de Trabajo sobre Internet, que es el más importante adoptado por el Grupo de Trabajo sobre la privacidad en Internet, hacía hincapié en esta idea en su capítulo 3, página 23:

Véase http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37es.pdf

el Derecho laboral). No obstante, el Grupo de Trabajo «Artículo 29» está convencido de que las soluciones propuestas en el presente documento pueden ser útiles para alcanzar este difícil equilibrio de intereses.

4.2. LEGITIMACIÓN DE CONFORMIDAD CON LA DIRECTIVA 95/46/CE

Los mensajes electrónicos contienen datos personales que son protegidos por la Directiva 95/46/CE, por lo que los empleadores deben tener un motivo legítimo para proceder al tratamiento de estos datos. Como se explicó de manera detallada en el dictamen 8/2001, los trabajadores deben dar su consentimiento libremente y con conocimiento de causa; y los empleadores no deben recurrir al consentimiento como medio general de legitimar tratamientos de este tipo.

La legitimación más idónea de la vigilancia del correo electrónico puede encontrarse en la letra f) del artículo 7 de la Directiva, que prevé que el tratamiento sólo pueda efectuarse si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos. Antes de analizar la aplicación de esta disposición al ámbito que nos ocupa, conviene indicar que tal legitimación no puede anular derechos y libertades fundamentales de los trabajadores. Ello incluye, en su caso, el derecho fundamental al secreto de la correspondencia.

El Grupo de Trabajo ya ha opinado lo siguiente[22]:

«Si un empresario debe tratar datos personales como consecuencia inevitable y necesaria de la relación laboral, actuará de forma engañosa si intenta legitimar este tratamiento a través del consentimiento. El recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello.»

Dado que los mensajes electrónicos contienen datos personales que se refieren tanto al emisor como al destinatario y que los empleadores pueden en general obtener el consentimiento de una de estas partes sin demasiadas dificultades (a menos que el correo electrónico incluya también la correspondencia entre trabajadores de la empresa), la posibilidad de legitimar el control del correo electrónico sobre la base del consentimiento es muy limitada. Estas consideraciones se aplican también a la letra b) del artículo 7 de la Directiva, ya que una de las partes de la correspondencia nunca tendría contrato con el responsable del tratamiento con arreglo a dicha disposición, es decir, para el control de la correspondencia.

En esta fase, debe señalarse que cuando el trabajador recibe una cuenta de correo electrónico para uso estrictamente personal o puede acceder a una cuenta de correo web, la apertura por el empleador de los mensajes electrónicos de esta cuenta (excepto para detectar virus) sólo podrá justificarse en circunstancias muy limitadas[23] y no podrá justificarse en circunstancias normales con arreglo a la letra f) del artículo 7, ya que acceder a este tipo de datos no es necesario para satisfacer un interés legítimo del

---

[22] Véase el recuadro de la página 23 del dictamen 8/2001.

[23] Por ejemplo, actividades delictivas del trabajador que obliguen al empleador a defender sus intereses, cuando sea responsable de los actos del trabajador o cuando él mismo sea víctima del delito.

empleador. En este caso, prevalece por el contrario el derecho fundamental al secreto de correspondencia.

En consecuencia, la cuestión de en qué medida la letra f) del artículo 7 autoriza el control del correo electrónico depende de la aplicación caso por caso de los principios fundamentales explicados en el capítulo 3.2. Como ya se menciona en el apartado 3.1.4 (Legitimidad), al sopesar los intereses de las partes, conviene tener en cuenta el respeto de la vida privada de las personas ajenas a la organización afectadas por la actividad de vigilancia.

4.3 INFORMACIÓN MÍNIMA RECOMENDADA QUE UNA EMPRESA DEBERÍA FACILITAR A SU PERSONAL

Al elaborar su política, los empleadores deben respetar los principios enunciados en el apartado 3.1.3 relativo al principio general de transparencia[24], habida cuenta de las necesidades y el tamaño de la organización.

Además, en el ámbito más específico del correo electrónico, deberán abordarse los puntos siguientes:

a) Determinar si un trabajador está autorizado a disponer de una cuenta de correo electrónico de uso estrictamente personal, si está permitida la utilización de cuentas de correo web en el lugar de trabajo y si el empleador recomienda a su personal la utilización de una cuenta privada de correo web para utilizar el correo electrónico con fines exclusivamente personales (véase el capítulo 4.4).

b) Los acuerdos con los trabajadores sobre el acceso al contenido del correo electrónico, por ej. cuando el trabajador se ausenta repentinamente, y las finalidades específicas de este acceso.

c) Indicar el periodo de conservación de las posibles copias de protección de los mensajes.

d) Precisar cuándo se borran definitivamente los mensajes electrónicos del servidor.

e) Cuestiones de seguridad.

24

1. La política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales (por ejemplo, períodos y duración de utilización).

2. Los motivos y finalidad de la vigilancia, en su caso. Cuando el empleador autorice a los trabajadores a utilizar los sistemas de comunicación de la empresa con fines personales, las comunicaciones privadas podrán supervisarse en circunstancias muy limitadas, p. ej. para garantizar la seguridad del sistema informático (detección de virus).

3. Información detallada sobre las medidas de vigilancia adoptadas, p. ej. ¿quién? ¿qué? ¿cómo? ¿cuándo?

4. Información detallada sobre los procedimientos de aplicación, precisando cómo y cuándo se informará a los trabajadores en caso de infracción de las directrices internas y de los medios de que disponen para reaccionar en estos casos.

f) Participación de los representantes de los trabajadores en la formulación de la política.

Conviene señalar que el empleador debe garantizar permanentemente la actualización de su política de acuerdo con la evolución tecnológica y la opinión de su personal.

4.4 CORREO WEB[25]

El Grupo de Trabajo considera que la posibilidad de que los trabajadores utilicen una cuenta privada de correo electrónico o un correo web podría suponer una solución pragmática del problema. Una recomendación en este sentido por parte del empleador facilitaría la distinción entre el correo electrónico de uso profesional y el de uso privado y reduciría el riesgo de intromisión de los empleadores en la vida privada de sus trabajadores. Además, los costes suplementarios para el empleador serían nulos o mínimos.

Si se adopta esta política, el empleador podrá controlar, en casos específicos en que existan sospechas graves sobre el comportamiento de un trabajador, en qué medida éste utiliza su ordenador con fines personales, contabilizando el tiempo que emplea en las cuentas del correo web. Esta solución satisface los intereses del empleador y evita el riesgo de revelación de datos personales de los trabajadores, y, en particular, de datos delicados.

Además esta política favorecería también a los trabajadores, porque les permitiría saber con seguridad el nivel de confidencialidad que pueden esperar, lo que no quizá no sería el caso con códigos de conducta más complejos y confusos. Dicho esto, conviene también indicar lo siguiente:

a) **El hecho de autorizar la utilización del correo web o de cuentas privadas no es óbice para la plena aplicación de los puntos anteriores del presente capítulo a otras cuentas de correo electrónico en el lugar de trabajo.**

b) Al autorizar el correo web, las empresas deben saber que su uso puede comprometer la seguridad de sus redes, en particular, por lo que se refiere a la proliferación de virus.

c) Los trabajadores deberían saber que, a veces, los servidores del correo web están situados en terceros países que quizá no cuenten con un sistema adecuado de protección de los datos de carácter personal.

Debe tenerse en cuenta que estas consideraciones se aplican a las relaciones normales entre empleadores y trabajadores. Podría resultar necesario aplicar normas especiales a la comunicación de los trabajadores obligados a guardar secreto profesional.

[25] El correo web es un sistema de correo electrónico en la red que ofrece funciones de correo electrónico a partir de cualquier distribuidor POP o IMAP y que está protegido generalmente por un nombre de usuario y una contraseña.

5. CONTROL DEL ACCESO A INTERNET

5.1 UTILIZACIÓN DE INTERNET CON FINES PRIVADOS EN EL LUGAR DE TRABAJO

En primer lugar, conviene destacar que incumbe a la empresa decidir si autoriza a su personal a navegar en Internet con fines privados y, en caso afirmativo, en qué medida se tolera esta utilización privada.

El Grupo considera no obstante que una prohibición absoluta de la utilización de Internet con fines privados por los trabajadores 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.

5.2. PRINCIPIOS RELATIVOS AL CONTROL DE LA UTILIZACIÓN DE INTERNET

Al considerar la cuestión del control de la utilización de Internet por los trabajadores pueden aplicarse algunos principios.

En la medida de lo posible, **la prevención debería primar sobre la detección**. En otras palabras, al empleador le es más beneficioso prevenir la utilización abusiva de Internet por medios técnicos que destinar recursos a su detección. Dentro del límite de lo que es razonablemente posible, la política de la empresa respecto a Internet debería basarse en herramientas técnicas para limitar el acceso, más que en dispositivos de control de los comportamientos, por ejemplo, bloqueando el acceso a algunos sitios o instalando advertencias automáticas.

El suministro al trabajador de información rápida sobre la detección de una utilización sospechosa de Internet es importante para minimizar los problemas. Aunque sea necesaria, toda medida de control debe ser **proporcionada** al riesgo que corre el empleador. En la mayoría de los casos, la utilización abusiva de Internet puede detectarse sin tener que analizar el contenido de los sitios visitados. Por ejemplo, la comprobación del tiempo empleado o la elaboración de una lista de los sitios más visitados por un servicio podría bastar para confirmar al empleador que sus sistemas se emplean correctamente. Si estas comprobaciones generales revelaran una posible utilización abusiva de Internet, el empleador podría entonces considerar la posibilidad de proceder a nuevos controles en la zona de riesgo.

Al analizar la utilización de Internet por los trabajadores, los empleadores **deberían evitar sacar conclusiones precipitadas**, dada la facilidad con que pueden visitarse involuntariamente algunos sitios a través de respuestas de motores de búsqueda, vínculos hipertextuales ambiguos, pancartas publicitarias engañosas o errores al pulsar las teclas. En todos los casos, deberán presentarse al trabajador en cuestión todos los hechos de que se le acusa y ofrecerle la posibilidad de refutar la utilización abusiva alegada por el empleador.

5.3 CONTENIDO MÍNIMO RECOMENDADO DE LA POLÍTICA DE LA EMPRESA SOBRE LA UTILIZACIÓN DE INTERNET

1. La información que se especifica en el apartado 3.1.3., relativo al principio de transparencia[26].

   Además, en el ámbito más específico del correo electrónico, deberán abordarse los puntos siguientes.

2. El empleador deberá precisar claramente a los trabajadores en qué condiciones se autoriza la utilización de Internet con fines privados e indicarles los elementos que no pueden visualizar o copiar. Estas condiciones y restricciones deberán explicarse al personal.

3. Deberá informarse a los trabajadores de los sistemas instalados para impedir el acceso a algunos sitios o para detectar una posible utilización abusiva. Deberán precisarse el alcance del control, por ejemplo si este control se efectúa de manera individualizada o por departamentos de la empresa, o si el contenido de los sitios consultados será visualizado o registrado por el empleador en determinados casos. Además, la política de la empresa deberá especificar, cuando proceda, el uso que se hará de los datos recogidos sobre las personas que visitaron sitios específicos.

4. Deberá informarse a los trabajadores del papel de sus representantes, tanto en la aplicación de la política como en la investigación de las presuntas infracciones.

CONCLUSIÓN

El Grupo de Trabajo ha redactado el presente documento de trabajo con el fin de contribuir a la aplicación uniforme de las medidas nacionales adoptadas de conformidad con la Directiva 95/46/CE en el ámbito de la vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo. (Sírvanse consultar los resúmenes de las legislaciones nacionales que se adjuntan al presente documento).

El Grupo de Trabajo ha observado algunas divergencias entre las legislaciones nacionales, principalmente en ámbitos vinculados a la protección de datos que tratan de las excepciones al derecho fundamental al secreto de correspondencia y al alcance y repercusiones de la representación y la codecisión colectivas. Desearía, sin embargo, destacar que ninguna divergencia entre las legislaciones de los Estados miembros que

---

26

1. La política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales (por ejemplo, períodos y duración de utilización).

2. Los motivos y finalidad de la vigilancia, en su caso. Cuando el empleador autorice a los trabajadores a utilizar los sistemas de comunicación de la empresa con fines personales, las comunicaciones privadas podrán supervisarse en circunstancias muy limitadas, p. ej. para garantizar la seguridad del sistema informático (detección de virus).

3. Información detallada sobre las medidas de vigilancia adoptadas, p. ej. ¿quién? ¿qué? ¿cómo? ¿cuándo?

4. Información detallada sobre los procedimientos de aplicación, precisando cómo y cuándo se informará a los trabajadores en caso de infracción de las directrices internas y de los medios de que disponen para reaccionar en estos casos.

aplican la Directiva 95/46/CE constituye un obstáculo fundamental para la adopción del enfoque común previsto en los principios y buenas prácticas señaladas en el presente documento de trabajo.

El Subgrupo de Empleo seguirá revisando el presente documento de trabajo a la luz de la experiencia y de futuros avances en este ámbito durante 2002- 2003.

Hecho en Bruselas, el 29 de mayo de 2002

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA