



Se plantea en la presente si es conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, en adelante LOPD, y su normativa de desarrollo, la actuación de la consultante en cuestión consistente en la entrega a todos los trabajadores junto con la nómina de un determinado mes, de un Anexo al contrato relativo al deber de confidencialidad, así como respecto del uso de Internet y del correo electrónico para fines profesionales; Anexo que se adjunta a la consulta planteada.

## I

La primera cuestión planteada versa sobre el deber de secreto y de confidencialidad de los empleados. Con carácter general debe indicarse que los artículos 1 y 2 de la Ley Orgánica 15/1999, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como *“cualquier información concerniente a personas físicas identificadas o identificables”*.

El artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa que constituye un dato de carácter personal *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.”*

Y constituye un tratamiento de datos personales, de conformidad con lo previsto en el artículo 3.c) de la Ley Orgánica 15/1999, las *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.”*

Pues bien, dentro de este ámbito de protección de datos personales, el deber de confidencialidad es ya consagrado en el artículo 16 de la Directiva 95/46/CE de 24 de octubre de 1995 del Parlamento Europeo y del Consejo 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, que bajo la rúbrica *Confidencialidad del tratamiento* señala: *“Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal”*.

Por su parte, el artículo 10 LOPD bajo la rúbrica *Deber de secreto* señala que *“El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo”*.

El deber de secreto deberá acompañarse de la adopción por el responsable del tratamiento de los datos de las medidas de seguridad exigibles en orden a garantizar el mismo. Así el artículo 9 de la propia LOPD se refiere a la seguridad de los datos estableciendo que:

*“1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

*2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.*

*3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.”*

Las medidas de seguridad a adoptar aparecen reguladas en los artículos 79 y siguientes del Reglamento (RLOPD). Entre las mismas destaca el documento de seguridad del artículo 88 que deberá elaborar el responsable del tratamiento y que deberá tener entre su contenido lo señalado en su número 3. c), esto es, *“Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros”* y para el tratamiento automatizado de datos el artículo 89.2 establece que: *“2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.”*

Por último debe tenerse en cuenta que la vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal viene contemplado como infracción grave en el artículo 44.3 d) de la LOPD, con independencia de otras responsabilidades que pudieran ser exigibles en los demás órdenes jurídicos.

Desde esta perspectiva, el Anexo al contrato remitido a esta Agencia da cumplimiento al deber del responsable del fichero de adoptar las medidas necesarias para que el personal que tenga acceso a datos personales conozca su deber de secreto profesional respecto de tales datos, que subsistirá incluso una vez extinta la relación laboral.

Otra cosa distinta es que, junto con dicha información sobre el deber de confidencialidad o secreto de los datos personales a los que haya accedido, se incluya un deber más amplio de confidencialidad de toda la información – incluya ésta o no datos personales – relativa a la actividad de la persona jurídica. Pero esta Agencia entiende que el Anexo en cuestión, en lo que afecta a esta primera materia de información sobre el deber de confidencialidad, da cumplimiento suficiente a las previsiones de la legislación sobre protección de datos. Y si junto con dicho deber se incluye otro más amplio de secreto empresarial, excede del ámbito de competencias de esta Agencia.

## II

Junto con el deber de confidencialidad, el Anexo al contrato de trabajo versa en su apartado 2) sobre el uso de Internet y de la dirección de correo electrónico por los trabajadores. Entendemos que se refiere al correo electrónico corporativo, puesto que se reconoce la propiedad empresarial de dicho correo y que el mismo será destinado *“para fines profesionales, si bien se autoriza al trabajador a que pueda hacer uso de dichas herramientas de trabajo para fines personales, siempre que el mismo se realice de manera razonable y conforme al principio de buena fe contractual”*.

Esta cuestión afecta plenamente al futuro acceso que el empleador pueda hacer respecto de los datos personales de sus trabajadores, tanto los obtenidos a través de la navegación por Internet como los derivados del uso de correo electrónico corporativo.

Se plantea así el tema de la compatibilidad entre el control empresarial y el derecho a la protección de datos, de aquellos datos que resulten del uso del correo corporativo y el acceso a internet. Y es que, como es sabido, la jurisprudencia en estos casos viene apreciando como uno de los criterios – si no el esencial - para determinar si cabe el control empresarial sobre aquellos medios, la previa información o advertencia del empresario al trabajador sobre sus posibilidades de uso y control. Así, por su claridad, y aunque trate el tema desde el punto de vista del derecho fundamental a la intimidad y, en caso del correo electrónico, secreto de las comunicaciones, citamos la **Sentencia de la Sala de lo Social, Sección 1ª del Tribunal Supremo de 26 de septiembre de 2007**, casación para la unificación de doctrina núm. 966/2006, Ponente Excmo. Sr. Desdentado Bonete, en los siguientes términos (el subrayado es nuestro):

*“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 (...) 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. (...)

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. (...) 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 (...)

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 98/2000 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 para 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”.*

Y más recientemente la **Sentencia del Tribunal Constitucional, Sala 1ª 170/2013 de 7 de octubre** también parte de considerar que cabe el control empresarial sobre las herramientas informáticas, si bien estudiando si existe o no *“una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas”*; en dicho supuesto el convenio colectivo contenía una previsión expresa de uso exclusivo profesional, incluyendo un tipo sancionador al respecto, por lo que se consideró que el trabajador no podía tener tal expectativa de confidencialidad, por lo que el control era lícito. Ahora bien, reiteramos que en este ámbito se considera si el trabajador estaba o no *“advertido de la posibilidad de que sus comunicaciones pudieran ser objeto de seguimiento por la empresa”*, cuestión que *“ha llevado a admitir que dicho trabajador podía razonablemente confiar en el carácter privado de las llamadas efectuadas desde el teléfono del trabajo o, igualmente, en el uso del correo electrónico y la navegación por Internet (SSTEDH de 25 de junio de 1997, caso Halford c. Reino Unido, § 45; de 3 de abril de 2007, caso Copland c. Reino Unido, § 42 y 47). Sin embargo, en el supuesto que ahora nos ocupa, el régimen jurídico aplicable en la empresa respecto al uso de las herramientas informáticas de su propiedad hacía factible*

*y previsible la posibilidad de que el empresario ejerciera su facultad legal de vigilancia sobre los correos electrónicos del trabajador, tanto a efectos de supervisar el correcto cumplimiento de su prestación laboral desarrollada a través de este instrumento, como a fin de constatar que su utilización se ceñía a fines estrictamente profesionales y no personales o extralaborales. Tal circunstancia impedía en este caso abrigar una expectativa razonable de privacidad que determinara la entrada en la esfera de protección del derecho a la intimidad, de acuerdo con lo explicado en la ya citada STC 12/2012, FJ 5”.*

Y en el caso planteado, mediante la firma del Anexo al contrato de trabajo existiría una información al trabajador del uso que debe darse a este tipo de medios; la firma del Anexo es uno de los medios a través de los cuales el empresario puede probar dicha circunstancia; como podría por otro lado acreditarse mediante la aportación de otros indicios que coadyuvaran a entender cumplido este requisito, pero siendo la firma uno de ellos, totalmente lícita y admitida en Derecho.