GOVERTIS
Advisory Services

ADOPCIÓN DE UNA POLÍTICA DE USO Y CONTROL DE LAS TIC EN EL ÁMBITO LABORAL. NOCIONES JURÍDICAS BÁSICAS.

ÍNDICE DEL DOCUMENTO.

Versión	Fecha	Autor	Cambios
01	28/02/2016	Marina Medela Patrick Monreal	Versión inicial

1. - INTRODUCCIÓN.

Este documento trata de ser una ayuda para que un Empresario o Empleador sepa cómo llevar a cabo un control o vigilancia de las Tecnologías de la Información y la Comunicación (TIC), sin menoscabar el derecho a la intimidad, secreto de las comunicaciones o la protección de datos de carácter personal de los trabajadores.

Las **Tecnologías de la Información y la Comunicación (TIC)** pueden definirse como aquellas herramientas informáticas que procesan, almacenan, sintetizan, recuperan y presentan información expuesta de la más variada forma. Constituyen nuevos soportes y canales para dar forma, registrar, almacenar y difundir contenidos. Ejemplo de estas tecnologías son: el ordenador personal, el proyector multimedia, los cuadernos de bitácoras (en inglés, blogs), los podcast y, por supuesto, la web.

Las **Nuevas Tecnologías en el ámbito laboral** influyen no sólo en la capacidad productiva empresarial, sino que también ejercen gran influencia en relación con el mercado de trabajo y el mantenimiento del empleo. Así, la utilización del correo electrónico, el acceso a Internet, la utilización sindical de una intranet, la aceptación de la firma electrónica como modo de contraer obligaciones contractuales, el tratamiento automatizado de datos e informaciones relativas al trabajador, la aplicación de las nuevas tecnologías en la vigilancia y control de la prestación laboral o el teletrabajo; son algunas de las manifestaciones de la generalización de las nuevas tecnologías en la empresa.

A priori, pueden señalarse tres puntos de análisis en relación con la utilización de las nuevas tecnologías en el lugar de trabajo:

1. La utilización de las TIC por los trabajadores para fines no empresariales.

2. Las medidas que puede adoptar el Empresario en el ejercicio de su facultad disciplinaria.

3. El poder de dirección y sus límites, pues éstos pueden resultar lesivos para los derechos fundamentales de la persona del trabajador, más concretamente puede vulnerar el derecho al honor e intimidad personal, pudiendo dar lugar a sanciones en el orden social e incluso penal, siendo, por tanto, el Derecho el encargado de encontrar el equilibrio entre la utilización de las nuevas tecnologías en el ámbito laboral y el respeto de los derechos fundamentales del trabajador.

2. - MARCO NORMATIVO.

- 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.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. (ET)
- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.
- Jurisprudencia del Tribunal Constitucional, Tribunal Supremo, Tribunales Superiores de Justicia de las Comunidades Autónomas y Audiencias Provinciales.
- Informes y resoluciones de la Agencia Española de Protección de Datos. (AEPD)

Esta relación no es cerrada y tan sólo pretende hacer referencia a la principal normativa de aplicación en esta materia.

3.- LEGITIMACIÓN PARA EL CONTROL Y VIGILANCIA.

El Empresario estará legitimado para la adopción de estas medidas de control, teniendo en cuenta que en ocasiones, los 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.

Es evidente, la cada vez mayor utilización de las nuevas tecnologías en general y, en particular, en el ámbito laboral. Ello conlleva, entre otras consecuencias, la posibilidad de contar con herramientas informáticas por parte de los trabajadores. El control de estas herramientas por parte del Empresario puede suponer, en ocasiones, una merma cuando no, una quiebra total de la privacidad del trabajador.

Pero este derecho del trabajador *"ha de 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."*

Históricamente, se ha producido un debate sobre la aplicabilidad al control de las TIC de uno u otro artículo del Estatuto de los Trabajadores ponderando, por un lado, la inviolabilidad de la persona del trabajador y, por otro, la dirección y control de actividad laboral:

Artículo 18. Inviolabilidad de la persona del trabajador.

<< Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible >>

Artículo 20.3 Dirección y control de la actividad laboral.

<< El Empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso >>

El Tribunal Supremo en el transcurso del tiempo ha tenido diferentes pronunciamientos.

El último realizado con carácter relevante es el recogido en la **sentencia de 16 de junio de 2014,** la cual ha venido a alterar el estado de las cosas en lo que respecta a técnicas de monitorización y acceso al correo electrónico profesional del empleado, creando dos líneas jurisprudenciales diferentes a la hora de valorar la licitud de una prueba, lo que obliga a rediseñar los protocolos, manuales, documentos y procedimientos internos relativos a la seguridad de la información y protección de datos.

Así, el TS en esta sentencia distingue:

- Los mensajes de correo que ya han sido abiertos, o leídos, por su destinatario, pasan a ser considerados ficheros de datos.
- Los que permanecen cerrados o, todavía no leídos, se ven afectados por el secreto de las comunicaciones.

El Alto Tribunal declara que para acceder a estos últimos se requiere disponer previamente de autorización judicial en virtud del derecho fundamental al secreto de las comunicaciones y en concordancia con el artículo 579 de la Ley de Enjuiciamiento Criminal (LECRIM).

Hasta ese momento, la reiterada jurisprudencia de la Sala de lo Social del Tribunal Supremo y del propio Tribunal Constitucional venían amparando estas prácticas en base a lo dispuesto en el artículo 20.3 del Estatuto de los Trabajadores.

De este modo, el Empresario podrá adoptar las medidas de control y vigilancia de acuerdo con las exigencias de la buena fe:

- Si hubiera advertido previamente de tal circunstancia y se hubieran fijado las reglas del juego.

- Si hubiera prohibido, total o parcialmente, el uso personal de estos medios profesionales.

Es práctica cada vez más frecuente que las organizaciones notifiquen por escrito a sus empleados la prohibición de utilizar para asuntos propios durante la jornada de trabajo el ordenador, los móviles, internet o cualquier otro medio puesto a su disposición para el desempeño de la actividad laboral.

En un primer momento, el **Tribunal Supremo en su Sentencia de 26 de septiembre de 2007** ante el supuesto planteado de si la empresa puede acceder al correo electrónico del trabajador estableció que "*en síntesis prevé la posibilidad de que el Empresario pueda acceder al control del ordenador, del correo electrónico y los accesos a Internet de los trabajadores, siempre que la empresa de buena fe haya establecido previamente las reglas de uso de esos medios con aplicación de prohibiciones absolutas o parciales e informado de que va existir un control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos*".

Posteriormente, el **Tribunal Supremo da un paso más en su sentencia de 6 de octubre de 2011** en la que estableció que "*si la empresa prohíbe totalmente el uso de estas tecnologías con fines particulares, ya sea dentro o fuera del horario laboral, no se puede entender que el Derecho Fundamental a la Intimidad o al Secreto de las comunicaciones opera en el uso de estos equipos*".

NOTA: Si el Empresario o la Organización , extralimitándose en las facultades que le otorga el Estatuto de los Trabajadores, incurrirá en responsabilidad penal de acuerdo con el art. 197 CP[1] si realiza alguna de las conductas reflejadas, ya que estará vulnerando el derecho a la intimidad del trabajador.

[1]Artículo 197 del Código Penal, supuestos:

- Aquel que se apodere de papeles, cartas, mensajes de correo electrónico o de otros efectos personales con el fin de descubrir secretos o vulnerar la intimidad de otra persona.

-Quienes intercepten telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o

4.- VIGILANCIA Y CONTROL DE LAS COMUNICACIONES ELECTRÓNICAS EN EL LUGAR DE TRABAJO.

4.1 DERECHO A LA INTIMIDAD Y DERECHO A LA PROTECCIÓN DE DATOS.

El **Derecho a la Intimidad** confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona regulado en el artículo 18 de la Constitución Española. Asimismo, el derecho a la intimidad incluye el derecho a la intimidad personal y familiar, el secreto de las comunicaciones y por último, el derecho a la al honor y a la propia imagen.

Sin embargo, el **Derecho de la Protección de Datos** se refiere a todo tipo de datos, sean íntimos o no. Por tanto el ámbito que protege es mucho más amplio y se encuentra regulado en el artículo 18.4 de la CE

Si bien, es cierto que muchas veces se entremezclan ambos conceptos pero conviene marcar la diferencia.

Además desde el año 2000 **el Tribunal Constitucional en su Sentencia 292/2000 de 30 de noviembre** ha consagrado el derecho a la protección de datos como derecho fundamental autónomo e independiente del derecho a la intimidad y familiar del artículo 18 CE.

En el ámbito de los derechos fundamentales laborales, la doctrina y la jurisprudencia han diferenciado dos tipos; los **derechos fundamentales laborales específicos,** que son aquéllos que el trabajador únicamente ejerce dentro de las relaciones laborales, siendo sus titulares los trabajadores asalariados o los Empresarios, en tanto que también son sujetos de la relación laboral. Entre ellos se pueden destacar el derecho de huelga, el derecho al salario o el derecho a la negociación colectiva.

Y en el ámbito de los **derechos fundamentales laborales inespecíficos** son aquéllos que el trabajador tiene fuera del ámbito laboral, pero que cuando son ejercitados dentro de la relación jurídica laboral se convierten en verdaderos derechos laborales por razón de los sujetos y de la naturaleza de la relación jurídica en que se hacen valer.

---

reproducción del sonido o de la imagen.

- El apoderamiento, utilización o modificación, en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro, que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado.
- La pena de prisión será de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.
- Si estos hechos se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros.
- Cuando los hechos descritos afecten a datos de carácter personal que re-velen la ideología, religión, creencias, salud, origen racial o vida sexual o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.
- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior.

4.2 DEL ACCESO A LOS DATOS DE TRÁFICO DE LAS COMUNICACIONES ELECTRÓNICAS Y DE LA AUTORIZACIÓN JUDICIAL NECESARIA PARA ACCEDER AL CONTENIDO.

Ahora bien, sentado que la Organización puede estar legitimada para el control o monitorización del correo electrónico, siempre y cuando haya informado previamente a los empleados acerca de la adopción de esta medida y las normas de uso de las TIC, no con esto estará facultado para el acceso al contenido de las comunicaciones hechas por correo electrónico.

Asimismo, la **Sentencia 2844/2014 de la Sala de lo Penal de Tribunal Supremo de 16 de junio de 2014** "*...el ordenador registrado era una herramienta propiedad de la empresa y facilitada por la empresa a don AAA exclusivamente para desarrollar su trabajo, por lo que entendemos que incluso en aquel supuesto en que pudiera utilizar el ordenador para emitir algún tipo de mensaje de carácter personal, entendemos que al utilizar precisamente un ordenador ajeno, de la empresa, y destinado exclusivamente para el trabajo a la empresa, estaba asumiendo -cediendo- la falta de confidencialidad -secreto- de las comunicaciones que pudiera tener el señor AAA utilizando tal terminal informático*". De esta sentencia, podemos extraer que:

1. El artículo 18.3 de la Constitución, que garantiza el secreto de las comunicaciones, no exceptúa dicha garantía por la titularidad del medio, ni por su carácter empresarial, ni por el momento en que sucede la comunicación.

2. Tampoco permite excepciones a la exigencia de autorización judicial para la intervención de los medios de comunicación, a diferencia de la entrada en el domicilio (18.2 CE).

3. Ni siquiera contempla la posibilidad de que el interesado renuncie a esta libertad (lo que sí se permite en el caso de la entrada en domicilio).

4. Además, la interceptación afecta a la libertad del tercero con quien se comunica el empleado, que puede ser ajeno a la relación laboral.

Se cuestiona a raíz de la presente sentencia, si es necesaria la **AUTORIZACIÓN JUDICIAL** para intervenir en un medio de comunicación, y que sin la misma se puede vulnerar el secreto de las comunicaciones, puede ser, incluso, constitutivo de delito.

No obstante, y esto es importante, el Tribunal Supremo matiza que el art. 18.3 de la Constitución (secreto de las comunicaciones) no protege los mensajes, sino los medios de comunicación propiamente dichos. Por tanto, el secreto de las comunicaciones no limita ni condicionan la actividad de control empresarial que consista en analizar y obtener pruebas de:

- Los mensajes "una vez recibidos y abiertos por su destinatario".

- Los datos de tráfico (circunstancias de tiempo, líneas utilizadas, duración de la comunicación, etc.).

- El uso del ordenador para navegar por Internet (páginas visitadas, tiempo consumido navegando, etc.).

Es decir, según esta sentencia, no se precisa de autorización judicial para investigar los archivos en el disco duro del ordenador del empleado, o los mensajes remitidos o leídos en las bandejas de correo electrónico (normalmente en el servidor), ni los datos de tráfico de las comunicaciones.

En estos supuestos no se precisa autorización judicial por no quedar afectado el secreto de las comunicaciones, pero si se deben de respetar las garantías que exijan otros derechos del ámbito de la privacidad como son el derecho a la protección de datos o el derecho a la intimidad.

El **secreto de las comunicaciones**, que la Constitución garantiza salvo resolución judicial, es un concepto rigurosamente formal, en el sentido de que ***"se predica de lo comunicado, sea cual sea su contenido"*** (SSTC 114/1984, de 29 de noviembre, FJ 7; y 34/1996, de 11 de marzo, FJ 4).

El objeto de protección en este caso, no será el contenido mismo de la comunicación, cuyo contenido puede ser de carácter personal, íntimo o de interés profesional, sino el propio proceso de comunicación en sí mismo considerado, a través de canales o medios cerrados y con respecto a injerencias de terceros.

Como siempre, hay ejemplos de conductas que pueden justificar el control del correo electrónico de un trabajador para obtener información o una prueba de determinados actos del mismo, son los siguientes:

- Investigar una posible actividad delictiva de un trabajador que obligará al Empleador a defender sus intereses, por ejemplo cuando es responsable subsidiario de los actos del trabajador.

- Detectar virus y, en general, cualquier actividad realizada por el Empleador para garantizar la seguridad de la misma.

- Cabe mencionar que la apertura del correo electrónico de un trabajador puede también resultar necesaria 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).

Por otro lado, la Agencia Española de Protección de Datos se ha pronunciado al respecto en distintos informes, como el **Informe 0247/2008** y el **Informe 0615/2009**, en los que manifiesta lo siguiente:

<< 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. 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 >>.

4.3 OBLIGACIÓN DE PROPORCIONAR INFORMACIÓN AL INTERESADO.

El Empleador debe transmitir a 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, se muestra por ejemplo el **Informe 582/2009** de la AEPD. Esta información debería incluir **necesariamente**:

- 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).

- 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, por ejemplo para garantizar la seguridad del sistema informático (detección de virus).

- Información detallada sobre las medidas de vigilancia adoptadas, por ejemplo, quién ha adoptado las medidas, qué medidas se han adoptado y cuándo.

- 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.

Adicionalmente, **es conveniente**:

Que se informe inmediatamente al trabajador de cualquier abuso de las comunicaciones electrónicas detectado, salvo que haya razones imperiosas justifican la continuación de la vigilancia, lo que normalmente no es el caso.

Ello se puede hacer de diversas formas:

- Transmitirse información rápida fácilmente mediante un programa informático, por ejemplo, a través de 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, atendiendo a un principio de transparencia empresarial, 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.

- Además, 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.

En definitiva, podemos decir que lo determinante para que la Organización pueda legalmente controlar el correo de sus empleados, es que previamente les haya advertido de dicha circunstancia y de que la medida esté orientada a mejorar las tareas laborales.

Y es **obligatoria**:

La notificación a la Agencia Española de Protección de Datos los ficheros o tratamientos que se produzcan, para que los trabajadores siempre puedan comprobar en los registros, por ejemplo, qué categorías de datos personales de los trabajadores puede procesar el Empleador, con qué finalidad y para qué destinatarios.

Y frente a su **vulneración** cabe:

El ejercicio de los derechos Acceso, Rectificación, Cancelación y Oposición (A.R.C.O.). Esto es, un trabajador como afectado o interesado que es, tendrá estos derechos en relación con sus datos de carácter personal tratados por su Empleador, teniendo en cuenta que éstos, como cualquier otro, no son absolutos, teniendo límites en su ejercicio.

4.4. JUICIOS DE PROPORCIONALIDAD, NECESIDAD E IDONEIDAD DE LAS MEDIDAS DE CONTROL.

El Tribunal Constitucional (TC) considera que el ejercicio de cualquier derecho fundamental consagrado en nuestra Constitución, no es de carácter absoluto, sino que se debe contraponer con el ejercicio de otros derechos o bienes jurídicos protegidos, siendo la función de los órganos jurisdiccionales y, en concreto del TC, preservar el equilibrio necesario ante una posible colisión de intereses contrapuestos.

Para comprobar si una medida es restrictiva de un derecho fundamental ésta debe superar o cumplir los tres siguientes requisitos o condiciones:

- Si tal medida es susceptible de conseguir el objetivo propuesto (**juicio de idoneidad**);

- Si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (**juicio de necesidad**);

- Y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (**juicio de proporcionalidad, en sentido estricto**) (STC 96/2012, de 7 de mayo, FJ 10; o SSTC 14/2003, de 28 de enero, FJ 9; 89/2006, de 27 de marzo, FJ 3).

A mayor abundamiento, para que una actividad de control sea legal y se justifique, deben respetarse todos los principios siguientes:

- **Necesidad.-** Según este principio, antes de proceder a este tipo de control, debe comprobar si una forma cualquiera de vigilancia es absolutamente necesaria para un objetivo específico. Este principio supone contar que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia. Por tanto, el Empleador, antes de proceder a este tipo de control, debe comprobar que es absolutamente necesaria para un objetivo específico.

- **Legitimidad.-** Este principio significa que el acceso a las comunicaciones electrónicas sólo puede efectuarse si su finalidad es legítima. La necesidad de proteger su sistema de amenazas importantes, por ejemplo para evitar la transmisión de información confidencial de trabajadores, puede considerarse un interés legítimo.

- **Proporcionalidad.-** Según este principio, de la medida adoptada, de control y vigilancia, se derivarán más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

- **Seguridad.-** Este principio obliga a aplicar las medidas de seguridad, técnicas y organizativas, adecuadas para proteger el sistema de comunicación y, por ende, los datos personales, de toda intromisión exterior. Se trata de la facultad de 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.

En la **sentencia 186/2000, de 10 de julio del TC**, considera que la medida de instalación de un circuito cerrado de televisión, que controlaba la zona donde el trabajador desempeñaba su actividad laboral, era una medida justificada (ya que existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo); idónea para la finalidad pretendida por la empresa (verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja y a una duración temporal limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE.

Con esto, el TC desestimó el recurso de amparo presentado por el trabajador, al considerar que su derecho a la intimidad no había sido vulnerado. El TC reitera que el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho (SSTC 57/1994, F. 6, y 143/1994), teniendo siempre presente el principio de proporcionalidad.

5.- CONTROL TRÁFICO DE RED O USO DE 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.

No obstante, 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.

De esta manera, si el medio se utiliza para usos privados en contra de las prohibiciones de uso 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.

En la **sentencia de 6 de octubre de 2011**, el **Tribunal Supremo** dice que en el caso de uso personal de los medios informáticos de la empresa, no puede existir un conflicto de derechos cuando hay una prohibición válida (la prohibición absoluta podría no ser válida si, por ejemplo, el convenio colectivo reconoce el derecho a un uso personal de ese uso). La prohibición determina que ya no exista una situación de tolerancia con el uso personal del ordenador y que tampoco exista lógicamente una "expectativa razonable de confidencialidad".

El mismo **Tribunal Supremo** (TS), en **sentencia del 26 de septiembre de 2007** , dispuso que la empresa no está obligada, tras prohibir el uso de sus medios (ordenadores, móviles, internet etc...) para fines personales, tanto dentro como fuera del horario de trabajo, a informar de que podrá existir un control de los mismos y la forma en que podrá llevarse a cabo, pudiendo instalar sistemas que no se limiten a controlar genéricamente tiempo y páginas visitadas por los trabajadores sino que permitan observar lo que estos ven y la captación de pantallas para su posterior visualización.

5.2.- PREVENCIÓN VS. DETECCIÓN DEL MAL USO DE INTERNET.

Al considerar la cuestión del control de la utilización de Internet por los trabajadores, el Empresario ha de primar la prevención sobre la detección del mal uso. Así, la política de la empresa 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.

5.3.- CONTENIDO MÍNIMO RECOMENDADO EN UNA POLÍTICA DE EMPRESA SOBRE CONTROL Y ACCESO A INTERNET.

El control por parte del Empleador debe de reflejar en su política de empresa, al menos, los puntos siguientes:

- 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.

- Deberá informarse a los trabajadores de los sistemas instalados para impedir el acceso a algunos sitios o para detectar una posible utilización abusiva.

- Deberá 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.

- 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.

- 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.

En definitiva, para que la empresa pueda proceder al control del uso del ordenador por parte del trabajador, sin vulnerar su "expectativa de confidencialidad" y, por ende, su dignidad, no sólo ha de haber establecido instrucciones para su uso, sino también haber advertido de los controles que van a aplicarse. No es suficiente con que el Empresario establezca válidamente una prohibición absoluta de uso de medios de la empresa (ordenadores, móviles, internet, etc...) para fines propios, tanto dentro como fuera del horario de trabajo sino que, además, ha de advertir de los controles que se van a utilizar para conocer el uso del ordenador por parte del trabajador.

6.- CONTROL DEL CORREO ELECTRÓNICO.

6.1.- LEGITIMACIÓN.

En el control y vigilancia del correo electrónico, a diferencia del control o monitoreo de la navegación por Internet, añade como límite al Empresario, no sólo la intimidad sino también el secreto del contenido de las comunicaciones. De este modo, *a priori*, se podría tener un acceso a los *logs*, esto es, datos de localización y tráfico, sin mayor identificación de remitente y destinatario. En caso de acceder al contenido de la comunicación electrónica, pudiera vulnerarse el secreto de la misma, más cuando no es de índole laboral.

Para ello, 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.

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 del artículo 29 [2]ha opinado a este respecto lo siguiente: *"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.

6.2.- CORREO ELECTRÓNICO ¿HERRAMIENTA DE TRABAJO O INSTRUMENTO DE PRODUCCIÓN?.

La jurisprudencia ha tenido que discernir si debía considerar el correo electrónico como una herramienta de trabajo o un instrumento productivo propiedad del Empresario.

[2] El Grupo de Trabajo del artículo 29 es un grupo consultivo independiente compuesto por representantes de las autoridades de los Estados Miembros, encargados 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.

- Si se considera como una herramienta de trabajo, se aplicaría por analogía lo establecido en el artículo 18.1 del Estatuto de los Trabajadores para su registro, de una forma similar a, por ejemplo, las reglas del registro de taquillas.

- Sin embargo, la doctrina jurisprudencial considera que es un instrumento o medio de producción del que es titular el Empresario, concretamente en **Sentencia de 26 de septiembre de 2007 del Tribunal Supremo**, que, en relación al correo electrónico apunta se *"facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia del Empresario"*.

Esta facultad reconocida al Empresario, de supervisión de las comunicaciones electrónicas del trabajador queda, por tanto, enmarcada en lo dispuesto en el artículo 20.3 del Estatuto de los Trabajadores, como un medio de producción sobre el que *"el Empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso".*

Por tanto, debe comunicarse a los trabajadores que se ha puesto a disposición instrumentos de producción, cuya titularidad pertenece a la entidad y única y exclusivamente debieran utilizarse para menesteres laborales.

7.- TELEFONIA IP.

Las consideraciones hechas para el correo electrónico se tendrán también para el control o monitoreo de las llamadas telefónicas por Internet, esto es, voz IP. El Empresario o Empleador deberá informar previamente a los trabajadores acerca del control y vigilancia del medio, sin vulnerar (acceder) al contenido de la comunicación. Podrá observar la relación de *logs*, datos de localización y tráfico, de la comunicación.

Asimismo, la generalización de este tipo de medios no sólo en el ámbito profesional, sino también en el privado, ha generado una mayor tolerancia por parte del Empresario. A ello se suma el hecho de que los horarios laborales tienden a flexibilizarse, y cuando ello ocurre, con frecuencia no es posible un control basado en el horario laboral. Además, se puede percibir como injustificado prohibir el uso de unas herramientas que facilitan una mejor conciliación de la vida personal y laboral cuando el trabajador ha incrementado sustancialmente su disponibilidad a través precisamente de dispositivos móviles o accesos remotos a la red de empresa.

8.- HISTORIAL DE ACCESOS DE UN USUARIO A LA RED. DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

Con el historial de accesos de un Usuario a la Red (Internet) se puede obtener un perfil psicológico y sexual del solicitante.

Ante esto, a continuación, se analizará hasta qué grado puede considerarse estos datos del historial de accesos, como datos de carácter personal del Usuario.

De acuerdo con el artículo 5.f) RDLOPD, se define como **"Datos de carácter personal"** cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Para saber cuando la información es considerada de carácter identificable de una persona física, tendremos que estar al concepto recogido en el artículo 5.2 RDLOPD, **"Persona identificable"** es toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

Para el caso que nos atañe, la información que pueden arrojar los datos de localización o tráfico no es *per se* de carácter personal. Ahora bien, desde el momento que puede relacionarse o asociarse esta información a un individuo (Usuario), el cual puede ser identificado sin utilizar tiempo o medio desproporcionados, se convierte en datos de carácter personal.

Por ejemplo, si un Usuario desde su puesto de trabajo accede a páginas de cierto contenido pornográfico y/o efectúa llamadas IP a un número de teléfono de tarificación adicional [803: contactos y eróticos. Servicios para adultos], podría inferirse o deducirse cierta orientación, filia/s o parafilia/s sexual/es; estaríamos ante información o datos de carácter personal de carácter sensible, la cual deberá salvaguardarse con mayor celo.

Si del resultado de la búsqueda se arroja o desprende este tipo de información de carácter sexual del Usuario, como cualquier otro tipo de información de carácter personal, debe guardarse secreto profesional (artículo 10 LOPD), por parte del personal del Depto. Área de Sistemas aun después de finalizar su relación funcionario o laboral con la Organización.

Si bien, la misma debe conservarse a los efectos, por ejemplo, de amonestar o llevar a cabo otro tipo de actuación sobre el Usuario (Empleado), deberá estar en lugar, lógico y/o físico, con las medidas de seguridad, técnicas y organizativas, de máximo nivel (artículo 81.3 RDLOPD).

Esta información se mantendrá en estado de bloqueo para su puesto a disposición, en su caso, de los Juzgados o Tribunales, u otra autoridad competente. Y, se conservará mientras esté en vigor o en liza la relación y responsabilidad del Usuario en cuestión. Después de realizadas las acciones. Todo esto, de conformidad con el artículo 8.6 RDLOPD:

"Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento "

Más, de conformidad con el artículo 8.4 RDLOPD*, "Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido ".*

9.- CÁMARAS PARA EL CONTROL EMPRESARIAL.

Como se ha mencionado, el Estatuto de los Trabajadores faculta al Empresario para adoptar las medidas que estime más oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, que deberán guardar la consideración debida a la dignidad humana y tener en cuenta la capacidad real de los trabajadores con discapacidad.

La aplicación del artículo 20.3 ET, ya mencionado, no legitima por sí solo el tratamiento de las imágenes, si bien este será posible, aún sin contar con el consentimiento del afectado en caso de que el trabajador haya sido debidamente informado de la existencia de esta medida, debiendo además ser claro que, conforme a lo exigido por el artículo 4.2 LOPD, los datos no podrán ser utilizados para fines distintos.

A raíz de ello la AEPD ha elaborado unas "FICHAS PRÁCTICAS DE VIDEOVIGILANCIA: VI. CÁMARAS PARA EL CONTROL EMPRESARIAL" y ofrece un modelo de inscripción de ficheros de videovigilancia, mediante su sistema NOTA.

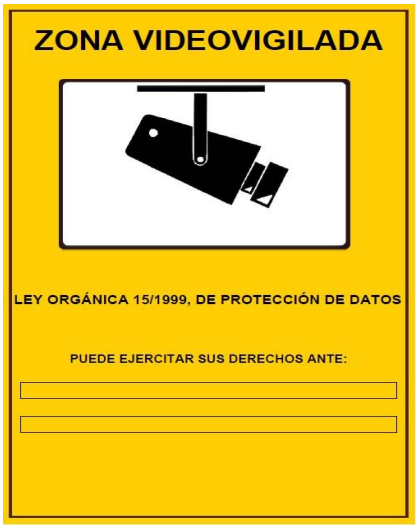
9.1.- DEBER DE INFORMACIÓN.

Esta obligación de informar se acometerá del siguiente modo:

1. Colocación carteles "Zona Videovigilada"
2. Comunicación de la medida a trabajadores y órganos de representación.

1. Colocación carteles "Zona Videovigilada"

De conformidad con el artículo 3 de la Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, deberá informarse acerca de la colocación de cámaras mediante carteles:



La colocación de carteles advirtiendo de que está en una "Zona Videovigilada". Estos carteles estarán en lugar suficientemente visible. El cartel recogerá la identidad del responsable de la instalación, y ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos.

De acuerdo con los Informes 0084/2007 y 0006/2009 de la Agencia Española de Protección de Datos, se resuelven varias cuestiones en cuanto a la interpretación y aplicación de la Instrucción.

Entre otras cuestiones, a continuación se relacionan diversos aspectos tratados por la AEPD:

- No existe ningún criterio de la Agencia, en el que se refiere a dimensiones, debiendo ser un cartel informativo acorde con el espacio en el que se vaya a ubicar, dado que no es equiparable colocar el cartel informativo en un autobús o en la entrada de un edificio.
- Respecto a la ubicación del cartel informativo, no es necesario que se coloque debajo de la cámara, será suficiente conforme lo dispuesto en el Artículo 3 a) de la citada Instrucción, colocar el distintivo informativo en lugar suficientemente visible, tanto en espacios abiertos como cerrados. Por tanto, resultaría aconsejable que si tratándose de un edificio sometido a video vigilancia, en la entrada del mismo, se ubicara el cartel informativo.
- No pueden conservarse las imágenes grabadas por un tiempo superior a un mes [Artículo 6 Instrucción 1/2006 *<< Los datos serán cancelados en el plazo máximo de un mes desde su captación>>*]

2. Comunicación de la medida a trabajadores y órganos de representación.

Por supuesto, sobre la adopción de esta medida de vigilancia habrá de informarse de manera personalizada a los trabajadores y a los órganos de representación (Sindicatos, Delegados de personal, Comité de Empresa), por cualquier medio que garantice la recepción de la información. Nunca deberá efectuarse a direcciones particulares de los trabajadores ni a través de llamadas a sus móviles privados.

Nota.- En cualquier caso se recomienda que todos los trabajadores afectados firmen las normas de uso y control de las TIC.

9.2.- INSTALACIÓN DE LAS CÁMARAS.

Las cámaras sólo captarán imágenes de los espacios indispensables para el control laboral:

- En ningún caso se ubicarán en zonas de vestuarios, baños y espacios de descanso de los trabajadores.
- Si se utilizan cámaras orientables y/o con zoom, será necesaria la instalación de máscaras de privacidad para evitar captar imágenes de la vía pública, terrenos, viviendas o cualquier otro espacio ajeno.
- No se registrarán conversaciones privadas.