1. Los códigos de conducta informática como vía de autorregulación de las nuevas tics en la empresa

Codes of computer conduct as a way of self-regulation of new ict in the company

(Autor)

LOURDES MELLA MÉNDEZ

Catedrática de Derecho del Trabajo y de la Seguridad social. Universidad de Santiago de Compostela (España) lourdes.mella@usc.es

Sumário:

Área do Direito: Trabalho

Resumen:

Este trabajo analiza los códigos de conducta informática que muchas empresas están elaborando

como una vía adecuada para regular el uso de las herramientas digitales en el marco del contrato de trabajo. Esta autorregulación, aunque mejorable en muchos aspectos, tiene el valor de aportar seguridad jurídica a los trabajadores sobre los límites de lo permitido con aquellas y el control empresarial a realizar. Al hilo de la reciente normativa española sobre protección de datos y garantía de los derechos digitales y la jurisprudencia nacional e internacional, estos códigos adquieren, cada vez más, una mayor importancia en la empresa.

Abstract:

This paper analyses the codes of computer conduct that many companies are developing as an adequate way to regulate the use of new information and communication technologies. This self-regulation, although improvable in many aspects, has the value of providing legal security to employees over the limits of what is allowed with those. Following the recent judgments of the ECHR, these codes acquire, increasingly, a greater importance in the company.

Palabras Clave: códigos de conducta, autorregulación, nuevas tecnologías
Keywords: codes of conduct, self-regulation, new technologies

1. Tradicional anomia legal en el ámbito de las tics e importancia creciente de la autorregulación[1]

Cuando la Organización Internacional del Trabajo lanza –al hilo de su Centenario- la iniciativa del futuro del trabajo, en el que uno de los puntos básicos es el cambio tecnológico y cómo lograr que la tecnología beneficie a todos, ya nadie puede dudar de la trascendencia de las disruptivas innovaciones tecnológicas que estamos viviendo, así como las que vendrán en los próximos años (por ejemplo, nuevas Tics, robótica, inteligencia artificial, Internet de las cosas, impresión 3D o, en fin, Industria 4.0). Estas innovaciones técnicas afectan profundamente a la tradicional forma de trabajar, producir bienes y servicios y hasta de vivir. En la empresa, el uso de Internet, de los dispositivos informáticos (portátiles, teléfonos inteligentes) y sus diversas aplicaciones (redes sociales) se convierte en un importante instrumento de trabajo. Y, consecuentemente, las nuevas Tics alteran profundamente el equilibrio tradicional de poderes, saliendo reforzado el poder de dirección y control del empresario sobre los derechos de los trabajadores. Por lo tanto, resulta fundamental una regulación detallada sobre el uso de estas nuevas tecnologías como instrumentos de trabajo, en orden a garantizar el necesario equilibrio entre los derechos de las partes, algo que, tradicionalmente, el legislador español omitió (hasta la reciente regulación de 2018).

Tal regulación detallada resulta necesaria y aporta seguridad jurídica a las partes, especialmente al trabajador, sobre lo que está o no permitido hacer con los instrumentos digitales y, por lo tanto, con las posibles sanciones que puedan imponerse cuando hay extralimitación en lo previamente dispuesto. Así las cosas, las opciones de autorregulación son diversas, según haya connivencia o no entre las partes sociales. En el primer caso, estas pueden acudir a procedimientos clásicos de negociación colectiva o individual, abordando la materia en un convenio colectivo estatutario o pacto o acuerdo de empresa informal o en el contrato de trabajo, respectivamente. Sin duda, la mejor opción parece la primera, la del convenio estatutario, en cuanto su carácter normativo y eficacia personal general garantizan la máxima aplicación y respeto para las cláusulas que específicamente traten la materia informática. Además, repárese en que, por un lado, ante la ausencia de disposición legal, lo propio es que la regulación convencional normativa emerja y cubra tal vacío, y, por otro, en función de los ámbitos de aplicación del convenio, lo paccionado tiene una importante capacidad de adaptación a las necesidades de cada sector, empresa o centro de trabajo. Quizás por ello, el III Acuerdo para el empleo y la negociación colectiva (2015 a 2017), actualmente prorrogado, prevé expresamente que los convenios colectivos deben tener como uno de sus objetivos fundamentales el de abordar “la incidencia de las tecnologías de la información y de la comunicación en el desarrollo productivo general y en las relaciones laborales”. Dichas tecnologías deben servir para establecer “canales de comunicación entre las partes y como vehículo de información a los trabajadores” por parte de la representación legal de los trabajadores, que deberán ser objeto “de un uso racional” (capítulo II, número 5)[2].

En cuanto al pacto individual, el contrato de trabajo también es un buen lugar para introducir (en una cláusula interna o en un anexo al mismo) precisiones respecto de las posibilidades de utilización privada de las nuevas Tics en relación con un concreto trabajador, especialmente cuando las circunstancias de este aconsejan incluir matices propios respecto de lo que se haya dispuesto, con carácter general, en el convenio colectivo o, incluso, en el código de conducta informático. Así, por ejemplo, para un alto directivo o un trabajador funcionalmente muy especializado puede disponerse el uso privado de los medios informáticos de la empresa, Internet o las redes sociales con un régimen particular y más favorable que el dispuesto para el resto de la plantilla. En tal caso, se acordaría, a nivel individual, una condición más beneficiosa de origen contractual. Con todo, bien conocida es la posición de superioridad en la que se halla el empresario en este ámbito contractual, en el que más que verdadera negociación a veces solo hay imposición y adhesión del trabajador a las condiciones unilaterales de aquel. En esta línea, resulta significativa alguna sentencia del TS que declaró nula por abusiva la cláusula tipo incluida en el contrato de trabajo de los tele-operadores, conforme a la cual estos cedían voluntariamente a la empresa ciertos datos personales (como el número de móvil y el correo electrónico personal)[3]. El Alto Tribunal –acogiendo la tesis del Ministerio Fiscal- estimó que se estaba ante unos datos de carácter personal cuyo conocimiento, uso y destino tiene que quedar bajo el control de su titular, y la incorporación al contrato de una cláusula como la cuestionada “supone una conducta abusiva”, por cuanto “no puede entenderse que el trabajador haya prestado su consentimiento de una manera libre y voluntaria”[4]. Por lo tanto, si el trabajador entiende abusiva una cláusula contractual relativa al uso de los medios informáticos empresariales, como Internet o las redes sociales, por restringir sus derechos o conllevar una sanción disciplinaria, resulta aconsejable que someta su validez al criterio judicial.

En el supuesto de que no haya connivencia reguladora entre las partes, el empresario puede tratar, unilateralmente (aun con consulta previa a los representantes), el tema del uso de las nuevas Tics en un protocolo interno, bien como parte de un protocolo empresarial más amplio (un código ético[5]), bien como protocolo de conducta[6] específico y monográfico en la materia, denominado “código de conducta informática” o “código de conducta telemático”[7]. Con todo, en ocasiones, el código de conducta aún remite a un documento más específico, denominado “normas de utilización de herramientas informáticas” o “Política de uso del correo electrónico y herramientas colaborativas”. Sea como fuere, esta regulación específica es una solución que últimamente se ha puesto de moda, quizás por la rapidez y comodidad que para la empresa supone el tener una regulación mínima en la materia tratada, si bien también aquí cabe estar vigilantes sobre posibles abusos para la posición del trabajador.

Además, cabe apuntar ya que esta es la solución por la que se inclina el legislador estatal en el primer texto regulatorio de las Tics en el ámbito laboral. En efecto, la reciente Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDYDD), con la que se adapta el ordenamiento jurídico español al Reglamento General de protección de datos (aplicable directamente desde el 25 mayo 2018), contiene algunas disposiciones de interés sobre el asunto que nos ocupa. En efecto, la citada Ley aprovecha la ocasión para añadir unas garantías de los derechos digitales de la ciudadanía, conforme al mandato constitucional de respeto al derecho a la intimidad *ex* art. 18.4 Constitución (Título X; arts. 79 a 97)[8]. Entre los derechos que ahora se reconocen expresamente por ley, cabe citar el derecho a la intimidad del trabajador en relación con el uso (que él haga) de dispositivos digitales de la empresa o frente a la utilización por el empresario de dispositivos de videovigilancia, de grabación de sonidos y sistemas de geolocalización, o el derecho a la desconexión digital para garantizar el derecho al descanso y salud de aquel. La valoración de tal regulación legal es crítica, en cuanto general y carente de concreción. El legislador se limita a declarar el derecho del trabajador al reconocimiento de sus derechos fundamentales al hilo del uso de los instrumentos digitales en el ámbito laboral, pero la concreción de estos se deja a la posterior voluntad del empresario, aun con consulta previa a los representantes de los trabajadores. De esta manera, el legislador impulsa, con decisión, la implicación del empresario en la elaboración de una política interna dirigida a los trabajadores en la que se establezcan los criterios de utilización de los dispositivos digitales (art. 87.3) u otros aspectos, como las modalidades de ejercicio del derecho a la desconexión (art. 88.3).

En fin, esta actuación empresarial de elaboración de una política interna sobre el uso de las herramientas digitales recibe un impulso similar de la jurisprudencia europea, pues la Sentencia de la Gran Sala del TEDH de 5 de septiembre de 2017 (caso Barbulescu), incide sobre ella. Así, tras distintas referencias al marco internacional protector de los derechos fundamentales y la necesaria protección de los datos personales de los trabajadores, se apunta a la especificidad de la relación laboral subordinada y a la necesidad de que los Estados y los agentes sociales fijen el marco de actuación legal o convencional en el que deberá desenvolverse la actuación laboral del trabajador, lo que incluye el régimen aplicable a las comunicaciones electrónicas realizadas con las herramientas digitales. En esta línea, se añade que, de no actuar aquellos, el empresario puede aprobar una regulación interna o código de conducta, si bien este tiene que ser igualmente protector de los intereses de los trabajadores, indicando, claramente, todas las limitaciones que se introduzcan en el uso privado de los medios tecnológicos y el concreto control empresarial a realizar[9]. Sobre estos puntos se profundizará *supra.*

2. Sobre la configuración de los códigos de conducta

2.1. General

Desde un punto de vista tradicional, estos códigos de conducta informática se pueden definir como una guía interna o conjunto de disposiciones dictadas unilateralmente por el empresario (aun con participación de los representantes) para regular los instrumentos de trabajo de carácter informático puestos a disposición de los trabajadores, con el fin de aportar seguridad jurídica sobre el alcance de la utilización permitida a estos[10].

Como se aprecia, la finalidad de estos códigos de conducta es cubrir un vacío de regulación legal o convencional sobre un aspecto específico e importante para la empresa y, con ello, ofrecer una mayor certeza y transparencia sobre el comportamiento esperado respecto de aquel y las consecuencias de no hacerlo así. De esta manera, se dan indicaciones precisas y claras sobre la conducta esperada por la plantilla, esta sabe a qué atenerse y, por tanto, se reduce la conflictividad laboral y mejora el clima en la empresa. Por supuesto, esta mejora de la paz social también implica la de la productividad y eficiencia en el desarrollo de la prestación laboral, pues las conductas están pautadas y se actúa con mayor seguridad y sin pérdidas de tiempo de trabajo. En esta línea, se expresa algún código al declarar que su objeto es “el garantizar el buen uso, tanto de la información como de los medios técnicos propiedad” de la empresa. Sin duda, el establecimiento de “reglas claras” al respecto propician “la mayor eficiencia en los sistemas de información y evitan la utilización incorrecta o inadecuada” de los mencionados medios[11]. Por lo demás, esa mejora social también deriva del hecho de que la aplicación del código implica una igualdad de trato para todos los trabajadores, sin posibilidad de aceptar decisiones empresariales diferenciadas e injustificadas ante una misma conducta.

Aunque los directamente favorecidos por esta actividad empresarial son las partes del contrato de trabajo (trabajadores y empresarios), de una manera indirecta, también los terceros relacionados con la empresa (representantes legales, sindicatos, clientes o proveedores) se benefician. En efecto, la difusión del código a la sociedad permite a esta el conocer las pautas de comportamiento esperado en una empresa y, en su caso, el tercer cliente o proveedor ya puede evitar entrar en conductas prohibidas o no permitidas para el trabajador. Además, la imagen social de la empresa queda reforzada, en cuanto se presenta como una entidad preocupada por abordar aspectos que pueden generar conflictos por su previa falta de regulación o, en su caso, por su ambigüedad regulativa.

2.2. Naturaleza jurídica: autorregulación con participación de los representantes

Dadas las importantes ventajas recién expuestas, resulta evidente que cada empresa debería ser proactiva y tomar la iniciativa de adoptar una política interna de uso de los dispositivos digitales, ejerciendo así su responsabilidad de proporcionar una regulación mínima al respecto. También cabe que, ante las dudas que vayan surgiendo, sean los propios trabajadores o sus representantes (o, incluso, terceros, como clientes o proveedores) los que apunten la necesidad de que tal política

sea adoptada. Con todo, la existencia de una verdadera obligación legal del empresario de negociar esos protocolos internos no está clara, ni siquiera con la nueva LOPDYDD. En efecto, *a priori,* esta norma parece bastante taxativa en la imposición al empresario de la obligación de elaborar protocolos internos informáticos, pues, por un lado, dispone que "los empleadores *deberán* establecer criterios de utilización de los dispositivos digitales" (art. 87.3), y, por otro, que el empleador "*elaborará* una política interna dirigida a los trabajadores" (art. 88.3). Sin embargo, cabe preguntarse cuál será la sanción si el empresario no cumple con ese deber legal, pues el legislador no lo ha aclarado. Ello permite pensar que, a pesar de los términos imperativos "deberán" y "elaborará", aquel está efectuando una mera declaración sobre la facultad que el empresario tiene de redactar estas políticas internas.

Ahora bien, lo que legalmente queda claro es que, si procede a la elaboración de estas políticas, el empresario debe consultar a los representantes de los trabajadores, como límite o garantía formal frente a la actuación unilateral de aquel, en un ámbito tan sensible como este del uso de las herramientas informáticas, que fácilmente puede colisionar con los derechos fundamentales de aquellos. De alguna manera, el legislador quiere limitar o condicionar el poder unilateral del empresario, estableciendo la necesidad de oír a los representantes de los trabajadores y que estos se involucren en la redacción de esa política interna de la empresa. Así, respecto del establecimiento de los criterios de uso de los dispositivos digitales, se prevé que, "en su elaboración, deberán participar los representantes de los trabajadores" (art. 87.3), y, en relación con la desconexión digital, se establece que debe darse "previa audiencia" a estos (art. 88.3). Por lo tanto, resulta evidente la necesidad de consultar y oír la opinión de los referidos sujetos.

Claro lo recién expuesto, de inmediato, surgen varias dudas, entre ellas, la relativa a si la garantía formal de participación de los representantes es la misma en ambos preceptos, pues, en un caso, el legislador se refiere, genéricamente, a la participación de aquellos, y, en el otro, se especifica que dicha participación debe concretarse en una "audiencia previa". Aunque hay argumentos para defender lo contrario, la mejor opción es sostener que se trata de un mismo tipo de garantía formal, y que el segundo precepto aclara cómo debe ser esa participación de los trabajadores en la elaboración de la política interna. Por lo tanto, el empresario debe dar audiencia previa a los representantes, lo que significa que estos deben ser informados previamente por aquel de la intención de elaborar el código y de las materias y contenidos más relevantes, dudosos o polémicos que afecten a los derechos fundamentales de los trabajadores (por ejemplo, libertad de expresión o intimidad), y, después, deben disponer de un plazo para poder aportar, oralmente o por escrito, las consideraciones que estimen convenientes. Desde luego, debe existir una voluntad real de negociar y alcanzar acuerdos, pues cuanto más consenso exista en la elaboración del código, más posibilidad habrá de observancia pacífica de su contenido. Además, si el legislador no hubiera querido que se tuviese en cuenta la opinión de los representantes no hubiese introducido esta modificación en la elaboración del código de conducta. Ahora bien, la conclusión es un poco decepcionante, en cuanto el informe de los representantes no resulta vinculante para el empresario, quien una vez oídos aquellos, puede proceder a finalizar el protocolo interno como estime conveniente y bajo su exclusiva responsabilidad. Repárese en que el legislador introduce este requisito formal (oír a los representantes) en el marco del código de conducta, no de un verdadero convenio colectivo o acuerdo de empresa. De hecho, el art. 88 LOPDYDD deja claro que se está ante ámbitos reguladores diferentes, pues el núm. 2 del citado precepto se refiere a esos dos acuerdos colectivos propiamente dichos, y el núm. 3 a la política interna (unilateral) del empresario, aun con audiencia de los representantes.

De otro lado, otra duda importante es la de la consecuencia jurídica de la omisión de esta formalidad de consulta previa. Aunque el legislador no lo dice, parece que la omisión de tal requisito formal debe conllevar la ineficacia del protocolo (de impugnarse), a modo de lo que sucede en otros casos en los que el legislador también impone al empresario este requisito formal de consulta a los representantes antes de adoptar determinadas decisiones (como sucede en los despidos disciplinarios de los trabajadores aforados). En fin, cabe pensar que, dada la falta de precisión legal, la dimensión exacta de la participación de los representantes en la elaboración de estos protocolos telemáticos será una cuestión que tendrán que precisar los tribunales laborales en el futuro.

Tradicionalmente, la legitimidad del empresario para redactar unilateralmente estos protocolos se fundamentó en su poder de dirección y organización de la actividad productiva, previsto en el art. 20 Estatuto de los Trabajadores (ET), según cuyo núm. 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". Tras la LOPDYDD, dicha competencia –y deber- aparece atribuida expresamente al empresario (aun con audiencia previa a los representantes) por los ya citados artículos 87.3 y 88.3 de aquella. Por su parte, la obligación del trabajador de observar pacíficamente lo dispuesto en estas guías deriva del mismo art. 20.2, de acuerdo con el que, a la hora de cumplir con la obligación de trabajar asumida en el contrato, aquel debe al empresario "la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o *instrucciones* adoptadas por aquel en el ejercicio regular de sus facultades de dirección". En cualquier caso, tanto el empresario como el trabajador deben respetar las exigencias de la buena fe, lo que impedirá a aquel adoptar un código de conducta lesivo para los derechos e intereses legítimos del trabajador y a este realizar conductas contrarias a su contenido legítimo.

Aun cuando el código de conducta telemático suele ser unilateral, podría suceder que, al hilo de la audiencia previa de los representantes, el empresario haya contado con el pleno consentimiento de estos y aquel sea fruto del mutuo acuerdo. En esta línea de pactos consensuados, incluso cabe pensar en el supuesto concreto de que se hayan observado los requisitos de capacidad y legitimación negociadora, contenido y procedimiento previstos en los arts. 87 y ss. del Título III ET, siendo, en tal caso, la naturaleza del código pactado jurídica similar a la de un convenio colectivo, incluso estatutario. Lógicamente, en este supuesto, la eficacia personal del código –asimilado a un verdadero convenio colectivo de empresa- sería general y afectaría a todos los incluidos en su ámbito de aplicación y su naturaleza sería normativa, constituyendo derecho objetivo de obligada observancia. Otro tanto sucedería si el código se incluyese como contenido propio del convenio colectivo aplicable a la empresa.

Sin embargo, la situación recién expuesta de connivencia entre las partes parece excepcional (muy diferente es la disposición exigida para negociar un convenio o un código), y lo habitual será que el código telemático sea un producto unilateral de la empresa y, de ser así, resulta claro que carece de eficacia jurídica normativa por sí mismo, o sea, de fuerza vinculante en los términos del art. 37 Constitución Española. A partir de ahí, surgen muchas dudas sobre la naturaleza y eficacia de estos protocolos internos. En principio, podría argumentarse que, aun cuando son redactados unilateralmente por el empresario, su eficacia práctica queda garantizada, en cuanto consisten en instrucciones escritas derivadas de su poder de dirección (relativas, por ejemplo, en lo que aquí interesa, a criterios de uso de los dispositivos digitales utilizados como instrumentos de trabajo) y, que son de obligado cumplimiento para el trabajador.

3. Criterios de regulación: forma y contenido

Cuando el empresario decide elaborar su política interna de uso de los diversos instrumentos informáticos por parte de la plantilla durante el tiempo de trabajo, debe tener en cuenta dos aspectos: la forma y el fondo.

3.1. Forma

La forma debe ser la escrita, pues es lo que naturalmente se corresponde con un instrumento que se denomina "protocolo o código de conducta". Además, la forma escrita aporta una mayor seguridad jurídica sobre su contenido y facilita su negociación y difusión, así como su inclusión, en su caso, en el convenio colectivo. En este último supuesto, de ser el código inicialmente oral pasaría a adquirir la forma escrita al integrarse en el clausulado del convenio. La redacción debe ser clara y concreta; lo primero exige el uso de un lenguaje llano y sencillo, que sea entendible por todo el mundo (ciudadano medio), evitando, en la medida de lo posible, anglicismos y tecnicismos, propios del mundo informático; lo segundo, requiere precisión en las ideas expuestas, sin ambigüedades ni circunloquios que dificulten la comprensión del régimen que el empresario quiere imponer. Tal precisión resulta especialmente importante en aquellos aspectos que imponen

limitaciones de uso en las Tics y cuya vulneración implica una sanción disciplinaria u otro tipo de consecuencia similar para el trabajador.

Desde el punto de la vista de la estructura formal, no existe nada predeterminado legalmente, salvo lo que el convenio colectivo pueda disponer. Con todo, resulta adecuada -y se valora positivamente- una estructura ordenada que, incluya, por ejemplo, una introducción o exposición de motivos, la finalidad u objeto del código, su ámbito de aplicación, los principios generales que rijan la materia y, después, las cláusulas detalladas de contenido telemático propiamente dicho. Sobre la extensión recomendable del código, tampoco hay nada regulado, por lo que aquella será la exigida por la correcta y completa exposición de las ideas, sin reiteraciones innecesarias. Ahora bien, este aspecto de la extensión también puede depender de si el código trata o no de manera monográfica las normas de uso de las Tics, pues, a veces, no ocurre así, y aquellas se incluyen en códigos de conducta generales de la empresa, en el que se abordan muchos aspectos distintos (así, en los códigos éticos se trata la responsabilidad social de aquella con los accionistas o sociedad en general, normas de ética y prevención de conductas de acoso y actos discriminatorios y otras similares)[12].

La parte introductoria del código suele referirse a los motivos o necesidad de su redacción y a la filosofía general de la empresa, en cuanto al deseo de transparencia y seguridad jurídica en la materia. En relación con los motivos, la finalidad del código suele concretarse en el establecimiento de "las pautas generales de actuación de todos los empleados de la empresa respecto a los equipos informáticos, programas y todo tipo de software e información facilitado por la empresa para el desempeño de sus funciones profesionales"[13]. En cuanto al ámbito subjetivo, estos códigos suelen dirigirse a todos los empleados de la empresa, tanto en lo referente al manejo de las herramientas, datos e informaciones propias como de otras posibles empresas con las que tenga relación profesional (por ejemplo, empresa con las que se subcontrata o colabora). En ocasiones, el código incluso se extiende al personal externo a la empresa, que, aun sin relación laboral, colabora con aquella y usa puntualmente sus equipos informáticos. Lógicamente, en tal caso, dicho personal solo vendrá obligado a observar las reglas del código que les sean pertinentes por su actividad[14].

3.2. Contenido: aspectos generales

Respecto del fondo o contenido telemático propiamente dicho, la regla general es la de su amplitud. El empresario puede escoger el tratar aquellos aspectos que más le preocupan dentro de su empresa y en la gestión de su plantilla, desechando otros ajenos o más generales. De hecho, repárese en que el objetivo último del código será, general y lógicamente, el regular los aspectos relativos a las nuevas Tics que más interesan a la empresa, en aras de proteger sus propios intereses. Un sucinto examen de algunos códigos de conducta revela que los puntos temáticos más tratados son los siguientes:

1) El general uso laboral de los instrumentos informáticos (v. gr., servidores, ordenadores personales, teléfonos inteligentes, disqueteras, lectores o grabadores de CD, sistemas de videoconferencia, impresoras, proyectores, faxes, programas informáticos, redes sociales y otros medios informáticos o audiovisuales)[15]. Se suele comenzar con una inicial declaración general relativa a que los medios informáticos de cualquier tipo facilitados por la empresa deben usarse, exclusivamente, como herramienta de trabajo para el desarrollo de tareas profesionales, y, en consecuencia, no para fines privados o ajenos a aquellas. Esta restricción de uso privado puede referirse, bien al manejo que el trabajador da a los equipos informáticos, en sí mismos, bien a la actividad realizada a través de ellos. Por lo que se refiere al primer aspecto, se suele prohibir el almacenamiento de datos o archivos de carácter personal en el ordenador de la empresa, así como la instalación o utilización de *software* ajeno no facilitado por aquella, como, por ejemplo, programas de juego, música, renta u otras utilidades[16]. En la misma línea, los trabajadores no podrán, salvo autorización expresa, modificar la configuración de sus equipos ni programas informáticos (borrar, dañar, alterar, hacer inaccesible el contenido), ni añadir o eliminar elementos periféricos asociados a aquellos.

En cuanto a la navegación por Internet, esta se suele limitar a aquellos trabajadores que realmente

la necesiten para realizar su actividad laboral, y ello debido al coste económico de la línea y a la sobrecarga que, en caso contrario, se produciría en esta y que perjudicaría el acceso de los clientes, proveedores o colaboradores a los *sites* de la empresa, así como la utilización de sus propias aplicaciones. También aquí la empresa puede restringir el acceso de los trabajadores a webs no deseadas de contenido considerado ilegal, no apropiado o, simplemente, ajeno a la actividad laboral (v. gr., páginas de contenido sexual, racista, juego, difamatorio y otras parecidas, como programas de mensajería o chats)[17], así como la divulgación o transmisión de ese tipo de información por cualquier clase de formato (fotografías, textos, videos, *banners* publicitarios o enlaces a páginas externas). También se suele prohibir la reproducción y distribución de cualquier información, material pirateado o *software* que contenga virus dañinos para la integridad de los sistemas informáticos o que pueda infringir derechos de propiedad intelectual, así como facilitar material o acceso a recursos sobre *hacking*, *cracking* o cualquier otra información que se considere susceptible, aun potencialmente, de comprometer la seguridad o integridad de los sistemas informáticos de la empresa[18].

Las razones de esta general prohibición de uso privado se relacionan con la legítima salvaguarda de los intereses de la empresa, concretada en: 1) la necesidad de protección de los equipos informáticos, evitando la entrada de virus o programas maliciosos del exterior, lo que busca la máxima duración y eficiencia de aquellos; 2) el impedir la comisión de delitos relacionados con el uso ilegal u ofensivo de aquellos o de aplicaciones sin licencia, que podrían perjudicar la reputación e imagen social de la empresa; y 3), el evitar la distracción del trabajador y la consiguiente disminución de su rendimiento laboral. De ahí que la prohibición de uso extra-laboral de los medios informáticos no se limite estrictamente a la jornada laboral, sino que puede ir más allá y abarcar el tiempo de descanso, ya se gaste este en las instalaciones de la empresa (especialmente el previo o posterior al término de la jornada laboral) o en otras privadas. En este segundo caso, la mencionada prohibición de uso del equipo fuera del ámbito de la empresa se relaciona, sobre todo, con los dos primeros objetivos (protección de equipos y evitación de delitos)[19].

En ocasiones, los códigos de conducta establecen este uso profesional de los instrumentos informáticos con carácter exclusivo y absoluto, sin margen alguno para el uso privado (al menos, contemplado formalmente en el código). Estos códigos son especialmente proteccionistas de los intereses de la empresa, y la calificación del uso profesional como “exclusivo” o “absoluto” busca definir con claridad la posición de la empresa al respecto, sin abrir la puerta a excepciones de uso privado que puedan derivar en posteriores abusos. Como ejemplo de este tipo de códigos, cabe citar los del Grupo Sacyr[20], KH Lloreda[21], CEPSA, Nestlé[22], Inditex[23], Grupo Mediapro, Viscofan, o, en fin, Delaviuda[24]. Con todo, ello no impide que, en un caso concreto, previa solicitud del trabajador, se pueda autorizar un uso privado no previsto expresamente. Sin embargo, en otras ocasiones, el propio código, tras la declaración inicial de uso general profesional, ya admite ciertos supuestos de uso privado, como veremos a continuación.

2) El carácter limitado del uso privado de los instrumentos de trabajo informáticos. Aunque, en general, estos protocolos suelen ser restrictivos, prohibiendo el uso extra-laboral de las Tics, no faltan ocasiones en las que se permite un cierto uso privado de las mismas. Esta moderada flexibilidad resulta lógica y positiva, pues, en la actualidad, algunas Tics forman parte de la vida privada y social de las personas, que ya no pueden prescindir de ellas, y, de este modo, ante circunstancias imprevistas y que es necesario atender de manera urgente, se evita la ausencia del trabajador del puesto de trabajo o, en otro caso, el daño causado por no permitirle gestionar ese interés privado dentro de la jornada laboral. Como se deduce de lo recién expuesto, ese uso extralaboral tiene carácter privado y está relacionado con la satisfacción de intereses particulares del trabajador e, incluso, de terceros[25] (por ejemplo, sus familiares, amigos o clientes de la empresa).

Este uso privado debe caracterizarse por la concurrencia simultánea de tres notas: a) excepcionalidad, lo que implica que no es algo habitual ni generalmente consentido por la empresa, sino meramente ocasional, mínimo o moderado. b) Justificación objetiva, lo que indica la aparición de causas justas concurrentes en el trabajador afectado (por ejemplo, urgencia en la realización de una gestión o trámite privado, cuyo plazo concluye a determinada hora o día

laboral o la necesidad de atender los intereses familiares, o sea, por razones de conciliación[26]); en estos casos, el uso privado permitido debe ser proporcional a la entidad de las causas que lo amparan. Y c) no lesividad ni abuso para los intereses de la empresa, en cuanto no dañe su imagen ni conlleve consecuencias económicas negativas para la misma[27]. Repárese en que esta última condición, que es la que justifica la prohibición absoluta de uso privado, debe seguir observándose cuando este uso se admite parcialmente y aparece apoyado en las circunstancias del supuesto concreto. Por lo tanto, lo que siempre debe cumplirse es que el interés empresarial quede salvaguardado y que, en su caso, el uso personal de la herramienta informática nunca cause perjuicio a la empresa. Así, pues, esta nunca pierde o acusa impacto negativo alguno en su patrimonio o posición comercial, que sigue intacta. Esta condición proteccionista se justifica en que se está ante la utilización de herramientas proporcionadas por la empresa para la realización de la actividad laboral. La ausencia de estas consecuencias económicas negativas para la empresa suele estar relacionada con la primera nota, pues un uso privado ocasional no merma de manera significativa la duración de la jornada laboral, los recursos de la empresa ni la productividad del trabajador.

La admisión excepcional del uso privado puede condicionarse a la previa autorización del empresario o dejarse al criterio subjetivo del propio trabajador, quien tiene que decidir, en cada situación, si se observan los requisitos necesarios para aquel uso[28]. El primer supuesto es el que aporta mayor seguridad jurídica para las partes, y, en especial, para el trabajador, pues si, ante la aparición de determinadas circunstancias, aquel procede a consultar al empresario sobre la posibilidad de hacer un uso privado de los instrumentos de trabajo, su posterior comportamiento podrá adaptarse (o no) a la respuesta empresarial con total conocimiento de causa. Y, si hay un incumplimiento de lo permitido, este será querido y consciente, por lo que el empresario tendrá más fácil imponer una consecuencia disciplinaria.

La autorización previa del empresario de un uso privado razonable de las herramientas tecnológicas puede preverse en los códigos de conducta, bien de manera expresa, bien de manera más indirecta y ambigua. Lo primero sucede cuando, por ejemplo, tras establecerse la prohibición de uso privado, se añade que el empresario puede autorizar ciertas excepciones o que cualquier uso privado debe sujetarse a la previa autorización de aquel o que, en fin, se prohíbe el uso particular de las herramientas de trabajo sin autorización previa del empresario[29]. Como muestra de un supuesto de mayor ambigüedad, cabe citar el código que enumera varios supuestos de conductas inaceptables por parte de los trabajadores y, entre ellos, se refiere al “uso personal no autorizado” de las herramientas informáticas, lo que permite interpretar, *a contrario sensu*, que el empresario puede autorizar algunos supuestos.

La autorización es competencia del empresario, quien puede ejercerla directamente o delegarla en otra persona adecuada, como un director de sección o de recursos humanos. Aunque los códigos no suelen aportar datos sobre el procedimiento de solicitud de esta autorización de uso privado, lo que podría indicar que es algo informal, cabe recomendar que la solicitud del trabajador se haga por escrito, indicando con precisión el supuesto de uso particular para el que pide autorización, lo que requiere, por ejemplo, describir el bien o herramienta empresarial que se desea utilizar (por ejemplo, teléfono de la empresa, ordenador personal, correo electrónico o la red corporativa), el fin de ese uso (v. gr., para llamadas familiares o mensajes privados), su previsible frecuencia de utilización (diaria, mensual o anual), el tiempo empleado en ello o, en fin, el impacto en la empresa. Asimismo, es importante motivar la solicitud del referido uso, alegando las razones que podrían ampararlo, las cuales deben estar relacionadas con las circunstancias ya apuntadas.

De igual manera, resulta aconsejable que la respuesta empresarial se notifique por escrito para quede constancia de esta y, en su caso, preconstituir prueba del alcance del uso autorizado, en cuanto a su dimensión material (actos concretos permitidos) y temporal (una o varias veces o con carácter indefinido). Si este uso se acepta para una determinada situación y ocasión en concreto, puede que, de repetirse la necesidad de aquel en el futuro, tenga que volverse a pedir la autorización.

De otro lado, cabe referirse a los códigos de conducta que dejan el uso privado de las Tics al criterio directo del trabajador, siempre que aquel sea un uso ‘responsable’, ‘correcto’ o ‘aceptable’.

El empleo de tales conceptos jurídicos indeterminados puede llevar a valoraciones contradictorias sobre los límites de lo permitido en una misma situación. Repárese en que, en tales supuestos, el que primero tiene que decidir sobre la responsabilidad o corrección del uso privado es el propio trabajador y, después, el empresario, quien debe vigilar la conducta de aquel y decidir sobre su sanción en caso de entender que hay extralimitación en el referido uso. Por lo tanto, en este segundo supuesto, sería importante que el código entrase a delimitar con claridad y precisión esos conceptos jurídicos generales, por ejemplo, poniendo ejemplos concretos de lo permitido y lo prohibido, esto es, de lo que se considera uso correcto e incorrecto. Un buen ejemplo de concreción lo ofrece algún código de conducta al prever que el "eventual" uso personal de las Tics (el teléfono, el correo electrónico e Internet) se acepta expresamente siempre y cuando tal uso: a) no consuma mucho tiempo o recursos de la empresa; b) no interfiera negativamente con el desempeño laboral del trabajador o sus compañeros, lo que parece relacionarse con la nota anterior y apuntar hacia la idea de que el trabajador debe ser productivo durante la jornada laboral y dedicarse a la prestación laboral; c) no involucre material ilegal, sexualmente explícito, discriminatorio o de otro modo inadecuado, lo que se vincula con el necesario cumplimiento de la legalidad del ya visto punto uno; d) no se relacione con intereses comerciales externos, lo que parece querer evitar la competencia desleal y el daño económico a la empresa; y, en fin, e) no viole el código de conducta o cualquiera de las políticas de la empresa, lo que resulta redundante con la letra c)[30].

Ahora bien, en estos supuestos, en los que se deja a la voluntad del trabajador el decidir la corrección y oportunidad del uso privado, sería adecuado que el código especificase las condiciones a observar por el referido uso (las tres ya antes expuestas: excepcionalidad, justificación objetiva y no lesividad para la empresa). Asimismo, sería importante dejar claro si, en los casos de uso privado permitido, el trabajador goza de una expectativa de privacidad o no, siendo lo lógico lo primero. En tal caso, debería añadirse algún tipo de indicación sobre la clase y condiciones del control empresarial a realizar sobre ese uso privado de las herramientas. En fin, estos códigos que permiten un cierto uso privado de las Tics deberían ser todo lo explícitos y concretos que fuese posible, para evitar situaciones de incertidumbre y consecuencias no deseadas[31].

3) La referencia específica a algunas populares aplicaciones de comunicación social: el correo electrónico, las redes sociales, mensajería instantánea y blogs. En cuanto importante herramienta de comunicación social y de gestión laboral, que permite un rápido y eficaz tráfico de datos, la aplicación del correo electrónico suele tener especial atención en los códigos de conducta. Cuando se reserva exclusivamente para fines empresariales, se suele prever que la dirección interna de correo electrónico que se adjudica por el departamento de informática a cada empleado no se considera privativa de este, sino de la empresa. Esta cuenta de correo puede reservarse expresamente para "transmitir comunicados, partes de producción, permisos, bajas y la información que sea necesaria para el correcto desarrollo de las tareas y funciones asignadas"[32]. Desde tal punto de vista, se hace responsable al trabajador de no recibir correos particulares del exterior y ajenos al trabajo y, en su caso, de proceder a su inmediata destrucción, comunicando al emisor la improcedencia de tales envíos. De igual manera, el trabajador no puede usar el correo para enviar al exterior información de la empresa, sin consentimiento de esta. En tal sentido, la empresa puede establecer filtros en las direcciones de salida de los correos para evitar su uso indebido. Respecto del uso sindical del correo electrónico, como medio de comunicación entre los representantes y la plantilla, se suele remitir a lo acordado específicamente entre aquellos y la empresa.

En otro orden de cosas, en los últimos años también se empieza a regular el uso de las redes sociales y blogs. Sabido es que las redes sociales están adquiriendo progresivamente una mayor importancia en la empresa, en cuanto elemento estratégico de inmediata interacción con la sociedad y puesta en contacto con los consumidores y clientes de sus productos o servicios. En este sentido, algunos códigos dedican especial atención a las redes sociales, incluso pueden ser monográficos sobre este particular[33], y distinguen entre el uso corporativo y privado que los empleados puedan hacer de aquellas. El uso corporativo es el más exigente y delicado, pues debe ser autorizado por la propia empresa y observar sus requerimientos (v. gr., uso de logo oficial, emitir solo determinados contenidos u opiniones relacionados con la actividad profesional). En tal

supuesto, el uso de la red social forma parte de la actividad laboral del trabajador y de su jornada laboral, sin que pueda relegarse al tiempo de descanso de aquel, máxime ahora, tras la regulación del derecho a la desconexión digital, al que nos referiremos *infra*. Lógicamente, el empresario puede controlar la actividad desarrollada en la red social y, en su caso, adoptar las medidas disciplinarias que correspondan.

Por lo que respecta al uso privativo de las redes sociales, en principio, este es una decisión libre del trabajador. Con todo, los códigos suelen exigir que no se involucre a la empresa y se respeten sus intereses económicos. Esto último exige, por ejemplo, que no se use el correo electrónico corporativo para darse de alta o gestionar el perfil privado en la red social, no emitir opiniones o mensajes que puedan vincularse a la empresa ni usar los signos distintivos de esta, no facilitar datos de clientes ni vincular la posibilidad de la geolocalización del usuario de la red a la sede física de aquella[34]. De manera similar, se prevé que los trabajadores deberán abstenerse de utilizar las redes sociales, correo electrónico y medios de comunicación social para difundir información, realizar manifestaciones, utilizar expresiones o mostrar imágenes que puedan afectar de cualquier modo al prestigio y reputación de la empresa, o que puedan menoscabar o atentar contra el honor de sus profesionales, sus grupos de interés o terceros en general[35]. En esta línea, puede exigirse al trabajador que la información relativa a la empresa (si alguna), incluida en su perfil social, sea verídica y esté actualizada.

En supuestos más generosos, puede llegar a aceptarse un uso privativo de las redes sociales durante el tiempo de trabajo, siempre que sea moderado y responsable, siguiendo la regla del correo electrónico o de otras herramientas Tics. Como se aprecia, la preocupación empresarial es proteger los intereses de la compañía promoviendo la toma de conciencia del trabajador sobre la transcendencia que puede tener su participación -aun privada- en la red social, la responsabilidad que puede derivar de sus actos y, por ello, la necesidad de observar una conducta apropiada y respetuosa con aquellos intereses.

4) La declaración de la propiedad empresarial de los trabajos realizados en los equipos informáticos. Según la legislación específica aplicable, la titularidad de los desarrollos informáticos, aplicaciones, textos, hojas de cálculo, bases de datos y otros documentos similares creados por los trabajadores, como consecuencia de las funciones propias de su puesto de trabajo en la empresa, con los medios de esta y dentro de la jornada de trabajo, corresponde a aquella. La legislación sobre propiedad intelectual y derechos de autor protege los programas informáticos. Por ello y como norma general, no deberán efectuarse copias de *software*, excepto si son de seguridad. Igualmente, tampoco deben efectuarse copias de programas informáticos de desarrollo interno, salvo en la medida en que sean necesarias para su explotación[36].

5) Tras la aprobación de la reciente y ya citada LOPDYDD, un contenido nuevo que el empresario debe incorporar a los códigos de conducta (u a otro documento similar) es el relativo al ejercicio del derecho a la desconexión digital de los trabajadores. Como ya se expuso, el art. 88 de la mencionada Ley reconoce expresamente -aun sin ser necesario- tal derecho a fin de garantizar (al margen de la jornada laboral) el respeto del tiempo de descanso, permisos y vacaciones, así como la intimidad personal y familiar de aquellos. A efectos de regular las modalidades de ejercicio de este derecho, se debe apuntar, en primer lugar, a la negociación colectiva o, en su defecto, al acuerdo entre la empresa y los representantes de los trabajadores. Ahora bien, con independencia de tal regulación colectiva, y a modo de complemento, "el empleador, previa audiencia de los representantes de los trabajadores, debe elaborar una *política interna*" dirigida a los trabajadores, en la que se concreten también esas modalidades de ejercicio del derecho a la desconexión y se incluyan las acciones de formación y de sensibilización de aquellos sobre un uso razonable de las herramientas tecnológicas. Esta obligación empresarial de cuidar la salud de los trabajadores y prevenir los riesgos laborales relacionados con el abuso de las Tics y la reducción del descanso necesario (v. gr., fatiga informática, tecnoestrés o tecnoadicción) debe alcanzar a todos los trabajadores, incluidos los directivos y los que prestan servicios a distancia (teletrabajadores o no). Ciertamente, el hecho de que estos trabajen fuera del centro de trabajo no debe llevar al empresario a omitirlos en sus políticas de protección, pues se trata de un colectivo de alto riesgo, en cuanto el uso de las herramientas informáticas se halla presente durante la mayor parte de la jornada laboral. En fin, esta mención legal a los trabajadores a distancia resulta positiva, pues

sirve para complementar la referencia general a su derecho a la seguridad y salud, contenida en el art. 13.4 ET.

3.3. Sobre el control empresarial del correcto uso de las Tics (por los trabajadores) en los códigos de conducta

Generalmente, los códigos de conducta suelen indicar, de forma expresa, que la empresa puede impulsar medidas de supervisión y control para constatar la adecuada utilización de las Tics dentro de lo permitido (v. gr., exclusivo uso profesional o privado limitado, contenido emitido o recibido, destinatarios contactados, etc.). Así pues, este control de contenido o fondo sobre la actividad del trabajador en la red o la utilización de los medios informáticos es ajeno al examen meramente técnico que pueda hacerse sobre tales instrumentos. Dicho control puede preverse con *carácter puntual o periódico*. En ocasiones, este control periódico se establece para los casos más extremos, en los que hay una prohibición absoluta de uso privado de las herramientas informáticas. Así, con objeto de asegurar "el correcto funcionamiento de los sistemas de información, y con el fin de evitar cualquier tipo de abuso o utilización fraudulenta de los mismos, la empresa se reserva el derecho de monitorizar y analizar, periódicamente, todos los equipos y sistemas puestos a disposición de sus empleados"[37]. Ahora bien, ese control cíclico también puede establecerse para verificar los usos privados permitidos.

En el caso de que se prevea un control puntual, este no suele estar previamente fijado, sino que lo habitual es que se active ante la aparición de circunstancias que así lo justifiquen, como puede ser la existencia de indicios de una extralimitación en los usos permitidos. En este sentido, en ocasiones, se apunta expresamente que, aunque por lo general, no se controla el uso que el empleado hace de las Tics (correo electrónico, teléfono, correo de voz, Internet y demás sistemas informáticos), la empresa "se reserva el derecho a hacerlo cuando aprecie indicios suficientes" que así lo aconsejen[38]. De este modo, aquella podrá acceder a los equipos y sistemas correspondientes, así como al correo electrónico corporativo "de forma extraordinaria", bien con motivo de verificar el correcto uso de los recursos informáticos, bien por motivos de continuidad de negocio[39]. O, en otros términos, que, en caso de que sean detectados "mensajes inadecuados" relacionados con el uso del correo electrónico, la empresa "se reserva la facultad de iniciar una investigación y establecer las medidas que considere pertinentes"[40].

Desde el punto de vista subjetivo, el control puede ejercerse, no solo sobre los trabajadores que presentan indicios de extralimitación en el uso permitido, sino también sobre cualquier otro, como sucede cuando aquel control se hace con carácter aleatorio[41]. Además, en cuanto a su situación contractual, todo trabajador puede ser investigado, tanto si es presencial y utiliza los recursos informáticos en el centro de trabajo, como si es a distancia, y presta servicios en la modalidad de teletrabajo o desde cualquier otro acceso externo[42].

Estos indicios o sospechas de conducta irregular también pueden ser puestos en conocimiento de la empresa por compañeros de trabajo o terceros (clientes, proveedores u otros colaboradores). A tal efecto, algunos códigos de conducta ya prevén un procedimiento de *denuncia anónima* (por ejemplo, dejando una nota en un buzón físico o ubicado en la web) de los posibles incumplimientos del código para conseguir la máxima observancia de lo allí dispuesto, a la vez que se protege al sujeto denunciante. A partir de la recepción de la denuncia, la empresa valora su veracidad y, de ser esta alta, puede decidir poner en marcha medidas adicionales de control y, en su caso, una posible sanción al trabajador incumplidor. Sobre este particular, algún código de conducta dispone expresamente que la empresa valorará "seriamente" y analizará, "de forma inmediata", "todos los informes de supuestas violaciones del código", adoptando las decisiones que correspondan a la vista de los resultados de la investigación[43]. En estos supuestos de denuncia anónima, incluso puede preverse la intervención de una comisión interna encargada de la instrucción de un procedimiento de investigación para determinar la realidad de la denuncia, como típicamente sucede en los códigos o protocolos de lucha contra el acoso sexual o moral. En función de su nivel de detalle, los códigos de conducta pueden entrar a especificar el papel y modo concreto de actuación de los instructores y el comportamiento esperado del trabajador investigado. Respecto de los primeros, al igual que cuando es el empresario el que realiza la supervisión, se exige una actuación objetiva e imparcial, que respete los derechos de información,

defensa y contradicción del posible sujeto incumplidor. El procedimiento de investigación puede incluir entrevista personal a este y al denunciante, así como la aportación y examen de pruebas documentales, testificales o de otro tipo, según proceda. El trabajador investigado debe colaborar plenamente con la investigación abierta, sin incurrir en conductas obstaculizadoras o dilatorias, a la vez que podrá defenderse como estime conveniente. Finalmente, si el control realizado evidencia una extralimitación por parte del trabajador, la comisión instructora puede proponer las medidas que considere adecuadas para corregir el abuso, evitar su repetición y reparar sus consecuencias a los sujetos afectados, según las conclusiones alcanzadas.

Las medidas de supervisión y control pueden llevarse a cabo directamente por la empresa o encargarse al personal informático especializado[44], como suele suceder cuando la medida consiste en la revisión periódica de los correos electrónicos enviados y recibidos por el trabajador, la instalación de programas de captura periódica de pantalla, el registro de la navegación por Internet a través del análisis de los discos duros u otros sistemas de almacenamiento de información, el establecimiento de alertas informáticas o una auditoría interna que requiere el acceso completo y detallado a los registros telemáticos.

En aras de la seguridad jurídica, a veces el código de conducta aporta reglas específicas sobre el procedimiento o forma concreta de realización del control, especificando que, por ejemplo, este se lleve a cabo desde el puesto de trabajo del trabajador, en presencia de este y, de ser posible, un representante legal, a efectos de acreditar el respeto de sus derechos. En alguna ocasión, el código de conducta somete la validez del control empresarial a la previa autorización de un órgano específico de la empresa (denominado, por ejemplo, comité ético o comisión ética), que actúa como órgano independiente y en aras de la defensa de la legalidad vigente y el mutuo interés de las partes del contrato[45]. Dicho órgano puede limitarse a la autorización y supervisión del control empresarial o asumir un papel más activo, como cuando hay, por ejemplo, una previa denuncia de incumplimiento del código por un trabajador, como ya se vio. En todo caso, el titular del poder disciplinario es el empresario, por lo que solo él puede adoptar las sanciones disciplinarias que estén previamente tipificadas, sin quedar vinculado por ninguna comisión u órgano interno o externo a la empresa.

Por lo demás, cabe referirse al control empresarial en aquellos códigos que establecen un uso profesional exclusivo de las herramientas digitales. Aquellos buscan reforzar ese uso profesional de dos maneras; por un lado, con una regulación contundente sobre el poder de vigilancia empresarial. Así, es fácil encontrar cláusulas relativas a la reserva que la empresa se hace a sí misma de “la posibilidad de controlar, inspeccionar y acceder” a los dispositivos electrónicos y cuentas de correo, previo requerimiento y autorización de la Dirección del Grupo, con el fin de: 1) comprobar el correcto uso de las comunicaciones electrónicas, 2) verificar la información transmitida en la red, y 3) acceder a los expedientes electrónicos, datos y archivos localizados en los dispositivos y ordenadores, facilitados por la compañía[46].

De otro lado, estos códigos suelen pronunciarse sobre la falta de expectativa de privacidad del trabajador. Así, por ejemplo, se añade que la información contenida en los recursos tecnológicos e informáticos puestos a disposición de los trabajadores (por ejemplo, ordenador, correo electrónico o redes sociales corporativas) será considerada “profesional y, en ningún caso, privada o personal, pudiendo acceder la compañía a la misma a los efectos de realizar los controles que resulten proporcionados y convenientes para comprobar su buen uso” (y siempre con respeto a la legalidad vigente y a las buenas prácticas). Por lo tanto, se añade que aquellos no pueden “albergar ninguna expectativa razonable de privacidad” en relación con la utilización y contenido de los referidos recursos[47]. En esta línea, parece que solo la aceptación de un cierto uso privado ampara la expectativa de privacidad o secreto en las comunicaciones del trabajador[48]. En otras palabras, la regla general sigue siendo el uso profesional de los instrumentos de trabajo y el empresario debe poder vigilar y comprobar que aquella es respetada.

3.4.La valoración del control empresarial establecido en los códigos de conducta a la luz de la reciente normativa y jurisprudencia

La legalidad de las cláusulas de los códigos de conducta (y convenios colectivos) relativas al control

empresarial del uso de las herramientas digitales depende de la observancia de lo establecido en la normativa vigente en cada momento sobre protección de los derechos individuales de las personas. El propio código suele recordar la obligación empresarial de respeto de los derechos fundamentales del trabajador, especialmente el de su intimidad, secreto de comunicaciones y protección de datos personales[49]. En este punto, resulta de interés analizar, también, la posición de la jurisprudencia reciente (española e internacional) para ver en qué medida los códigos de conducta se adaptan a la misma, así como establecer criterios claros a respetar por las partes negociadoras en el futuro. A la vista de esta normativa y jurisprudencia actuales, cabe efectuar las siguientes consideraciones generales.

1) Se refuerza la posibilidad de un uso privado de los dispositivos digitales facilitados por el empresario a los trabajadores. En este punto, el ya citado art. 87.3, párrafo primero, LOPDYDD prevé que deberán establecerse "criterios de utilización de los dispositivos digitales respetando, en todo caso, los estándares mínimos" de protección de la intimidad de los trabajadores, "de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente". Y, a continuación, se admite expresamente la mencionada utilización con fines privados. En este punto, resulta de interés referirse a una de las primeras sentencias del Tribunal Constitucional (STC) español -la número 241/2012, de 17 diciembre- que analizó el control empresarial sobre el uso de los instrumentos de trabajo digitales por parte de los trabajadores. En este caso, la mayoría de la Sala estima conforme a derecho el control del empresario consistente, por un lado, en el acceso a uno de los ordenadores de la empresa para comprobar si se había infringido su prohibición de instalar en aquel un programa informático de mensajería instantánea y, por otro, en la apertura de ficheros y posterior lectura de las conversaciones realizada por el responsable del servicio, ante los supervisores y los trabajadores que instalaron el programa.

Con todo, lo que ahora interesa es destacar el primer argumento del voto particular que se formula por dos magistrados[50] para rebatir la aparente razonabilidad de los argumentos del fallo. Así, este voto comienza cuestionando la legitimidad del carácter restrictivo de la decisión empresarial de prohibir el uso privado de las herramientas digitales. Se parte de que el art. 18.3 Constitución garantiza la libertad de las comunicaciones, no solo el secreto de las mismas, y por ello hay que empezar analizando la validez de la orden empresarial de prohibición del uso privado del ordenador, pues, por un lado, "el contrato de trabajo no incomunica al trabajador", o sea, no lo pone "en una situación de incomunicación hacia el exterior" y, por otro, el que el empresario sea el propietario de esas tecnologías de la información y comunicación no le da derecho a introducir "restricciones caprichosas" en su uso. En otras palabras, el voto discrepante parece admitir un *uso social privado* de las herramientas Tics propiedad de la empresa, que esta no puede prohibir injustificadamente. De igual manera, se pronuncia la STEDH de 5 septiembre de 2017, ya citada, cuando se refiere a la necesaria protección de las comunicaciones electrónicas privadas realizadas en el ámbito laboral, pues forman parte del "ejercicio de una vida privada social". A la vista de estos argumentos, parece imponerse un cierto derecho del trabajador a usar privadamente las herramientas digitales facilitadas por la empresa, siempre que ese uso privado sea excepcional y no cause perjuicio a la empresa. De ser así, parece que los códigos de conducta que se negocien en el futuro no podrán contener cláusulas que impongan un uso profesional exclusivo de dichas herramientas (como vimos en el apartado anterior) y prohíban todo uso privado.

2) Se fortalece el derecho fundamental del trabajador *a la intimidad personal y familiar*, incluso en situaciones en que este incurre en incumplimiento laboral. El reforzamiento del uso privado de las herramientas digitales está directamente relacionado con la mayor protección de ese derecho fundamental de los trabajadores vinculado a aquel uso (art. 18 Constitución española). El 87.1 LOPDYDD reconoce expresamente el derecho de los trabajadores "a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador", lo que debe entenderse en un sentido amplio, que abarque, por un lado, los derechos fundamentales al secreto de las comunicaciones y la protección de datos personales; y, por otro, se extienda al mayor número posible de situaciones.

Se conecta así con la posición del ya citado voto particular efectuado a la STC 241/2012, que defiende que el derecho fundamental al secreto de las comunicaciones del trabajador debe

entenderse desde un punto de vista formal y absoluto, esto es, con independencia de cuál sea el contenido de aquellas, y ante cualquier situación, incluso aquella que pueda constituir un incumplimiento contractual del trabajador a una orden empresarial, como sucede en el caso de autos. Cabe recordar que, en este, el empresario había prohibido a los trabajadores la instalación de programas informáticos en los ordenadores de la empresa. Dicha orden empresarial era de general conocimiento, por lo que no había expectativa razonable de privacidad o confidencialidad para el trabajador que hiciese un uso privado de aquellos. A pesar de ello, algunos trabajadores desobedecieron la orden e instalaron un programa para hablar de temas personales; además, actuaron de manera descuidada, pues, a pesar de que el ordenador era de uso común y carecía de contraseñas de acceso, aquellos no adoptaron ningún tipo de cautela para garantizar la privacidad de las conversaciones, por lo que podían ser leídas por cualquier que accediese al ordenador (como así pasó)[51].

Para el voto particular, el empresario puede sancionar este incumplimiento laboral de los trabajadores, pero, para hacerlo, no puede vulnerar el contenido de las comunicaciones, pues ello implicaría violar el contenido esencial del mencionado derecho fundamental al secreto de aquellas. Desde el momento que el empresario o un tercero no destinatario lee o conoce el contenido de la comunicación, esta última ya deja de ser secreta y la medida de control empresarial ya no supera el test de proporcionalidad al que debe someterse el control empresarial, como veremos *infra*. Y, además, ese mismo carácter absoluto del derecho fundamental al secreto de las comunicaciones protege su contenido esencial incluso cuando el trabajador que realiza la comunicación actúa descuidadamente y no hace nada para protegerla (comunicación privada en un ordenador común y sin clave de acceso). Pues quien abre -precisa el voto particular- un enlace o un archivo que sabe que contiene conversaciones ajenas actúa igual que quien abre una carta dirigida a otra persona y es hallada, por error, en su buzón.

Una posición similar, de refuerzo del derecho fundamental a la intimidad y secreto de las comunicaciones reconocido en el art. 8.1 del Convenio Europeo de Derechos Humanos, se halla en la Sentencia de la Gran Sala del TEDH de 5 septiembre de 2017, ya citada, que rectifica la anterior sentencia de la Sala cuarta del mismo tribunal (de 12 enero 2016) para defender aquellos derechos del trabajador incumplidor de una orden empresarial de no usar privadamente las herramientas digitales[52]. En efecto, en el caso de autos, el trabajador fue despedido porque incumplió la normativa interna de la empresa que prohibía el uso de recursos tecnológicos puestos a su disposición por el empleador para fines personales.

3) Se consolida la obligación de que el empresario facilite a los trabajadores una información previa y completa sobre los usos permitidos con las herramientas digitales y el posterior control a realizar. El trabajador debe estar debidamente informado sobre los límites de la utilización de aquellas herramientas y la capacidad de control del empresario sobre la misma, para tomar sus decisiones con pleno conocimiento, y evitar situaciones de indefensión. En este sentido, conviene seguir con el análisis de la ya citada STEDH de 5 de septiembre de 2017, que resulta clave en este punto[53]. En tal supuesto, el trabajador impugnó el despido en su país (Rumanía) y solicitó su nulidad por vulneración de su derecho a la intimidad y secreto de las comunicaciones. La demanda fue desestimada por entender el Tribunal interno que el empleador había actuado conforme a la normativa y el trabajador había sido avisado de los límites de uso de las herramientas digitales y la posibilidad de control de su actividad y, por ello, no tenía una expectativa razonable de privacidad. La Sala Cuarta del TEDH confirmó esta posición.

Sin embargo, la Gran Sala del TEDH concluye que, de los hechos probados, no puede entenderse acreditado que el trabajador hubiese sido informado adecuadamente sobre los extremos apuntados. La información adecuada requiere efectuarse: 1) de una determinada forma (clara y precisa, con en un lenguaje accesible) y por escrito, por ejemplo, en el código de conducta; 2) en un concreto momento, el anterior al inicio de la actividad laboral o, en su caso, de la entrada en vigor de la medida empresarial adoptada. En otras palabras, el acto informativo debe realizarse con anticipación suficiente para que el trabajador tenga tiempo de conocer las reglas de juego y atenerse o no a ellas conscientemente. Y 3) con un contenido y alcance determinados, de manera que se den datos suficientes para que el destinatario tenga un conocimiento completo de la situación. Esto implica que, cuando se trata de restringir y controlar el uso privado de las

herramientas informáticas, aquella información debe referirse claramente a: a) las limitaciones que van a regir en el uso privado de aquellas, incluida la confidencialidad de las comunicaciones que el trabajador efectúe con las mismas; es decir, el trabajador debe conocer con exactitud qué está permitido y prohibido; b) la extensión y naturaleza de la vigilancia a efectuar por su empleador, esto es, el alcance de aquella (número e intensidad de los controles) y el grado de intromisión en la vida privada del trabajador, debiendo indicar, en su caso, el posible acceso al 'contenido' de las comunicaciones realizadas en tiempo y lugar de trabajo; y c) el concreto procedimiento a seguir por aquel, lo que implica el conocer quién efectuará el control, cómo, cuándo y dónde se realizará y cuánto tiempo durará.

En esta línea, el reciente art. 87.3, párrafo segundo, LOPDYDD condiciona el acceso del empleador al contenido de los dispositivos digitales (respecto de los que se haya admitido su uso con fines privados) a que se hayan especificado, "de modo preciso, los usos autorizados" y establecido garantías para preservar la intimidad de los trabajadores, tales como, en su caso, "la determinación de los períodos en los que los dispositivos podrán utilizarse con fines privados". Adicionalmente, en el párrafo siguiente, se añade que "los trabajadores deberán ser informados de los criterios de utilización". A la vista de lo recién expuesto, será fundamental que los futuros códigos de conducta establezcan, con precisión, los usos permitidos y no permitidos a los trabajadores y el posterior control a desarrollar por el empresario. En caso contrario, aquellos podrían declararse nulos por causar indefensión al trabajador.

4) Se confirma que el control empresarial está sujeto al principio de proporcionalidad. En este punto, el ya citado art. 87.2 LOPDYDD establece que el empleador podrá acceder a los contenidos derivados del uso de los medios digitales facilitados a los trabajadores "a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos". En otras palabras, el control empresarial debe estar justificado por razones laborales.

Además, aun cuando el referido control procede y está justificado es necesario que supere el denominado test de proporcionalidad, establecido por la jurisprudencia constitucional española cuando se está ante limitaciones a los derechos fundamentales del trabajador (como el de intimidad, secreto de las comunicaciones o protección de datos de carácter personal). En efecto, la activación del referido principio exige que el mencionado control sea: 1) idóneo (juicio de idoneidad), esto es, que resulte adecuado y útil para conseguir el objetivo propuesto; 2) necesario o indispensable (juicio de necesidad), lo que implica que no exista otra medida más moderada o menos invasiva para conseguir aquel con igual eficacia; y 3) ponderado o equilibrado (juicio de proporcionalidad en sentido estricto), en cuanto del control realizado derivan más ventajas para el interés general que perjuicios sobre el bien o derecho fundamental en conflicto. En todo caso, quede claro que, con independencia de la superación de ese principio de proporcionalidad, la medida de vigilancia empresarial no puede nunca vulnerar el contenido esencial de aquel derecho, pues, de ser así, nunca resultaría admisible.

En el caso analizado en la Sentencia de la Gran Sala del TEDH de 5 de septiembre de 2017, cabe concluir que el control empresarial no fue razonable ni proporcionado. Aparte de que el trabajador no fue debidamente informado del alcance del control empresarial, se cuestiona la existencia del *juicio denecesidad* de tal acto, en cuanto se entiende que el empresario podría haber alcanzado el mismo fin de vigilancia de la actividad del trabajador con un método menos invasivo y lesivo de sus derechos fundamentales.

Cuando el empresario descubre el uso irregular del correo corporativo, y el trabajador lo niega, aquel procede a difundir una transcripción de los mensajes privados intercambiados por el sujeto incumplidor con sus familiares. Desde luego, tal lectura de esos mensajes privados y su posterior difusión no parecen actos absolutamente necesarios para probar la extra-limitación en el uso profesional de los medios informáticos, pues al empresario ya le constaba la actuación incumplidora del trabajador. En otras palabras, aquel realiza un acto de intromisión ilegítima en la privacidad de este al vulnerar el derecho al secreto de su comunicación privada, pues la lee y difunde siendo consciente de que lo era e innecesario para el fin perseguido. Como se aprecia, la Sentencia de la Gran Sala del TEDH hila muy filo a la hora de valorar todas las concretas

circunstancias del caso para proteger los derechos fundamentales del trabajador, lo que, finalmente, le permite concluir que ni el poder de control empresarial ni la sanción disciplinaria (el despido) impuesta al trabajador fueron razonables ni proporcionados.

A la vista de lo recién expuesto, resulta recomendable que los códigos de conducta hagan hincapié en que el control empresarial debe respetar el principio de proporcionalidad.

3.5. Incumplimiento del código de conducta y poder disciplinario del empresario

En previsión de que el trabajador no cumpla con lo dispuesto en el código de conducta, cabe preguntarse si es posible que el empresario incluya en este las posibles conductas sancionables y, adicionalmente, la concreta sanción a imponer a aquel. En tal caso, estas cláusulas del código deberían valorarse desde el punto de vista del principio de la *tipificación* de las faltas y sanciones que rige en cualquier ámbito sancionador, también en el laboral.

Como es sabido, dicho principio laboral exige que todas las conductas y sus posibles sanciones, estén tipificadas previa y expresamente para conocimiento general y, en definitiva, para aportar seguridad jurídica a las partes y, especialmente, al trabajador afectado. Dicha labor de tipificación corresponde a la ley y, en particular, al convenio colectivo, el cual, tradicionalmente, se ocupa de la materia disciplinaria con detenimiento (faltas, sanciones y procedimiento disciplinario). La norma estatutaria solo tipifica los incumplimientos contractuales culpables y graves o muy graves (según las circunstancias) que pueden ser objeto de la máxima sanción disciplinaria: el despido disciplinario (art. 54.2 ET), a la que vez que se limita a mencionar otra sanción: la suspensión de empleo y sueldo por razones disciplinarias [art. 45.1.h)]. Para el resto de las sanciones (por ejemplo, amonestación verbal o escrita, postergación para el ascenso, movilidad geográfica forzosa), habrá que estar a los listados de faltas que, habitualmente, se incluyen en los convenios colectivos aplicables a la empresa. Adicionalmente, estos convenios también pueden entrar a detallar, matizar o complementar los incumplimientos objeto del despido disciplinario, así como prever otras sanciones para faltas graves o muy graves (aparte de la del despido disciplinario) o precisar la intensidad de la sanción de suspensión de empleo y sueldo, algo que no hace el ET. Como se aprecia, el papel del convenio colectivo en materia disciplinaria es importante y los agentes sociales deberían ejercerlo con responsabilidad, precisando con detalle todas las conductas sancionables y las correspondientes sanciones, sin dejar vacíos legales que el empresario pretenda cubrir por la vía del código unilateral[54].

Es frecuente que estos códigos de conducta incluyan una mera referencia genérica a las consecuencias de la extralimitación en el uso laboral de los medios informáticos, sin entrar a detallar el nivel de gravedad de cada tipo de incumplimiento laboral ni su posible sanción o medida correctora, remitiendo, directamente, al régimen disciplinario vigente en la empresa de carácter convencional o legal. Así, algún código prevé expresamente que el uso indebido y no autorizado por el trabajador de las herramientas de la empresa genera un incumplimiento de los deberes laborales de aquel y puede ser considerado una transgresión de la buena fe contractual y abuso de la confianza respecto de las tareas encomendadas, por lo que la empresa podrá adoptar las medidas correctoras y disciplinarias necesarias, en proporción a la gravedad de la infracción[55]. De manera similar, algún otro código establece que el quebranto del deber de confidencialidad en el uso y tratamiento de datos, tanto de carácter personal como empresarial, será considerado un grave incumplimiento de las obligaciones laborales y podrá motivar la adopción de las referidas medidas correctoras[56].

De entrar el código de conducta a detallar las faltas y sanciones de los trabajadores, lo ideal es que lo dispuesto en este también se incluya en el apartado de “faltas y sanciones” del convenio colectivo[57], pues, en tal caso, la garantía de la tipificación legal quedaría garantizada y reforzada por su carácter *normativo*. Sucede así, por ejemplo, cuando la conducta del trabajador (en el supuesto, obtención irregular de información reservada) es contraria al código de conducta empresarial y, al mismo tiempo, al convenio colectivo aplicable, el cual la considera falta grave o muy grave sancionable con el despido[58]. Otro supuesto también óptimo es aquel en el que el código de conducta es negociado con los representantes de los trabajadores y concluido de mutuo acuerdo con estos, pues entonces lo pactado puede tener una naturaleza equivalente a la de un

convenio colectivo de empresa.

Ahora bien, cuando la conducta infractora del trabajador está prevista en el código interno, pero no en el convenio colectivo, y se desea imponer a aquel la sanción del despido disciplinario, resulta necesario que dicha falta pueda incluirse directamente en alguno de los incumplimientos tipificados en el art. 54.2 ET, lo que no resulta difícil en cuanto la mayoría están configurados en términos muy amplios y ambiguos, como el de la transgresión de la buena fe contractual o la indisciplina o desobediencia a órdenes dadas [letras d) y b)]. Con todo, queda claro que la necesaria tipificación legal (convencional o estatutaria) en materia sancionadora limita el papel del código de conducta empresarial en aquella, pues este puede entrar a precisar, matizar o adaptar ciertos tipos infractores a las peculiaridades de la empresa, pero no añadir otros nuevos y diferentes a los legales, los cuales, en su caso, serían nulos[59]. Esa labor de concreción resulta positiva, pues aporta seguridad jurídica a las partes, especialmente en los casos en los que lo previsto en el convenio colectivo se caracteriza por conceptos jurídicos indeterminados.

En el supuesto de que el código interno, concluido unilateralmente por el empresario, previese una sanción inferior en gravedad a la de la norma legal para el sujeto incumplidor, cabría preguntarse sobre la posibilidad de que aquel aplicase directamente este régimen sancionatorio legal (por ejemplo, despido disciplinario) en vez del del código previsto por él y más favorable al trabajador. En contra de la aplicación directa y preferente de la norma estatutaria, podría alegarse su carácter más lesivo para los intereses del citado sujeto, lo que parece oponerse a la filosofía y los principios de las normas laborales que buscan la mayor protección posible de la parte débil del contrato, así como la existencia de una declaración escrita de voluntad empresarial más específica y favorable para aquel (el código). Sin embargo, no cabe alegar la prevalencia de la norma unilateral interna con base en la citada filosofía tuitiva, que busca garantizar la protección del trabajador con la imposición de la menor sanción a su conducta incumplidora. El código interno no tiene el valor de una condición más beneficiosa de origen contractual que deba ser respetada por el empresario. Por ello, si la conducta del trabajador vulnera los deberes generales a que queda sometido conforme a la buena fe contractual, cabe la aplicación directa del régimen sancionador del ET, que se superpone al previsto en el código interno, siempre –claro es- que la sanción legal elegida se corresponda a la gravedad de la falta imputada y no existan comportamientos previos de tolerancia de esta por el empresario[60]. Ahora bien, si el código fuese negociado y concluido de mutuo acuerdo con los representantes, y tuviese el valor de norma jurídica (equivalente a un convenio colectivo de empresa), debería ser respetado por el empresario.

En fin, cabe añadir que, tras constatar la actuación incorrecta del trabajador, algún código prevé medidas adicionales a las estrictamente disciplinarias aplicadas sobre aquel, al disponer que la empresa se reserva el derecho a eliminar, sin previo aviso, el contenido de la actividad desarrollada por el sujeto en la herramienta de trabajo (correo electrónico o red social)[61]. Esta medida resulta lógica y acertada, siempre que la empresa tenga la certeza de la actuación incumplidora y la ilicitud de dichos contenidos.

4. Criterios de aplicación: difusión y observancia estricta

Una vez redactado, el código de conducta telemático debe darse a conocer, de manera fehaciente, a todos sus destinatarios, con el fin de aumentar la seguridad jurídica. Esta actividad de publicidad e información debe realizarse con carácter individual y general, lo primero requiere una notificación a cada uno de los sujetos que directamente quedan incluidos en su ámbito de aplicación subjetivo, y que habitualmente son los trabajadores de la empresa, incluidos los representantes legales y sindicales, aunque también pueden ser los proveedores, clientes y terceros contratantes o colaboradores. En este caso, la notificación debe ser escrita y directa, a la particular cuenta de correo electrónico u ordinario (carta), incluso con carácter certificado y acuse de recibo. Esta información también puede reiterarse por vía oral en la empresa, a modo de asambleas o charlas informativas.

La actividad de información de carácter general va dirigida a todo posible interesado, que, en

términos amplios, puede ser la sociedad en general, por ello, también se aconseja su difusión en medios abiertos y cuyos destinatarios son todos los ciudadanos, como, por ejemplo, la página web de la empresa u otra específica, una *newsletter* o boletín de noticias interno, un periódico o, incluso, un diario oficial. También se puede aumentar la difusión con su inclusión en un anexo del convenio colectivo u otro pacto de empresa.

Junto a la información, también es importante la actividad de *formación* a los interesados sobre los puntos más dudosos o complejos que puedan presentarse en relación con el manejo de las Tics y los posibles límites en el uso privado. En este sentido, el art. 88.3 LOPDYDD exige al empresario que, en la política interna de la empresa, incluya, aparte de las modalidades de ejercicio del derecho a la desconexión, las acciones de formación y sensibilización del personal sobre un uso razonable de las herramientas tecnológicas, con el fin de proteger la salud del trabajador. Adicionalmente, la actividad formativa puede centrarse en el manejo puramente técnico de las herramientas digitales y en la resolución de dudas. Sea como fuere, es importante que la empresa haga todos los esfuerzos necesarios para asegurarse que los destinatarios del código conozcan y comprendan perfectamente su contenido. En esta línea, algún código de conducta prevé expresamente que la empresa dará formación sobre el código a sus empleados vía *online*, si estos tienen acceso a Internet y correo electrónico. Como prueba de tal instrucción, los trabajadores formados *online* deben dar fe de haber leído y comprendido el código interno. Asimismo, aquellos deben certificar su cumplimiento, así como poner en conocimiento de la empresa cualquier conflicto potencial de intereses o cualquier otra causa que pueda excepcionar el cumplimiento del código. Ahora bien, la falta de colaboración por parte del trabajador para leer el código o avisar de cualquier duda o problema que surja no exime a aquel de la obligación de cumplirlo[62].

Una vez que la plantilla está informada y formada sobre el contenido del código de conducta, y, en su caso, una vez aclaradas las dudas o mejorada la redacción de alguna cláusula que pueda resultar confusa, es un buen momento para fijar su entrada en vigor. Por lo tanto, parece ideal que esta se posponga, con una *vacatio legis,* a un momento posterior a su difusión y puesta en conocimiento de los interesados. Una vez que está en vigor, como ya se apuntó, la empresa debe procurar mantener actualizado su contenido, en función de las necesidades y problemas que vayan surgiendo en la empresa, los continuos cambios que se producen en el ámbito de las Tics, las nuevas funcionalidades de las herramientas informáticas, así como de los criterios jurisprudenciales o legales que se puedan ir fijando en la materia, como recientemente ha ocurrido con la nueva LOPDYDD. En efecto, un código desfasado no solo no sería útil, sino que también podría causar problemas de aplicación. De efectuarse tal actualización, y producirse cambios en el texto, los interesados deben ser nuevamente informados y formados sobre los mismos. La actualización del contenido y la transparencia en la misma aumentan la seguridad jurídica, a la vez que sirven de recordatorio de la existencia del código y la necesidad de su observancia.

Una vez informados del código, su contenido debe ser observado estrictamente por los trabajadores, y, por su parte, el empresario debe estar atento y hacerlo cumplir, avisando a aquellos de las posibles consecuencias o adoptando las medidas que sean necesarias. De no hacerlo así, el contenido del código quedaría afectado por la conducta consentidora expresa o tácita del empresario. En efecto, en tal caso, la voluntad inicialmente manifestada en aquel, en cuanto al necesario respeto de unos límites en el uso de los instrumentos informáticos, quedaría superada por la posterior conducta de *tolerancia empresarial* sobre el particular. Una vez apreciada claramente esa tolerancia, esta juega a favor de los trabajadores y, en aras de su seguridad jurídica y de la buena fe contractual, el empresario ya no puede volver a exigir, unilateralmente y cuando lo estime conveniente, el cumplimiento del contenido más restrictivo de lo previamente establecido en el código. Sin duda, tal anárquica actuación vulneraría los derechos de los trabajadores, que no sabrían a qué atenerse, y, por ello, siempre que hay tolerancia empresarial respecto de una determinada conducta de los trabajadores, resulta necesario que el empresario la rompa o elimine antes de ejercer su poder disciplinario sobre aquellos. A la vista de lo recién expuesto, se aconseja una aplicación coherente, firme y uniforme de las cláusulas del código de conducta.

5. Conclusiones

1. El uso de las herramientas digitales en la empresa puede negociarse en un convenio colectivo o abordarse unilateralmente por el empresario en un código de conducta. Este código es un protocolo interno que puede formar parte de otro más amplio (por ejemplo, un protocolo de carácter ético) o, por el contrario, ser monográfico en la materia, denominado "código de conducta informática" o "código de conducta telemático".

2. Esta vía de autorregulación ha venido siendo una manera rápida y cómoda de que la empresa tuviese una regulación mínima sobre el uso de las herramientas digitales. Con todo, tras la reciente aprobación de la LOPDYDD y la jurisprudencia del TEDH, la importancia de esta autorregulación ha aumentado claramente. El legislador español se limita a reconocer los derechos fundamentales del trabajador (especialmente el de la intimidad) cuando este use las herramientas digitales en el ámbito laboral, pero los límites de dicho uso y la concreción del posterior control empresarial se deja a la voluntad de los agentes sociales o, en su defecto, del empresario. Así, el legislador impulsa, con claridad, la implicación de este en la elaboración de una política interna, en la que se establezcan los criterios de utilización de los dispositivos digitales (art. 87.3) u otros aspectos, como las modalidades de ejercicio del derecho a la desconexión (art. 88.3).

3. Esta actuación empresarial de elaboración de una política interna sobre el uso de las herramientas digitales recibe un impulso similar de la jurisprudencia europea, como la STEDH de 5 de septiembre de 2017 (caso Barbulescu). Tras distintas referencias al marco internacional protector de los derechos fundamentales, dicha Sentencia apunta a la especificidad de la relación laboral subordinada y a la necesidad de que los Estados y los agentes sociales fijen el marco de actuación legal o convencional en el que deberá desenvolverse la actuación laboral del trabajador. Ahora bien, se añade que, de no actuar aquellos, el empresario puede aprobar una regulación interna, que sea igualmente protectora de los intereses de los trabajadores, indicando, claramente, todas las limitaciones que se introduzcan en el uso privado de los medios tecnológicos y el concreto control empresarial a realizar. Otra sentencia del mismo Tribunal Europeo que deja clara la importancia de la existencia en las empresas de protocolos internos sobre uso de herramientas digitales es la de 22 de febrero de 2018 (caso Libert *versus* France).

4. Un sucinto análisis de algunos de los códigos de conducta revela que la regla general es la de que el uso de las herramientas digitales debe ser estrictamente laboral, prohibiéndose expresamente, en algunos de ellos, cualquier uso privado de aquellas. Con todo, tras la LOPDYDD, se refuerza la posibilidad de un uso privado de los dispositivos digitales facilitados por el empresario a los trabajadores, pues el ya citado art. 87.3, párrafo primero, admite expresamente dicho uso. En esta línea, parece confirmarse la doctrina del voto particular efectuado a la STC 241/2012, de 17 diciembre, que defendió un uso social privado de las herramientas Tics propiedad de la empresa, y que esta no puede prohibir injustificadamente. En el mismo sentido, se pronuncia la STEDH de 5 septiembre de 2017, cuando se refiere a la necesaria protección de las comunicaciones electrónicas privadas realizadas en el ámbito laboral, pues forman parte del "ejercicio de una vida privada social". A la vista de estos argumentos, cabe reconocer un cierto derecho del trabajador a usar privadamente las herramientas digitales facilitadas por la empresa, siempre que ese uso privado sea excepcional y no cause perjuicio a aquella. De ser así, parece que los futuros códigos de conducta no podrán contener cláusulas que impongan un uso profesional exclusivo de dichas herramientas.

5. Tras la aprobación de la reciente LOPDYDD, un contenido nuevo que el empresario debe incorporar a los códigos de conducta es el relativo al ejercicio del derecho a la desconexión digital de los trabajadores. El art. 88 de la mencionada Ley reconoce expresamente tal derecho a fin de garantizar el respeto del tiempo de descanso, permisos y vacaciones, así como la intimidad personal y familiar de aquellos. Esta obligación empresarial de cuidar la salud de los trabajadores y prevenir los riesgos laborales relacionados con el abuso de las Tics y la reducción del descanso necesario debe alcanzar a todos los trabajadores, incluidos los directivos y los que prestan servicios a distancia (teletrabajadores o no). Este reconocimiento legal -aun innecesario- es positivo y se espera que sirva para reforzar la protección de la salud del trabajador en los códigos

de conducta.

6. Otro aspecto importante del contenido de los códigos es el control empresarial de los usos permitidos de las herramientas digitales. Se consolida la obligación de que el empresario facilite a los trabajadores una información previa y completa sobre los usos permitidos con las herramientas digitales y el posterior control a realizar. El trabajador debe estar debidamente informado sobre los límites de la utilización de aquellas herramientas y la capacidad de control del empresario sobre la misma, para tomar sus decisiones con pleno conocimiento, y evitar situaciones de indefensión. La importancia de esta información previa queda puesta de manifiesto tanto en la ya citada STEDH de 2017 como en la nueva normativa española de protección de datos y derechos digitales.

7. En fin, tras los recientes cambios legislativos y jurisprudenciales, resulta claro que muchos de los códigos telemáticos deben ser renovados para cumplir con las nuevas exigencias de contenido y procedimiento. Respecto de este, resulta fundamental que el empresario cuente con la participación de los representantes de los trabajadores, dándoles la oportunidad de ser oídos durante la elaboración del código, pues, sin duda, el consenso es la mejor forma de garantizar su posterior observancia.

NOTAS AL PIE DE PÁGINA

1

Este trabajo es resultado del proyecto nacional de investigación del MINECO (España) titulado “Nuevas (novísimas) tecnologías de la información y comunicación y su impacto en el mercado de trabajo: aspectos emergentes en el ámbito nacional e internacional” (DER2016-75376-R), dirigido por la Prof. Lourdes Mella. También se enmarca en “la Red de excelencia: Red de estudio y difusión de las nuevas TICs en la empresa (DER2017-90700-REDT), de la AEI”. Los códigos de conducta citados en este trabajo están disponibles fácilmente en internet.

2

Aprobado por Resolución de la DGE de 15 de junio de 2015 y prorrogado por Resolución de 17 de julio de 2018, de la DGT, por la que se registra y publica el IV Acuerdo para el Empleo y la Negociación Colectiva.

3

STS de 21 septiembre 2015 (rec. casación núm. 259/2014).

4

“Este Tribunal en absoluto niega que voluntariamente puedan ponerse aquellos datos a disposición de la empresa, pues ello es algo incuestionable; es más, incluso pudiera resultar deseable, dado los actuales tiempos de progresiva pujanza telemática en todos los ámbitos. A lo que exclusivamente nos oponemos es que en el contrato de trabajo se haga constar -como específica cláusula/tipo- que el trabajador presta su «voluntario» consentimiento a aportar los referidos datos personales y a que la empresa los utilice en los términos que el contrato relata, siendo así que el trabajador es la parte más débil del contrato y ha de

excluirse la posibilidad de que esa debilidad contractual pueda viciar su consentimiento a una previsión negocial referida a un derecho fundamental, y que, dadas las circunstancias -se trata del momento de acceso a un bien escaso como es el empleo-, bien puede entenderse que el consentimiento sobre tal extremo no es por completo libre y voluntario".

5

El código ético de la empresa es un documento general que refleja la filosofía de esta como marca en el mercado y su compromiso ante los valores, políticas y principios democráticos de la sociedad. Actúa como un elemento de comunicación interna y externa, para que todo el mundo conozca la posición e imagen de la empresa como entidad social. En algún caso, el código se denomina dé ética y conducta, como en el caso de la empresa CEPSA.

6

El código de conducta es un documento más concreto y específico. Aunque puede incluir también los valores de la empresa, los vincula con los objetivos de la misma y los concreta en una *guía* que describe las conductas esperadas y prohibidas de los trabajadores respecto de una determinada materia (como las herramientas Tics); todo ello se suele completar con indicaciones concretas de cómo proceder en caso de incumplimiento por parte de aquellos. Como se aprecia, se busca la efectividad de cumplimiento a través de la concreción.

7

Por ejemplo, código de conducta para el uso de internet y del correo electrónico de Scotiabank.

8

La disposición final tercera de la LOPDYDG crea un nuevo art. 20 bis en el ET, denominado "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión", que deberá ser interpretado conforme a lo dispuesto en el referido Título X de la nueva Ley Orgánica.

9

De igual manera, la STEDH de 22 febrero 2018 (caso Libert *versus* France) también evidencia la importancia de los códigos informáticos en la empresa. Cfr., mi trabajo, "El control empresarial de los correos y archivos electrónicos del trabajador: valoración crítica de la reciente jurisprudencia nacional y europea", *RevistaDerecho de las Relaciones Laborales*, diciembre 2018.

10

Según el código de conducta de Abanlex, este código contiene "consejos de actuación y tendrá la consideración de guía orientativa que, en todo caso, deberá ser completada o suplida por el sentido común y la adecuada gestión reflexiva del caso concreto".

11

Código de conducta y buenas prácticas de Down Madrid. Capítulo II. 2.9.

12

Un ejemplo de código general es el código de conducta global de PepsiCo (de 1 octubre 2012). También, código de conducta del Grupo Sacyr.

13

El Código de conducta Informática (en adelante, CCI) de Goiko-Auto S.A.

14

Ibídem.

15

CC del grupo Cobra (de noviembre 2015). CC Abanlex, cit. ("las cuentas de correo de Abanlex (usuario [arroba] abanlex.com), así como el material, los ordenadores y demás equipos y sistemas informáticos que se faciliten al trabajador, son de uso exclusivamente profesional").

16

Código de conducta empresarial SCI, apartado 11.

17

Código ético de Endesa. También, CC empresarial de CSI, ya citado: "el personal se abstendrá, tanto en horario laboral como fuera de él, de usar los accesos a Internet proporcionados para realizar alguna de las siguientes acciones: 1) navegar por contenidos que no tengan relación directa con las funciones y tareas asignadas, incluyendo las páginas web de contenidos multimedia en línea. 2) Descargar archivos y /o aplicaciones que no estén justificados para el desarrollo de las funciones asignadas, como vídeo, música y juegos. 3) Conectar a grupos de conversación o actividad interactiva, como Chats, juegos en línea y foros de discusión. 4) Publicar contenidos o subir archivos para compartir en Internet".

18

CC del nuevo NH, ya citado.

19

CC empresarial de SCI ya citado. Apartado 1.1.5, código de conducta de Hiberus Tecnologías de la información, SL.: “La utilización de los equipos, sistemas y programas informáticos que Hiberus pone a disposición de los empleados para el desarrollo de su trabajo, incluida la facilidad de acceso y operativa en Internet, deberá ajustarse a criterios de seguridad y eficiencia, excluyendo cualquier uso, acción o función informática que sea ilícita o contraria a las normas o instrucciones de la empresa. Es decir, no se permite el uso de los equipos para utilizar programas o aplicaciones informáticas cuyo uso sea ilegal, que pueda dañar la imagen de Hiberus o su reputación, o para acceder, descargar o distribuir contenidos ilegales u ofensivos”.

20

Cfr. apartado 5.4: “Los empleados no utilizarán dichos recursos para usos personales o extra-profesionales y/o para el desempeño de actividades que no estén relacionadas directamente con el interés de la compañía o de otras empresas del Grupo SACYR, responsabilizándose asimismo de la protección de aquellos que le fueran confiados en relación con su trabajo, observando en su custodia el máximo cuidado”.

21

“Los activos de la empresa son para uso exclusivo de los empleados de la Organización, en el desempeño de su actividad laboral. No están destinados a un uso privado, por lo que la empresa se reserva el derecho de comprobar los contenidos de los mismos en el caso que se considere necesario”.

22

Art. 9: “Los empleados deben proteger los bienes de Nestlé y utilizarlos únicamente en forma adecuada y eficiente. Todos los empleados intentarán proteger los bienes de Nestlé contra pérdida, daño, uso incorrecto, robo, fraude, malversación y destrucción. Estas obligaciones cubren tanto a los activos tangibles como a los intangibles”, incluidos “los sistemas informáticos”.

23

Código de Conducta y Prácticas Responsables Grupo Inditex (julio 2012). Art. 4.10: “Los empleados de Inditex utilizarán eficientemente los bienes y servicios de la empresa y no harán uso de ellos en beneficio propio. A este respecto, los empleados de Inditex, en ningún caso, harán uso de los equipos que Inditex pone a su disposición para instalar o descargar programas, aplicaciones o contenidos cuya utilización sea ilegal, que contravengan las normas de la compañía o que puedan perjudicar su reputación”.

24

Apartado 4.3: “El correo electrónico, herramienta de comunicación de la empresa, debe ser utilizado para fines profesionales relacionados con el negocio. Los ordenadores y dispositivos electrónicos, así como las cuentas de correo electrónico que, en su caso, adjudica el Departamento de Sistemas a los empleados, no

están considerados como bienes privativos de estos", sino que son "propiedad de la empresa".

25

CC Huesa Water Technology (18 mayo 2018): "está prohibido usar el material, teléfonos móviles, herramientas, equipos informáticos (PC, internet, correo electrónico) para uso particular o beneficio propio o de terceros".

26

CC empresarial de CSI, ya citado: "se permitirá el uso privado de la cuenta de correo de la compañía de forma excepcional, no abusiva y circunstancial, a los efectos de atender asuntos inexcusables, que eviten la ausencia del puesto de trabajo o faciliten la conciliación de la vida familiar y laboral".

27

Código de conducta del nuevo NH (de 29 junio 2015); también CC de SCI: "la conexión a Internet se realizará únicamente mediante los accesos autorizados por los responsables de sistemas, siendo tolerado de forma excepcional para su uso privado, siempre que no se emplee abusivamente. El acceso a Internet a través de conexiones de datos incorporados a líneas asociadas a dispositivos móviles como teléfonos inteligentes, tabletas y similares, estarán sujetos a la misma norma que el resto de los accesos corporativos". También, Código de ética y conducta de Repsol (julio 2016): "la utilización de tales activos deberá mantenerse en niveles mínimos y sin afectar de manera negativa a la productividad y al entorno de trabajo".

28

CC Repsol, citado.

29

CC Huesa *Water Technology* (18 mayo 2018): "está prohibido usar el material, teléfonos móviles, herramientas, vehículos, equipos informáticos (PC, internet, correo electrónico) y resto de recursos de la empresa para uso particular o beneficio propio o de terceros sin autorización previa por parte de la Dirección".

30

Código de conducta global de PepsiCo, ya citado. Véase, también, apartado 3.5 CC BBVA; CC Scotiabank, que permite al trabajador "el uso personal razonable u ocasional de Internet y el correo electrónico mientras está trabajando". Como ejemplos de uso personal razonable u ocasional, se incluyen, entre otros: 1) controlar brevemente un correo electrónico personal, red social o cuenta de mensaje instantáneo (por ejemplo, durante la hora de almuerzo); 2) ingresar periódicamente a su cuenta de servicios bancarios por Internet o de corretaje; y 3) visitar sitios Web externos, como, por ejemplo, el pronóstico del tiempo, o

hacer rápidamente una compra en línea. En similar sentido, art. 5.7 Código de conducta de Acciona: "los equipos y sistemas informáticos de ACCIONA deben tener un uso exclusivamente profesional. No obstante, en aquellos supuestos en los que excepcionalmente se utilicen estos recursos para fines personales, su uso debe ser mínimo, razonable, adecuado y conforme al principio de buena fe contractual". Los recursos tecnológicos de ACCIONA no pueden utilizarse para: 1) emitir en nombre del grupo opiniones o acceder con igual objetivo a foros o redes sociales, salvo consentimiento expreso a tal efecto. 2) Almacenar o distribuir, ni visitar sitios de Internet con, material inapropiado que atente contra los derechos humanos, la intimidad, el honor, la propia imagen, la libertad religiosa; o contra la dignidad de las personas como racismo, xenofobia, apología de la violencia o del terrorismo, y material pornográfico o de apología sexista. 3) Usar, introducir, descargar, copiar, transmitir, reproducir, distribuir o almacenar cualquier tipo de software, obra editada o invención protegida por la propiedad intelectual o industrial sin la correspondiente licencia o autorización. 4) Realizar o participar en envíos masivos de correos electrónicos con cadenas de mensajes, bromas, o imágenes inapropiadas".

31

Cfr., en este sentido, GIL PLANA, J.: "El uso particular por los trabajadores de las nuevas tecnologías empresariales en los códigos de conducta", *REDT,* 2012, núm. 155 (BIB 2020/2800), pp. 37 y ss.

32

CC empresarial de SCI, ya citado.

33

Como ejemplo, cabe citar el código de conducta en redes sociales del Grupo Capgemini o el código de uso de las redes sociales para las empleadas y los empleados del Grupo Banco Sabadell (2011).

34

CCI Abanlex, cit. CC Banco Santander, art. 44.5: "la creación, pertenencia, participación o colaboración por los sujetos del código en redes sociales, foros o blogs en Internet, y las opiniones o manifestaciones que se realicen en los mismos, se efectuarán de manera que quede claro su carácter personal. En todo caso, los sujetos del código deberán abstenerse de utilizar la imagen, nombre o marcas del Grupo para abrir cuentas o darse de alta en estos foros y redes".

35

CC del nuevo NH, ya citado. También Código ético de Endesa, ya cit., no se pueden "enviar mensajes de correo electrónicos amenazantes o injuriosos, no recurrir a lenguaje improcedente, no realizar comentarios inapropiados que puedan suponer una ofensa a una persona y/o un daño a la imagen de la empresa". En igual sentido, CC empresarial de SCI, ya citado ("no se permitirá el uso de la cuenta de correo electrónico para enviar mensajes con contenidos ofensivos, poco éticos, amenazadores, discriminatorios o injuriosos. Del mismo modo, no se admitirá la difusión de correos no deseados, spam, virus ni cualquier

otro que contenga código o enlaces maliciosos, así como mensajes en cadena o de envío masivo que no guarden relación directa con las tareas y funciones encargadas") y CC Sareb de 21 diciembre 2017 (Sociedad de Gestión de Activos Procedentes de la Reestructuración Bancaria, S.A.) ("la creación, pertenencia, participación o colaboración por los Empleados en redes sociales, foros o "blogs" en Internet y las opiniones o manifestaciones que se realicen en los mismos, se deben efectuar de manera que quede claro su carácter personal, evitando emitir opiniones sobre Sareb ni en su nombre).

36

CCI de Goiko-Auto, cit.

37

Apartado 5.4 código de conducta del Grupo Sacyr, ya citado.

38

CC de PepsiCo, ya citado.

39

Código de Conducta del Grupo Mediapro (noviembre 2017).

40

CC empresarial de SCI, ya citado.

41

CC KH Lloreda, ya citado.

42

Código de ética profesional del Grupo Bankinter, apartado 4.2.

43

CC global de PepsiCo, ya citado.

44

Art. 4.10 CC Grupo Inditex: "Los empleados deben conocer que los documentos y datos contenidos en los

sistemas y equipos de tecnologías de la información de Inditex pueden estar sujetos a revisión por parte de unidades competentes de la compañía, o por terceros designados por ésta, cuando así se considere necesario y esté permitido por la normativa en vigor".

45

CC de Down Madrid, ya citado.

46

CC de Laviuda.

47

CC del nuevo NH, ya citado. CC empresarial de Nestlé, art. 9: "en la medida permitida por la legislación aplicable, la Compañía se reserva el derecho a controlar e inspeccionar el modo en el que los empleados utilizan sus activos", incluido "todos los correos electrónicos, datos y archivos mantenidos en la red de computadoras de la Compañía".

48

CC de Down Madrid, ya citado. Según el art. 4.2 Código de ética profesional del Grupo Bankinter: "La información almacenada o registrada por el empleado en servidores, medios o sistemas de propiedad del Banco, podrá ser objeto de acceso justificado por el Banco".

49

Por ejemplo, apartado 5.4 Código del Grupo Sacyr, ya citado: con objeto de asegurar "la empresa se reserva el derecho de monitorizar y analizar periódicamente todos los equipos y sistemas puestos a disposición de sus empleados, dentro del marco de lo establecido en la normativa vigente en cada momento sobre protección de derechos individuales de las personas".

50

Valdés Dal-Ré y Asúa Batarrita.

51

Cfr., también, STC 170/2013, de 7 octubre, que avala la legalidad del control empresarial sobre la cuenta de correo electrónico corporativa utilizada por el trabajador y la no vulneración de sus derechos a la intimidad y al secreto de las comunicaciones. En el caso de autos, se declara la legalidad de dicho control en atención a: 1) la existencia de una prohibición expresa de uso privado de las herramientas informáticas en el convenio colectivo aplicable, que configura dicha conducta como falta laboral sancionable; 2) la

inexistencia de tolerancia empresarial previa en dicho uso, por lo que el trabajador no puede alegar una expectativa razonable de privacidad o confidencialidad de las comunicaciones realizadas; 3) la existencia de fundadas sospechas de un uso irregular de aquellas (revelación de secretos de la empresa a terceros), y 4) la supervisión notarial del control empresarial del ordenador, realizado por medio de un perito informático.

52

Cfr. ROJO TORRECILLA, E.: "De Barbulescu I a Barbulescu II. La Gran Sala del TEDH refuerza la protección del trabajador frente al control y vigilancia de las comunicaciones electrónicas en el ámbito laboral por parte empresarial". Entrada 14 septiembre 2017.

http://www.eduardorojotorrecilla.es/2017/09/de-barbulescu-i-barbulescu-ii-la-gran.html

---

53

Cfr., también, STEDH de 22 febrero 2018, ya citada.

54

Según MORATO GARCÍA, R. Mª, "una estrategia autorreguladora que tenga como propósito limitar el papel de la negociación bilateral, restando competencias a las relaciones negociales con los representantes de los trabajadores, será claramente contraria a las competencias que al convenio le atribuyen la Constitución y las leyes laborales" *[Incumplimiento de los códigos de conducta y potestad disciplinaria del empresario,* en el volumen "Ética empresarial y códigos de conducta" (Madrid, 2011) (La Ley 15114/2011), p. 9].

55

CCI del grupo Cobra, cit.

56

CCI de Goiko-Auto, cit.

57

CAMÓS VICTORIA, I., "Despido disciplinario e incumplimiento del código de conducta de la empresa. Comentario a la Sentencia del TSJ de Castilla-La Mancha de 9 febrero 2017", *Iuslabor* 2/2017.

58

STSJ Castilla-La Mancha de 9 febrero 2017 (rec. núm. 1697/2016).

59

Art. 115.d) Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social.

60

Véase, por analogía, la STSJ Cataluña de 2 febrero 2011 (rec. núm. 4625/2010), relativa a un caso en el que el código interno sanciona una conducta del trabajador (compra de vehículos en el concesionario en el que se trabaja con descuento para revenderlos por su cuenta de forma inmediata) con la obligación de devolver el importe del descuento del que se había beneficiado e imposibilidad de adquirir otro coche durante dos años. Sin embargo, la empresa aplica directamente el art. 54 ET e impone el despido al trabajador, cuya procedencia es ratificada por el Tribunal *ad quem* por estarse ante una conducta contraria a los especiales deberes de conducta que debe presidir la correcta ejecución del contrato.

61

CC de PepsiCo, ya citado.

62

CC de PepsiCo, ya citado.