Se recomienda leer los materiales conjuntamente con el cuestionario correspondiente al tema para fijar la atención en las cuestiones de interés y hacer una lectura comprensiva.

También, materiales “Derecho y TICs”, Máster Oficial Sistemas y Servicios Sociedad de la Información www.uv.es/mastic

TEMA XII

XII. PRIVACIDAD Y PROTECCIÓN DE DATOS III. DATOS DE TRÁFICO Y CONTROL LABORAL

1. DATOS DE TRÁFICO 2
Derechos fundamentales en juego en materia de datos de tráfico: Tribunal Constitucional y AGPD *2*
LEY 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones *3*
LECRIM, art. 579 y secreto de las comunicaciones *10*
Doctrina básica Tribunal Constitucional para requisitos intervención de las comunicaciones telefónicas *11*
Intervención de las comunicaciones en la LGT *11*
2. EMPLEO Y CONTROL LABORAL DEL CORREO ELECTRÓNICO 13
Grupo del artículo 29, recomendaciones *13*
Sentencia unificación de doctrina, control por el empresario del uso de internet y el correo electrónico del trabajador *15*
Correo electrónico y uso sindical: La importante sentencia del Tribunal Constitucional en el caso CCOO vs. BBVA y el uso sindical del correo electrónico del empresario *23*

XII. PRIVACIDAD Y PROTECCIÓN DE DATOS III. DATOS DE TRÁFICO Y CONTROL LABORAL

1. Datos de tráfico

Derechos fundamentales en juego en materia de datos de tráfico: Tribunal Constitucional y AGPD

Tenga en cuenta el matiz del Tribunal Constitucional en sentencias 70/2002 o 56/2003. Crees que los datos de tráfico de la comunicación ya finalizada están protegidos por el artículo 18. 3 del secreto de las comunicaciones o "sólo" por el derecho a la intimidad del artículo 18. 1º y, en su caso por el derecho a la protección de datos personales (art. 18. 4º).

En efecto, en una línea jurisprudencial que recordaba el Tribunal Constitucional en su Sentencia 56/2003, se ha venido afirmando que "el concepto de "secreto", que aparece en el artículo 18.3, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales"; línea emprendida ya en la Sentencia 114/1984, de 29 de noviembre, que se hacía eco de la Sentencia del TEDH de 2 de agosto de 1984, caso Malone, en la que se reconoce expresamente la posibilidad de que el artículo 8 del CEDH pueda resultar violado por el empleo de un artificio técnico que, como el recuento ("comptage"), permite registrar cuáles han sido los números telefónicos marcados en un determinado aparato, aunque no el contenido de la comunicación misma.

En todo caso, debe notarse que, en su Sentencia 70/2002 precisó el Tribunal Constitucional que "la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos", de modo que la protección de este derecho alcanza a las interferencias habidas o producidas en el proceso de comunicación (precisión que también se recoge en la STC 56/2003).

Cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad. Informe 213/2004

"Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos."

LEY 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

I

..

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

…

II

…

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

La Ley enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos, que, se repite, en ningún caso revelarán el contenido de la comunicación, son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter general, de doce meses desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

El Capítulo III, al referirse al régimen sancionador, remite, en cuanto a los incumplimientos de las obligaciones de conservación y protección y seguridad de los datos de carácter personal, a la regulación contenida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Por otro lado, los incumplimientos de la obligación de puesta a disposición de los agentes facultados, en la medida en que las solicitudes estarán siempre amparadas por orden judicial, constituirían la correspondiente infracción penal.

…

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto de la Ley.

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. Sujetos obligados.

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. Datos objeto de conservación.

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.

ii) Nombre y dirección del abonado o usuario registrado.

2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.

ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.

iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.

ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.

ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.

2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.

ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).

2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.

2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.

ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.

iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.

iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

CAPÍTULO II

Conservación y cesión de datos

Artículo 4. Obligación de conservar datos.

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo

dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

NOTA: TÉNGASE EN CUENTA EL ARTÍCULO AL QUE SE HACE REFERENCIA, EN CONCRETO:
"38. 3.º En particular, los abonados a los servicios de comunicaciones electrónicas tendrán los siguientes derechos:
A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnacion de la factura del servicio o para que el operador pueda exigir su pago.
A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello."

RECUÉRDESE QUE ESTA OBLIGACIÓN PESA SOBRE:
"28. Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o de las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos; quedan excluidos, asimismo, los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas."

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. Período de conservación de los datos.

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un

máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

NOTA: "DICHO ARTÍCULO LOPD dice:

"Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado."

Artículo 6. Normas generales sobre cesión de datos.

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial.

2. La cesión de la información se efectuará únicamente a los agentes facultados.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Artículo 7. Procedimiento de cesión de datos.

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden.

Artículo 8. Protección y seguridad de los datos.

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Artículo 9. Excepciones a los derechos de acceso y cancelación.

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Infracciones y sanciones

Artículo 10. Régimen aplicable al incumplimiento de obligaciones contempladas en esta Ley.

El incumplimiento de las obligaciones previstas en esta Ley se sancionará de acuerdo con lo dispuesto en la Ley 32/2003, de 3 de noviembre, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

Disposición adicional única. Servicios de telefonía mediante tarjetas de prepago.

1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.
La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.

2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.

3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

…

LECRIM, art. 579 y secreto de las comunicaciones

Artículo 579.
1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.
2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

3. De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación le las comunicaciones postales, telegráficas o telefónicas de las personas obre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.
4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos oras desde que fue ordenada la observación.

Doctrina básica Tribunal Constitucional para requisitos intervención de las comunicaciones telefónicas

"la intervención de las comunicaciones telefónicas sólo puede considerarse constitucionalmente legítima cuando . se ejecuta con observancia del principio de proporcionalidad; es decir, cuando su autorización se dirige a alcanzar un fin constitucionalmente legítimo, como acontece en los casos en que se adopta para la investigación de la comisión de delitos calificables de graves y es idónea e imprescindible para la determinación de hechos relevantes para la misma (SSTC 49/1999, de 5 de abril, FJ 8; 299/2000, de 11 de diciembre, FJ 2). La comprobación de la proporcionalidad de la medida ha de efectuarse analizando las circunstancias concurrentes en el momento de su adopción (SSTC 126/2000, de 16 de mayo, FJ 8; y 299/2000, de 11 de diciembre, FJ 2)" (STC 184/2003, de 23 de octubre; FJ 9). Faltará en todo caso el carácter necesario de la intervención cuando la misma constituya "la primera medida de investigación penal, pues el juicio de necesidad, esto es, el carácter imprescindible de la medida como parte esencial del juicio de proporcionalidad, requiere ponderar la eventual existencia de medios alternativos de investigación" (STC 184/2003, FJ 9).

Intervención de las comunicaciones en la LGT

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. Secreto de las comunicaciones.

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del

Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que

intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones.

Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios Internet.

f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.

10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.»

2. Empleo y control laboral del correo electrónico

Grupo del artículo 29, recomendaciones

Grupo de Trabajo creado como órgano consultivo de la Unión Europea en materia de protección de datos y vida privada. Dicho Grupo, publicó en fecha 29 de mayo de 2002 un Documento proporcionando orientación sobre el contenido mínimo de las

directrices de las empresas en relación con la utilización del correo electrónico e Internet.

El documento de trabajo indica que para que una actividad de control empresarial sea legal y se justifique, deben respetarse una serie de principios:

a) 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.

b) 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.

c) 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. 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.

d) 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.

e) 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. 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).

f) Exactitud y conservación de los datos. Este principio requiere que todos los datos legítimamente almacenados por un empleador (después de tener en cuenta todos los demás principios) 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.

g) 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 "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 para la Protección de los Derechos Humanos y Libertades Fundamentales, que establece que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". En este sentido, el Grupo de Trabajo señala 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 sólo podrá justificarse en circunstancias muy limitadas y no podrá justificarse en circunstancias normales ya que acceder a este tipo de datos no es necesario para satisfacer un interés legítimo del empleador, debiendo prevalecer por el contrario el derecho fundamental al secreto de correspondencia.

Sentencia unificación de doctrina, control por el empresario del uso de internet y el correo electrónico del trabajador

Estatuto de los Trabajadores
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.

3. 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.

STS, Sala ***de lo Social, de 26 de septiembre de 2007 Recurso Num.: /*966/2006, *casación de sentencia del*** T.S.J.GALICIA SOCIAL, ***Ponente*** Aurelio Desdentado Bonete

Despido disciplinario por uso incorrecto de ordenador. Contradicción en cuanto a las garantías aplicables al control por parte de la empresa de ese uso. No se aplica el régimen del artículo 18 del Estatuto de los Trabajadores, pero la empresa debe determinar previamente que el uso está controlado.

hechos probados: … El actor prestaba sus servicios en un despacho sin llave, en el que disponía de un ordenador, carente de clave de acceso, y conectado a la red de la empresa, que a su vez dispone de ADSL. El ordenador tiene antivirus propio. ----3º.- El día 11 de mayo pasado, un técnico de la empresa SOFT HARD EQUIPOS Y PROGRAMACION S.L. fue requerido para comprobar los fallos en un ordenador que la empresa señaló como del actor, comprobación, que según dicho técnico, D. Alejandro San Millán Padrón se llevó a cabo a las cinco de la tarde del citado día. En dicha comprobación se constató la existencia de virus informáticos, como consecuencia de la navegación por páginas poco seguras de internet. A presencia del Administrador de la empresa comprueba la existencia en la carpeta de archivos temporales de antiguos accesos a páginas pornográficas, que procede a almacenar en un dispositivo USB y a su impresión en papel. Dichos archivos se corresponden con imágenes y videos de carácter pornográfico. El dispositivo USB es llevado a un notario para su custodia, así como la relación de páginas que en el mismo se contiene. Las operaciones llevadas a cabo en el ordenador se hicieron sin la presencia del actor ni de representantes sindicales ni trabajador alguno. ----4º.- El ordenador fue retirado de la empresa para su reparación y el 30 de mayo, una vez devuelto, se procede a la misma operación esta vez a presencia de dos delegados de personal, grabándose otro USB con las páginas almacenadas en el archivo temporal, y depositándole ante el notario, con el listado de paginas que se señalan. Tampoco estaba el actor presente.

…

El 18 de mayo de 2.004…se acuerda el cese y separación como Administradora Solidaria de Dº Manuela por deslealtad y riesgo ejerciendo la acción social de responsabilidad contra ella. Los motivos son la falta de preparación e idoneidad de los contratos suscritos con la actora y D. José Antonio Pardo Cuerdo, así como haberles otorgado poderes. Estos poderes fueron revocados por el Administrador Sr. Vilela en sendas escrituras de 28 de mayo y 27 de abril de 2.004.

El fallo de dicha sentencia [apelada] es del tenor literal siguiente: "Que desestimando la excepción de incompetencia de jurisdicción y estimando la demanda formulada por D. JUAN ANTONIO PARDO CUERVO declaro la improcedencia de su despido y sin opción por la indemnización para la empresa CORUÑESA DE ETIQUETAS S.L. a salvo lo dispuesto en el artículo 11.3 del Real Decreto 1382/85 la condena a abonarle la cantidad de 90.151€ en concepto de indemnización sin derecho a salarios de tramitación".

…

FUNDAMENTOS DE DERECHO

PRIMERO.- En los hechos probados de la sentencia de instancia consta que el actor, Director General de la empresa demandada, prestaba servicios en un despacho sin llave, en el que disponía de un ordenador, carente de clave de acceso y conectado a la red de la empresa que dispone de ADSL. Consta también que un técnico de una empresa de informática fue requerido el 11 de mayo para comprobar los fallos de un ordenador que "la empresa señaló como del actor". En la comprobación se detectó la existencia de virus informáticos, como consecuencia de "la navegación por páginas poco seguras de Internet". En presencia del administrador de la empresa se comprobó la existencia en la carpeta de archivos temporales de "antiguos accesos a páginas pornográficas", que se almacenaron en un dispositivo de USB, que se entregó a un notario. La sentencia precisa que "las operaciones llevadas a cabo en el ordenador se hicieron sin la presencia del actor, de representantes de los trabajadores ni de ningún trabajador de la empresa". El ordenador fue retirado de la empresa para su reparación y, una vez devuelto, el 30 de mayo se procedió a realizar la misma operación con la presencia de delegados de personal. La sentencia recurrida confirma la decisión de instancia que ha considerado que no es válida la prueba de la empresa porque ha sido obtenida mediante un registro de un efecto personal que no cumple las exigencias del artículo 18 del Estatuto de los Trabajadores.

…

estamos ante un problema sobre la determinación de los límites del control empresarial sobre un ámbito que, aunque vinculado al trabajo, puede afectar a la intimidad del trabajador.

SEGUNDO.- Establecida la contradicción en los términos a que se ha hecho referencia, hay que entrar en el examen de la infracción que se denuncia del artículo 18 del Estatuto de los Trabajadores en relación con el artículo 90.1 de la Ley de Procedimiento Laboral y con el artículo 18 de la Constitución. Como ya se ha anticipado, la sentencia recurrida funda su decisión en que en la obtención del medio de prueba, a partir del cual podría acreditarse la conducta imputada por la empresa para justificar el despido, no se han respetado las exigencias del artículo 18 del Estatuto de los Trabajadores, ya que: 1º) no se demuestra que fuera necesario llevar a cabo en ese momento y sin la presencia del trabajador el examen del ordenador o al menos la continuación del examen una vez que aparecieron los archivos temporales, 2º) no consta que todo el proceso de control se realizara en el lugar y en el tiempo de trabajo, pues el ordenador fue retirado para su reparación; 3º) tampoco se respetó la dignidad del trabajador al haber realizado el control sin su presencia y 4º) el control se efectuó sin la presencia de un representante de los trabajadores.

La cuestión debatida se centra, por tanto, en determinar si las condiciones que el artículo 18 del Estatuto de los Trabajadores establece para el registro de la persona del trabajador, su taquilla y sus efectos personales se aplican también al control empresarial sobre el uso por parte del trabajador de los ordenadores facilitados por la empresa. Pero el problema es más amplio, porque, en realidad, lo que plantea el recurso, desde la perspectiva de ilicitud de la prueba obtenida vulnerando los derechos fundamentales (artículo 91.1 de la Ley de Procedimiento Laboral), es la compatibilidad de ese control empresarial con el derecho del trabajador a su intimidad personal (artículo 18.1 de la Constitución) o incluso con el derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución Española), si se tratara del control del correo electrónico. El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos establece también que toda persona tiene derecho al respeto de la vida privada y familiar y prohibe la injerencia que no esté prevista en la ley y que no se justifique por razones de seguridad, bienestar económico, defensa del orden, prevención de las infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás. El derecho a la intimidad, según la doctrina del Tribunal Constitucional, supone "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" y ese ámbito ha de respetarse también en el marco de las relaciones laborales, en las que "es factible en ocasiones acceder a informaciones atinentes a la vida íntima y familiar del trabajador que pueden ser lesivas para el derecho a la intimidad" (SSTC 142/1993, 98/2000 y 186/2000). De ahí que determinadas formas de control de la prestación de trabajo pueden resultar incompatibles con ese derecho, porque aunque no se trata de un derecho absoluto y puede ceder, por tanto, ante "intereses constitucionalmente relevantes", para ello es preciso que las limitaciones impuestas sean necesarias para lograr un fin legítimo y sean también proporcionadas para alcanzarlo y respetuosas con el contenido esencial del derecho. En el caso del uso por el trabajador de los medios informáticos facilitados por la empresa pueden producirse conflictos que afectan a la intimidad de los trabajadores, tanto en el correo electrónico, en el que la implicación se extiende también, como ya se ha dicho, al secreto de las comunicaciones, como en la denominada "navegación" por Internet y en el acceso a determinados archivos personales del ordenador. Estos conflictos *surgen porque existe una utilización personalizada y no meramente laboral o profesional del medio facilitado por la empresa. Esa utilización personalizada se produce como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador -como sucede también con las conversaciones telefónicas en la empresa- y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa.* Pero, al mismo tiempo, hay que tener en cuenta que se trata de medios que son propiedad de la empresa y que ésta 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, que, como precisa el artículo 20.3 del Estatuto de los Trabajadores, implica que éste "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", aunque ese control debe respetar "la consideración debida" a la "dignidad" del trabajador.

TERCERO.- Estas consideraciones muestran que el artículo 18 del Estatuto de los Trabajadores no es aplicable al control por el empresario de los medios informáticos que se facilitan a los trabajadores para la ejecución de la prestación laboral. El artículo 18 del Estatuto de los Trabajadores establece que "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", añadiendo que en la realización de estos registros "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". *El supuesto de hecho de la norma es completamente distinto del que se produce con el control de los medios informáticos en el trabajo.* El artículo 18 está atribuyendo al empresario un control que excede del que deriva de su posición en el contrato de trabajo y que, por tanto, queda fuera del marco del artículo 20 del Estatuto de los Trabajadores. *En los registros el empresario actúa, de forma exorbitante y excepcional*, fuera del marco contractual de los poderes que le concede el artículo 20 del Estatuto de los Trabajadores y, en realidad, como ha señalado la doctrina científica, desempeña -no sin problemas de cobertura -una función de "policía privada" o de "policía empresarial" que la ley vincula a la defensa de su patrimonio o del patrimonio de otros trabajadores de la empresa. El régimen de registros del artículo 18 del Estatuto de los Trabajadores *aparece así como una excepción al régimen ordinario que regula la Ley de Enjuiciamiento Criminal (artículo 545 y siguientes).* Tanto la persona del trabajador, como sus efectos personales y la taquilla forman parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución del contrato de trabajo al que se extienden los poderes del artículo 20 del Estatuto de los Trabajadores. *Por el contrario, las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario "como propietario o por otro título" y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen.* Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18, pues incluso respecto a *la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que*, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del artículo 20 del Estatuto de los Trabajadores para entrar dentro de la esfera personal del trabajador.

De ahí que los elementos que definen las garantías y los límites del artículo 18 del Estatuto de los Trabajadores, no sean aplicables al control de los medios informáticos. En primer lugar, *la necesidad del control de esos medios no tiene que justificarse por "la protección del patrimonio empresarial y de los demás trabajadores de la empresa"*, porque la legitimidad de ese control deriva del carácter de instrumento de producción del objeto sobre el que recae. *El empresario tiene que controlar el uso del ordenador, porque en él se cumple la prestación laboral y, por tanto, ha de comprobar si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales. Tiene que controlar también los contenidos y resultados de esa prestación.* Así, nuestra sentencia de 5 de

diciembre de 2003, sobre el *telemarketing* telefónico, aceptó la legalidad de un control empresarial consistente en la audición y grabación aleatorias de las conversaciones telefónicas entre los trabajadores y los clientes «para corregir los defectos de técnica comercial y disponer lo necesario para ello", razonando que tal control tiene "como único objeto ...la actividad laboral del trabajador", pues el teléfono controlado se ha puesto a disposición de los trabajadores como herramienta de trabajo para que lleven a cabo sus funciones de "telemarketing" y los trabajadores conocen que ese teléfono lo tienen sólo para trabajar y conocen igualmente que puede ser intervenido por la empresa. El control de los ordenadores se justifica también por la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores (pedidos, relaciones con clientes ..), por la protección del sistema informático de la empresa, que puede ser afectado negativamente por determinados usos, y por la prevención de responsabilidades que para la empresa pudieran derivar también algunas formas ilícitas de uso frente a terceros. En realidad, el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 del Estatuto de los Trabajadores, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 del Estatuto de los Trabajadores.

En segundo lugar, la exigencia de respetar en el control la dignidad humana del trabajador no es requisito específico de los registros del artículo 18, pues esta exigencia es general para todas las formas de control empresarial, como se advierte a partir de la propia redacción del artículo 20.3 del Estatuto de los Trabajadores. En todo caso, hay que aclarar que el hecho de que el trabajador no esté presente en el control no es en sí mismo un elemento que pueda considerarse contrario a su dignidad.

En tercer lugar, la exigencia de que el registro se practique en el centro de trabajo y en las horas de trabajo tiene sentido en el marco del artículo 18, que se refiere a facultades empresariales que, por su carácter excepcional, no pueden ejercitarse fuera del ámbito de la empresa. Es claro que el empresario no puede registrar al trabajador o sus efectos personales fuera del centro de trabajo y del tiempo de trabajo, pues en ese caso sus facultades de policía privada o de autotutela tendrían un alcance completamente desproporcionado. Lo mismo puede decirse del registro de la taquilla, aunque en este caso la exigencia de que se practique en horas de trabajo tiene por objeto permitir la presencia del trabajador y de sus representantes. En todo caso hay que aclarar que las exigencias de tiempo y lugar del artículo 18 del Estatuto de los Trabajadores no tienen por objeto preservar la intimidad del trabajador registrado; su función es otra: limitar una facultad empresarial excepcional y reducirla al ámbito de la empresa y del tiempo de trabajo. *Esto no sucede en el caso del control de un instrumento de trabajo del que es titular el propio empresario.*

Por último, la presencia de un representante de los trabajadores o de un trabajador de la empresa tampoco se relaciona con la protección de la intimidad del trabajador registrado; es más bien, como sucede con lo que establece el artículo 569 Ley de Enjuiciamiento Criminal para intervenciones similares, una garantía de la objetividad y de la eficacia de la prueba. Esa exigencia no puede, por tanto, aplicarse al control normal por el empresario de los medios de producción, con independencia de que para lograr que la prueba de los resultados del control sea eficaz tenga que recurrirse a la prueba testifical o pericial sobre el control mismo.

No cabe, por tanto, aplicación directa del artículo 18 del Estatuto de los Trabajadores al control del uso del ordenador por los trabajadores, ni tampoco su aplicación analógica, porque no hay ni semejanza de los supuestos, ni identidad de razón en las regulaciones (artículo 4.1 del Código Civil).

CUARTO.- El control del uso del ordenador facilitado al trabajador por el empresario no se regula por el artículo 18 del Estatuto de los Trabajadores, sino por el artículo 20.3 del Estatuto de los Trabajadores y a este precepto hay que estar con las matizaciones que a continuación han de realizarse. La primera se refiere a los límites de ese control y en esta materia el propio precepto citado remite a un ejercicio de las facultades de vigilancia y control que guarde "en su adopción y aplicación la consideración debida" a la dignidad del trabajador, lo que también remite al respeto a la intimidad en los términos a los que ya se ha hecho referencia al examinar las sentencias del Tribunal Constitucional 98 y 186/2000. En este punto es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. ***Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.*** De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos.

La segunda precisión o matización se refiere al alcance de la protección de la intimidad, que es compatible, con el control lícito al que se ha hecho referencia. Es claro que las comunicaciones telefónicas y el correo electrónico están incluidos en este ámbito con la protección adicional que deriva de la garantía constitucional del secreto de las comunicaciones. La garantía de la intimidad también se extiende a los archivos personales del trabajador que se encuentran en el ordenador. La aplicación de la garantía podría ser más discutible en el presente caso, pues no se trata de comunicaciones, ni de archivos personales, sino de los denominados archivos temporales, que son copias que se guardan automáticamente en el disco duro de los lugares visitados a través de Internet. Se trata más bien de rastros o huellas de la "navegación" en Internet y no de informaciones de carácter personal que se guardan

con carácter reservado. Pero hay que entender que estos archivos también entran, en principio, dentro de la protección de la intimidad, sin perjuicio de lo ya dicho sobre las advertencias de la empresa. Así lo establece la sentencia de 3 de abril de 2007 del Tribunal Europeo de Derechos Humanos cuando señala que están incluidos en la protección del artículo 8 del Convenio Europeo de derechos humanos "la información derivada del seguimiento del uso personal de Internet" y es que esos archivos pueden contener datos sensibles en orden a la intimidad, en la medida que pueden incorporar informaciones reveladores sobre determinados aspectos de la vida privada (ideología, orientación sexual, aficiones personales, etc). Tampoco es obstáculo para la protección de la intimidad el que el ordenador no tuviera clave de acceso. Este dato -unido a la localización del ordenador en un despacho sin llave- no supone por sí mismo una aceptación por parte del trabajador de un acceso abierto a la información contenida en su ordenador, aunque ello suscite otros problema en los que en este recurso no cabe entrar sobre la dificultad de la atribución de la autoría al demandante.

QUINTO.- A partir de las consideraciones anteriores la pretensión impugnatoria debe ser desestimada, pues, de acuerdo con una reiterada doctrina de esta Sala, el recurso se da contra el fallo y no contra los fundamentos jurídicos de la sentencia recurrida y este fallo es correcto, pues la empresa no podía recoger la información obrante en los archivos temporales y utilizarla con la finalidad que lo ha hecho. Esa actuación en el presente caso ha supuesto una vulneración de su derecho a la intimidad. *En efecto, en el supuesto de que efectivamente los archivos mencionados registraran la actividad del actor, la medida adoptada por la empresa, sin previa advertencia sobre el uso y el control del ordenador, supone una lesión a su intimidad en los términos a que se ha hecho referencia en los anteriores fundamentos. Es cierto que la entrada inicial en el ordenador puede justificarse por la existencia de un virus, pero la actuación empresarial no se detiene en las tareas de detección y reparación*, sino que, como dice con acierto la sentencia recurrida, en lugar de limitarse al control y eliminación del virus, "se siguió con el examen del ordenador" para entrar y apoderarse de un archivo cuyo examen o control no puede considerarse que fuera necesario para realizar la reparación interesada. De esta forma, no cabe entender que estemos ante lo que en el ámbito penal se califica como un "hallazgo casual" (sentencias de 20 de septiembre, 20 de noviembre y 1 de diciembre de 2.006), pues se ha ido más allá de lo que la entrada regular para la reparación justificaba.

El recurso debe, por tanto, desestimarse con las consecuencias que de ello se derivan en orden a la imposición de las costas a la empresa recurrente, con pérdida del depósito constituido para recurrir y manteniéndose el aval en garantía del cumplimiento de la condena.

Por lo expuesto, en nombre de S. M. El Rey y por la autoridad conferida por el pueblo español.

F A L L A M O S

Desestimamos el recurso de casación para la unificación de doctrina interpuesto por la empresa CORUÑESA DE ETIQUETAS S.L., contra la sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Galicia, de 25 de enero de 2.006, en el recurso de suplicación nº 5844/05, interpuesto frente a la sentencia dictada el 30 de septiembre de 2.005 por el Juzgado de lo Social nº 3 de A Coruña, en los autos nº 521/05, seguidos a instancia de D. JUAN ANTONIO PARDO CUERDO contra dicha

recurrente, sobre despido. Decretamos la pérdida del depósito constituido para recurrir, manteniéndose el aval como garantía del cumplimiento de la condena. Condenamos a la empresa recurrente al abono de los honorarios del Letrado de la parte recurrida en la cuantía que, dentro de los límites legales, fijará la Sala si a ello hubiera lugar.

Correo electrónico y uso sindical: La importante sentencia del Tribunal Constitucional en el caso CCOO vs. BBVA y el uso sindical del correo electrónico del empresario

En la sentencia 281/2005, de 7 de noviembre, el Tribunal Constitucional afronta directamente la cuestión del uso sindical de los medios electrónicos y tecnológicos de la empresa.

Desde el día 2 de febrero de 1999 el sindicato CCOO enviaba por correo electrónico, desde un servidor externo (comfia.net[1]) y a través del servidor interno del grupo BBVA, mensajes de información sindical a sus afiliados y trabajadores de este banco, sin su oposición. Sin embargo, el 13 de febrero de 2000 envió nuevos mensajes que fueron rechazados por el servidor de la empresa, lo que también ocurrió en varias ocasiones más ese mes y en noviembre de 2000. Este rechazo fue motivado por la avalancha de correos masivos procedentes de la dirección comfia.net. Ante el desmesurado tamaño de las colas de espera, el grupo BBVA decidió filtrar la entrada desde aquella dirección, siendo rechazados los mensajes, con notificación al remitente. El 26 de septiembre de 2000 la empresa dictó normas de actuación para el uso racional del correo electrónico. Entre las "Prácticas a evitar" se señalaba la posibilidad de sanción por remisión de correos ajenos a la finalidades laborales[2]. Frente al Tribunal Supremo, en su sentencia 281/2005, de 7 de noviembre, el Tribunal Constitucional estima el amparo y reconoce con cierta precisión el

[1] Comfia se corresponde con Federación de Servicios Financieros y Administrativos de las Comisiones Obreras.

[2] Se decía: "El correo electrónico es una herramienta de productividad que el Grupo pone a disposición de sus empleados, para el desarrollo de las funciones que les tiene encomendadas. Los usos ajenos a éstos fines son por tanto considerados inapropiados y en el límite podrían configurar falta laboral. En particular la remisión a uno o varios usuarios de correos no solicitados, especialmente si esto se hace de forma masiva (actividad conocida como *spam*) es una práctica rechazable, y, dependiendo de las circunstancias que concurran, puede llegar a ser perseguible". Así las cosas, no era expresa la prohibición del uso sindical, pero sí implícita.

derecho de uso de los medios tecnológicos de los que ya dispone la empresa para la información sindical.

En la sentencia se recuerda que el contenido de la libertad sindical incluye también el de "desplegar los medios de acción necesarios para que puedan cumplir las funciones que constitucionalmente les corresponden [a los sindicatos] (por todas, SSTC 94/1995, de 19 de junio, FJ 2; 308/2000, de 18 de diciembre, FJ 6; 185/2003, de 27 de octubre, FJ 6, y 198/2004, de 15 de noviembre, FJ 5)." (FJ 3º). Como en ocasiones anteriores, se señala que "la información sindical forma parte del contenido esencial del derecho fundamental, que el sindicato puede hacerla efectiva a través de los cauces previstos en la ley y también por medio de otros que libremente adopte siempre que respete la normalidad productiva, y que el empresario tiene que asumir ciertas cargas tasadas en la ley y dirigidas a hacer efectivo el hecho sindical informativo."

Para fundamentar la sentencia, se discierne entre el contenido esencial del derecho, los derechos y facultades adicionales fijados por regulación de desarrollo[3] y los derechos de concesión unilateral del empresario[4]. La vulneración –con motivación antisindical- incluso de estos últimos derechos puede llegar a suponer una lesión de la libertad sindical.

En el caso del uso del correo electrónico, se señala que no hay obligación de base legal por lo que las empresas "no están obligadas a dotarse de esa infraestructura informática para uso sindical"[5]. Ahora

---

[3] "[L]os sindicatos pueden ostentar derechos o facultades *adicionales*, atribuidos por normas legales o por convenios colectivos, que se añaden a aquel núcleo mínimo e indisponible de la libertad sindical. […] de creación infraconstitucional y deben ser ejercitados en el marco de su regulación, pudiendo ser alterados o suprimidos por la norma legal o convencional que los establece". (FJ 3º)

[4] "[P]ueden también existir derechos sindicalmente caracterizados que tengan su fuente de asignación en una concesión unilateral del empresario (SSTC 132/2000, de 16 de mayo, y 269/2000, de 13 de noviembre). En estos casos, […] el empresario […] podrá suprimir las mejoras o derechos de esa naturaleza que previamente haya concedido. Pero, no exento control, puesto que voluntad empresarial […] en que no se verifique la supresión con una motivación antisindical (STC 269/2000, de 13 de noviembre, FJ 5)." (FJ 3º).

[5] FJ 5º: "que la obligación del empresario de permitir la comunicación entre el sindicato y los trabajadores mediante la utilización de su sistema interno de correo electrónico no nace de una lectura actualizada de la norma legal del art. 8.2 LOLS".

"Resulta claro que el derecho a contar para uso sindical con un sistema de correo electrónico a costa del empleador no encaja dentro de los límites de dicho precepto, pues sólo podría fundarse en una interpretación extensiva del derecho a un tablón de anuncios, que pasaría a considerarse como un tablón virtual. Una lectura extensiva de ese estilo no encuentra acomodo en nuestra doctrina sobre el contenido adicional de la libertad sindical, según la cual "no corresponde a este Tribunal determinar cuál es la

bien, si la tecnología está implantada en la empresa –hecho constatable-, se centra el debate en "la facultad del empleador de impedir un uso sindical útil para la función representativa en la empresa una vez que el sistema está creado y en funcionamiento" (FJ 6º). Sobre estos términos, el Tribunal señala que la resistencia al uso de las TICs del empresario para la información sindical, necesita "justificación en razones productivas o en la legítima oposición a asumir obligaciones específicas y gravosas no impuestas al empresario" (FJ 7º). Afirma que no se pueden oponer razones de derecho de propiedad del empresario, puesto que la titularidad permanece[6]. Por ello, se consagra la carga del empresario que cuenta con medios informáticos de que los ponga a disposición de los sindicatos para su goce pacífico, sin que unilateralmente pueda privar a los sindicatos de su empleo, con posibilidad de acudir a los tribunales si lo hace[7]. En todo caso, el Tribunal fija las condiciones para ello[8]:

---

interpretación más correcta de tal cuerpo normativo (STC 61/1989), ni resultaría constitucionalmente obligado que estando en juego una garantía legal del derecho fundamental se incline *a priori* por la interpretación aparentemente más beneficiosa para el titular de aquél, sino que basta con constatar si la interpretación llevada a cabo salvaguarda o no suficientemente el contenido del derecho fundamental" (STC 18/2001, de 29 de enero, FJ 2)."

"No cabe entender, consecuentemente, que exista una obligación legal de facilitar la transmisión de información sindical a los trabajadores, afiliados o no, a través de un sistema de correo electrónico con cargo al empleador. Las empresas, dicho en otras palabras, no están obligadas a dotarse de esa infraestructura informática para uso sindical."

6 "No pueden oponerse a esa conclusión los elementos estructurales de la definición misma del derecho a la propiedad privada. Señaladamente porque la propiedad no resulta en ningún modo desatendida por la utilización sindical de ese tipo de instrumentos empresariales, ya que su uso no la modifica. Que dicho uso no supone por sí mismo una ablación de la propiedad lo demuestra simplemente el hecho de que como consecuencia de él no pierde el empresario su titularidad de la herramienta de producción a través de la cual transmite el sindicato su información a los trabajadores." (FJ 7º).

7 "En conclusión, sobre el empresario pesa el deber de mantener al sindicato en el goce pacífico de los instrumentos aptos para su acción sindical siempre que tales medios existan, su utilización no perjudique la finalidad para la que fueron creados por la empresa y se respeten los límites y reglas de uso que a continuación enunciaremos, cuyo cumplimiento deberá examinarse en cada caso. En tales condiciones no puede negarse la puesta a disposición, ni puede unilateralmente privarse a los sindicatos de su empleo, debiendo acudirse al auxilio judicial si con ocasión de su utilización el sindicato llega a incurrir en excesos u ocasionar perjuicios, a fin de que aquéllos sean atajados y éstos, en su caso, compensados." (FJ 7º).

8 "Tales condiciones o restricciones son las siguientes:

a) La comunicación no podrá perturbar la actividad normal de la empresa.

b) Tratándose del empleo de un medio de comunicación electrónico, creado como herramienta de la producción, no podrá perjudicarse el uso específico empresarial preordenado para el mismo, ni pretenderse que deba prevalecer el interés de uso sindical, debiendo emplearse el instrumento de comunicación, por el contrario, de manera que permita armonizar su manejo por el sindicato y la consecución del objetivo empresarial que dio lugar a su puesta en funcionamiento, prevaleciendo esta última función en caso de conflicto. A tal efecto resultaría constitucionalmente lícito que la empresa

- la comunicación sindical no podrá perturbar la actividad normal de la empresa.

- Debe armonizarse el uso empresarial y sindical de la tecnología, prevaleciendo en conflicto el uso empresarial. Para ello la empresa puede regular el uso sindical del medio electrónico, sometiéndolo a límites, no absolutos.

- El uso sindical no debe no puede "ocasionar gravámenes adicionales" al empresario.

predeterminase las condiciones de utilización para fines sindicales de las comunicaciones electrónicas, siempre que no las excluyera en términos absolutos.

c) […] la utilización del instrumento empresarial no podrá ocasionar gravámenes adicionales para el empleador, significativamente la asunción de mayores costes." (FJ 8º).