

**ENTREVISTA DE LA UNIVERSIDAD INTERNACIONAL DE LA RIOJA AL FISCAL JOSE DIAZ CAPPA SOBRE
ALGUNOS ASPECTOS DE LA FUTURA REFORMA DEL CÓDIGO PENAL EN MATERIA DE
CIBERDELINCUENCIA**

¿Qué opinión le merecen los tipos penales que recoge en la actualidad el Código Penal para perseguir la Ciberdelincuencia?

Si hay una característica específica de lo que viene llamándose ciberdelincuencia (o criminalidad informática, que quizás sea el término más usual en el ámbito de la Administración de Justicia) es el de ser una especialidad que viene marcada por contener referencias, más que a tipos penales concretos, a aspectos de los mismos que sirven de medio para la comisión de algún hecho delictivo. Esta circunstancia supone, por un lado, que los tipos penales que pudiéramos considerar específicamente como propios de la especialidad serían muy pocos, pero, por otro, que prácticamente todos los tipos penales recogidos en el Código Penal o leyes penales especiales pueden, a su vez, tener algún contenido concreto propio de la materia que podría suponer su consideración como “ciberdelito”.

En este sentido, y siguiendo los criterios que, al respecto, se marcaron en la Instrucción 2/2011 de la Fiscalía General del Estado, recogiendo, sin duda, las directrices básicas del Convenio de Budapest sobre Ciberdelincuencia, podemos considerar que los tipos penales actuales en la materia se dividirían en, por un lado, aquellos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs (como el delito de daños, sabotaje informático o los ataques de denegación de servicios, o el acceso sin autorización a datos, programas o sistemas informáticos previstos en los artículos 264 y concordantes y 197.3 del Código Penal); por otro, aquellos delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs (entre los que destacarían las llamadas “estafas informáticas” de todo tipo –phising, pharming, etc.-, los delitos referidos al abuso sexual de menores, -como el *childgrooming* o la pornografía infantil-, o los delitos contra la propiedad intelectual derivados principalmente de la descarga en la Red de contenidos protegidos por aquella); y, finalmente, aquellos otros tipos penales en los que la actividad criminal, además de servir para su ejecución de las ventajas que ofrecen las TICs, entraña una especial complejidad en su investigación que demanda conocimientos específicos en la materia, en cuyo ámbito podríamos encuadrar prácticamente cualquier infracción penal para cuya investigación o instrucción fuera necesario analizar algún elemento informático de especial trascendencia o importancia (por ejemplo, falsificaciones, amenazas, coacciones, *ciberbullying* (delito contra la integridad moral), apología o incitación a la discriminación o al odio, o incluso genocidio, a través del uso inadecuado de las redes sociales, como medio más frecuente.

Teniendo en cuenta tales premisas, podría afirmarse que con los tipos penales actuales, cualquier clase de conducta delictiva realizada a través de medios informáticos, de Internet o de las TICs en general, ya tendría una ubicación adecuada en el Código penal actual sin necesidad de una reforma específica.

Ahora bien, es evidente que el principio de seguridad jurídica es absolutamente esencial en Derecho Penal, y ello conlleva la necesidad de ajustar y perfilar los tipos penales para, por un lado, impedir que una supuesta indefinición legal no interpretable jurisprudencialmente pueda acabar en una ausencia real de tipificación de alguna conducta reprochable penalmente, no tanto como ciberdelito en sí cuanto como delito en sí misma, debido simplemente a la falta de alguna precisión técnica propia del ámbito informático, y, por otro, para conseguir que, considerada como tal esa conducta, la misma no deje margen de arbitrariedad en caso de acusación y condena.

Atendiendo a ello es evidente que, tanto los tipos penales antes relatados como propios de la llamada ciberdelincuencia, como los que lo son por referencia o tangencialmente relacionados con aquellos, dan respuesta en la actualidad a los principales acometimientos delictivos a los bienes jurídicos protegidos penalmente ante los ataques informáticos, y, fundamentalmente ante los accesos ilícitos, interceptaciones ilícitas e interferencias en datos y sistemas si bien, como comenté, siempre es necesaria, o al menos conveniente, su actualización, su adecuación social y la matización de su contorno jurídico legal para la salvaguarda de la seguridad jurídica, circunstancias que bien podrían justificar algunos aspectos de la reforma legal que se pretende, tanto más en una especialidad que se mueve, precisamente, en un campo en constante y rápida actualización y en un marco de gran calado técnico e innovador, del que el mundo jurídico no puede quedar descolgado.

En todo caso, una cosa es evidente, de ser necesaria una reforma, esta lo es, sin duda, más que en el plano sustantivo de modificación del articulado de las posibles infracciones penales, en el ámbito procesal y en el de colaboración policial y judicial, tanto en el ámbito estatal interno como, y sobre todo, en el marco internacional.

¿Era necesaria una reforma?

Como he comentado, la reforma que se pretende, en lo que al Código Penal se refiere, salvo en algunos aspectos concretos, más que necesaria podría considerarse conveniente u oportuna. Insisto en que la reforma procesal, tanto interna como a nivel internacional es la realmente obligada, como luego comentaré. En todo caso es de destacar que siempre es plausible, e incluso obligatoria, una reforma que suponga la transposición al ordenamiento jurídico interno de normativas internacionales, cual lo hace la que ahora está en trámite, constatando, al final de su contenido, que mediante la misma se incorporarían al Derecho español elementos normativos tan importantes como la Decisión Marco 2008/675/JAI, de 24 de julio de 2008, relativa a la consideración de las resoluciones condenatorias entre los Estados miembros de la Unión Europea con motivo de un nuevo proceso penal; la Decisión Marco 2008/913/JAI, relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho Penal; la Directiva 2009/52/CE, por la que se establecen normas mínimas sobre las sanciones y medidas aplicables a los empleadores de nacionales de terceros países en situación irregular; la Directiva 2011/93/UE, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil; o la Directiva 2011/36/UE, de 5 abril de 2011, relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas.

En todo caso, y haciendo una somera referencia a los principales aspectos de la reforma en marcha, podría destacar como especialmente importantes, los referidos a las modificaciones en los delitos contra la libertad sexual mediante la transposición de la Directiva 2011/93/UE, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores, que obliga a los Estados miembros a endurecer las sanciones penales en la materia; asimismo, la punición de los actos de producción y difusión, e incluso la asistencia a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas discapacitadas, o el mero uso o la adquisición de pornografía infantil, o la sanción a quien acceda a sabiendas a este tipo de pornografía por medio de las TICs; en parecido sentido, aparece adecuada lo que vendría a ser una “ampliación” de la tipificación actual del llamado *childgrooming* del actual art 183 bis, mediante la tipificación en un nuevo precepto de numeración *ter* de la conducta consistente en contactar a través de medios tecnológicos con un menor de dieciséis años y realizar actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas.

José Díaz Cappa. Fiscal.
Delegado de Criminalidad Informática.

www.josediazcappa.es
jose.diaz@fiscal.es

Adecuada creo que es también la consideración como tipo agravado de la utilización en estos hechos de menores de dieciséis años, que, en la actualidad, aparece en el límite de trece años. Si bien esta última edad es coincidente con otras atendida la media de edad actual en el inicio de las relaciones sexuales, es evidente que la protección del menor, y, fundamentalmente la protección penal del menor ante los ataques a su libertad sexual por adultos, hace necesaria dicha modificación legal.

Polémico será, sin duda, el nuevo articulado en el que se consideran como pornografía infantil las imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales. El concepto de "imágenes realistas", trascendente a aspectos como el cómic, el dibujo artístico o similar, precisará, sin duda, de una adecuada interpretación y adecuación a la posibilidad de su consideración delictiva.

También me parece destacable, en el ámbito de la mayor protección de la intimidad, la tipificación del descubrimiento y revelación de secretos en los casos en que las imágenes o grabaciones de otra persona se han obtenido previamente con su consentimiento, pero son luego divulgados contra su voluntad, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión, sin el consentimiento de la persona afectada, lesione gravemente su intimidad.

En el ámbito de la protección de la propiedad intelectual destacaría, sin duda, por su necesidad, la tipificación, con determinadas condiciones, de la conducta consistente en la facilitación del acceso o la localización de obras o prestaciones protegidas ofrecidas ilícitamente en Internet, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. Con el texto penal actual han sido muchas las conductas que, salvo que se permitieran las llamadas "descargas directas", dejaban al margen de la tipificación penal el aprovechamiento claramente (y altamente) lucrativo por parte de muchos administradores de páginas web en las que su único contenido era la facilitación del acceso y contenido a páginas de enlace claramente vulneradores de los derechos de propiedad intelectual. Y en todo caso, correcto parece también el dejar al margen de la conducta delictiva a quienes desarrollen actividades de mera intermediación técnica, como puede ser, entre otras, una actividad neutral de motor de búsqueda de contenidos o que meramente enlacen ocasionalmente a tales contenidos de terceros, cual ocurre normalmente con los navegadores o buscadores en Internet.

Igualmente oportuna parece la introducción como delito de la conducta consistente en la eliminación o modificación, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, de las medidas tecnológicas eficaces incorporadas por éstos con la finalidad de impedir o restringir su realización, o la consistente en poner en circulación o tener cualquier medio principalmente concebido, producido, adaptado o realizado para facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones, pues con dichas conductas se hace patente la intención de acceso ilegítimo al halo de protección de aquel derecho, al margen de la propia ilicitud de la invasión técnica sobre "muros informáticos" especialmente destinados a la protección del derecho a la propiedad intelectual.

Sin embargo considero que deberían reconducirse al campo puramente administrativo, salvo en los supuestos de organizaciones criminales, las conductas relativas a la venta ambulante o "top manta" que se mantienen también como delito en el proyecto de reforma.

¿Echa de menos la introducción o tipificación de alguna actividad delictiva, alguna cláusula referente a la Ciberdelincuencia?

Como ya he comentado anteriormente, más que la introducción de nuevas modalidades delictivas, las actuaciones legales más imperiosas referidas al ámbito de la criminalidad informática deberían implementarse en otros campos. Fundamentalmente en el procesal y en el de la organización judicial. Me atrevería a indicar, sin ánimo exhaustivo, los siguientes en los que se debería incidir o que deberían ser potenciados:

- a) Reubicación sistemática conjunta en el Código Penal de los tipos penales en los que objeto de la actividad delictiva son los propios sistemas informáticos o las TICs.
- b) Consolidación sistemática en el mismo texto legal de aquellos delitos informáticos que, atendiendo al aspecto estadístico, constituyen, sin duda, el 80% de los mismos, esto es, las estafas informáticas, la pornografía infantil y la corrupción de menores, los delitos contra la propiedad intelectual e industrial y los referidos a la intimidad en referencia al descubrimiento y revelación de secretos.
- c) Especialización judicial. No existen, a diferencia de que ocurre a nivel de Ministerio Fiscal o de cuerpos policiales, Juzgados especializados en materia de criminalidad informática.
- d) Potenciación de las medidas cautelares y preventivas de protección de víctimas y perjudicados mediante la posibilidad de eliminación o suspensión urgente de los contenidos ilícitos en webs y redes sociales. Al respecto, es de aplaudir algunos aspectos de la reforma, en los que, por ejemplo, y dependiendo del tipo penal concretamente infringido, se permite que judicialmente se acuerde que la orden de retirada de contenidos dispuesta por la autoridad judicial esté referida tanto a la retirada de los archivos que contengan las obras o prestaciones protegidas como a la de los enlaces u otros medios de localización de las mismas; o que se faculte expresamente a los Jueces y Tribunales para que puedan ordenar la adopción de medidas necesarias para la retirada de las páginas Web de Internet que contengan o difundan pornografía infantil o, en su caso, para bloquear el acceso a dichas páginas, así como que puedan ordenar la adopción de las medidas necesarias para la retirada de las páginas Web de Internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español; o que en determinados casos, cuando a través de un portal de acceso a Internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente determinados contenidos, se pueda ordenar la interrupción de la prestación del mismo, y, de manera excepcional, cuando exista reiteración de la conducta y cuando resulte una medida proporcionada, eficiente y eficaz, se pueda ordenar el bloqueo del acceso correspondiente.
- e) Consolidación de la colaboración de los prestadores y proveedores de servicios de Internet para la rápida y adecuada actuación al respecto, potenciándose las posibilidades a tal fin contenidas en la Ley 34/2002 de 11 de Julio de Servicios de la Sociedad de la Información y del Comercio Electrónico, en relación con la Ley 4/2011 de Economía Sostenible (en la parte referida a la conocida como “Ley Sinde”) y en la Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de comunicaciones. Esta última, para la reconsideración del concepto de “delito grave” para obtener la correspondiente autorización judicial, pues es evidente que refiriéndose la gran parte de las actuaciones penales relativas a la llamada ciberdelincuencia al derecho fundamental al secreto de las comunicaciones, una interpretación restrictiva del concepto de delito grave hace

prácticamente inútil muchas labores investigadoras. Al respecto, asimismo, abundar en una nueva interpretación del contenido de los derechos contenidos en el artículo 18 de la CE, reconsiderando los conceptos de intimidad y de secreto de las comunicaciones en aras a mejorar y agilizar los procesos policiales y judiciales de investigación de este tipo de delincuencia. En este sentido, me remito a lo comentado en mi artículo sobre confidencialidad y delitos informáticos al respecto publicado en editorial La Ley (Pág. 9) y al que pueden acceder en www.josediazcappa.es

- f) Potenciación e implementación y mejora de los mecanismos normativos internacionales al respecto, algunos de ellos ya transpuestos al ordenamiento jurídico español, fundamentalmente los relativos a los diferentes mecanismos de Cooperación Jurídica Internacional, como los relativos al reconocimiento mutuo en relación con la obtención y validación de las pruebas obtenidas en el ámbito de la prueba transnacional, eliminando la incertidumbre propia de la admisión o no en base a la reciprocidad; asimismo, la necesaria concreción a nivel internacional de los parámetros de competencia para perseguir este tipo de delincuencia, teniendo en cuenta que la criminalidad informática se lleva a cabo, se materializa y produce efectos, normalmente en uno o varios países, planteándose problemas de competencia para su investigación tanto en sentido positivo (todos quieren tener la competencia), como, y lo que es peor, en sentido negativo (todos rechazan la competencia en base al principio de oportunidad). Sin perjuicio de que muchos convenios internacionales, como el de supresión del terrorismo de 1997 o el de 1999 sobre corrupción, o el propio sobre ciberdelincuencia de 2001, contienen algunas disposiciones específicas al respecto, lo cierto es que, salvo excepciones como la orden europea de detención y entrega, la práctica está bastante alejada de la realidad. Asimismo, mediante la coordinación internacional al respecto a través de las diferentes Redes de Cooperación Jurídica Internacional, Eurojust, IberRed, etc. Especial consideración merecería una hipotética relación internacional bilateral “USA-resto del mundo”, por motivos más que conocidos mediáticamente, y porque no se puede obviar que la mayor parte de las redes sociales o de los prestadores de servicios de correo electrónico en Internet, o, simplemente, navegadores o sistemas operativos, son y tienen su sede en EEUU. En otra ocasión se podría hablar largo y tendido sobre este aspecto concreto.
- g) En relación con lo anterior y fundamentalmente en el aspecto procesal al que me he referido en varias ocasiones, implementación de la reforma pendiente en materia procesal mediante la aprobación del llamado “Código Procesal Penal”, que modificaría la actual Ley de Enjuiciamiento Criminal, y que, sin perjuicio de otros aspectos del mismo ajenos a la materia de la que hablamos y de su susceptible mejora, contiene, sin duda, una importante y mejorada regulación, adaptada al Convenio de Budapest, en relación con las actuaciones de investigación necesarias para la limitación judicial de derechos fundamentales, y así las referidas a la forma de la interceptación de las comunicaciones telemáticas; a la forma de incorporación al proceso de los datos de tráfico o asociados; identificación de la IP o de los terminales mediante captación de códigos de identificación del aparato o de sus componentes, tales como la numeración IMSI o IMEI; la forma de la captación y grabación de conversaciones mediante la utilización de dispositivos electrónicos; investigación mediante agente encubierto; registros sobre dispositivos de almacenamiento masivo de información; registros remotos sobre equipos informáticos o sobre la manera de incorporación de datos personales automatizados al proceso, entre otras esenciales cuestiones procesales y relativas a los derechos fundamentales normalmente afectados en la investigación de los delitos informáticos.

¿Cree que el nuevo Código Penal va a "cambiar mucho" o mejorar los instrumentos judiciales para perseguir los delitos informáticos?

Creo haber comentado ya el contenido de esta cuestión. Sin perjuicio de ello, es evidente que la reforma del Código Penal, por sí sola, no va a suponer una importante mejora en la dinámica actual de la Administración de Justicia en relación con la persecución del cibercrimen. Considero que sólo será palpable la misma si viene acompañada del resto de reformas apuntadas, algunas de ellas también en marcha, y por supuesto, de otros avances legislativos como el Anteproyecto de Ley Orgánica de desarrollo de los derechos fundamentales vinculados al proceso penal.

En todo caso, cualquier mejora es siempre bienvenida.

Podría hacer un breve comentario sobre estos dos nuevos artículos que han suscitado la polémica:

“§ Se tipifica la facilitación de medios para suprimir o neutralizar las medidas tecnológicas utilizadas para proteger la propiedad intelectual. En ningún caso se actuará contra usuarios o buscadores neutrales, ni contra los programas P2P que permiten compartir contenidos. Las conductas más graves podrán ser sancionadas hasta con seis años de prisión”

Como ya he comentado, considero un importante avance en relación con la protección penal de la propiedad, la tipificación, con determinadas condiciones, de la conducta consistente en la facilitación del acceso o la localización de obras o prestaciones protegidas ofrecidas ilícitamente en Internet, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios, pues con la redacción actual del correspondiente tipo penal han sido y siguen siendo muchas las conductas que, al albur de diferentes interpretaciones judiciales y jurisprudenciales, en muchos casos contradictorias, han dejado al margen de la tipificación penal el aprovechamiento claramente (y altamente) lucrativo por parte de muchos administradores de páginas web en las que su único contenido era la facilitación del acceso y contenido a páginas de enlace claramente vulneradores de los derechos de propiedad intelectual.

En relación con esto, y para evitar confusiones con la actividad lícita de los navegadores y buscadores, así como las consecuencias de la indexación, parece correcto también el dejar al margen de la conducta delictiva a quienes desarrollen actividades de mera intermediación técnica, como puede ser, entre otras, una actividad neutral de motor de búsqueda de contenidos o que meramente enlacen ocasionalmente a tales contenidos de terceros, cual ocurre normalmente con los navegadores o buscadores en Internet. En este sentido, se añaden a la posible tipificación del hecho una serie de condiciones cumulativas ¹que, de cumplirse, difícilmente denotarían una ausencia de intencionalidad

¹ 1.º) Participe adquiriendo conocimiento o control de los medios por los que se facilite el acceso o la localización de las obras o prestaciones ofrecidas ilícitamente, en la vulneración de los derechos de forma significativa considerando, entre otros, su nivel de audiencia en España o el volumen de obras y prestaciones protegidas no autorizadas;

2.º) desarrolle una labor específica de mantenimiento y actualización de las correspondientes herramientas tecnológicas, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y prestaciones referidas anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios del servicio;

3.º) no se limite a un tratamiento meramente técnico o automático de los datos facilitados por terceros con los que no mantenga una colaboración, control o supervisión; y

delictiva y que los alejarían claramente de un proceso normal de búsqueda por criterios aleatoriamente introducidos por cualquier usuario particular de Internet cuando utiliza su ordenador.

“§ Será castigado con hasta un año de prisión la difusión no autorizada de imágenes o grabaciones íntimas obtenidas con consentimiento de la víctima pero sin autorización para su difusión”

Como se refleja en la Exposición de Motivos del proyecto de ley de modificación del CP, los supuestos a los que ahora se ofrecería respuesta con esta reforma mediante la tipificación de aquellas conductas consistentes en castigar al que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona, serían aquellos en los que las imágenes o grabaciones de otra persona se obtienen con su consentimiento, pero son luego divulgados contra su voluntad, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión, sin el consentimiento de la persona afectada, lesione gravemente su intimidad.

Este precepto no sería sino la consecuencia de una situación muy común en la actualidad, y muy cercana a la violencia de género y doméstica. Mientras las relaciones sentimentales o de amistad, o similares, van por buen camino, es frecuente compartir situaciones privadas, cuando no íntimas, normalmente de índole sexual, que, en el momento de documentarse, cuentan normalmente con la aquiescencia de los intervinientes. Sin embargo, cuando la situación empeora y se produce la ruptura, es frecuente que esas imágenes o grabaciones, que en un momento contaron con consentimiento para su posesión o incluso su reproducción, son utilizadas de forma anómala por alguno de ellos, justificando tal acción en el hecho del consentimiento previo obtenido y la “posesión compartida”. Con la nueva regulación se deja constancia, y considero que es de gran acierto, que cuando la situación futura no se corresponde con la anterior y la utilización de las imágenes o vídeos puede producir un claro y grave menoscabo de un bien jurídico personal, el uso ilícito de aquellos por alguna de las partes implicadas debe contar con el oportuno reproche penal al considerar la falta de eficacia de un consentimiento prestado inicialmente en condiciones muy diferentes.

¿Qué opinión le merece que entre los cambios previstos, se vaya a considerar como agravante en los delitos de hurto y robo el hecho de que afecten a las telecomunicaciones?

En ese caso, la reforma no está directamente relacionada con la llamada ciberdelincuencia.

Se trataría de una modificación destinada exclusivamente a proteger con mayor rigor la apropiación patrimonial de los medios materiales a través de los cuales se transmite la información en la Red, pero de la misma forma que podrían amparar el cableado eléctrico, las conducciones de gas u otras similares, pues la razón de la exasperación punitiva está, precisamente, en las situaciones de suspensión de

4.º) actúe con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio a tercero.

servicios públicos y el quebranto grave para los mismos que la sustracción de este tipo de materiales normalmente conlleva.

Como se dice en la Exposición de Motivos, el cambio vendría determinado debido al grave problema generado por la sustracción de cable de cobre de las redes de servicio público e interés general, por lo que también se ha considerado conveniente incorporar una agravación cuando los delitos de hurto o robo afecten a conducciones de suministro eléctrico o de telecomunicaciones.

¿Qué le parece la reciente sentencia del Tribunal Constitucional en la que se dio validez al despido de un trabajador cuyo correo electrónico fue controlado por la empresa?

La Sentencia del TC 170/2013, de 7 octubre, que parece ser la de referencia, no es la única al respecto en similares supuestos, y en todas ellas hay matices comunes que delimitan lo que es su objeto y finalidad y en modo alguno vienen a reflejar una posibilidad sin límites del empresario de poder tener conocimiento de cualquier dato o detalle de lo que un trabajador de la empresa pueda comunicar mediante el uso de los medios informáticos de la misma.

Es evidente que tratándose, además, de derechos fundamentales, estos se calibran en base a su consideración individual, y, por supuesto, para el caso concreto.

En una visión general de las diferentes SSTC que resuelven, en amparo, el tipo de conflictos a que nos referimos, se puede observar que se refieren a supuestos producidos en el ámbito de las relaciones laborales, -cuestión importante, sin duda-, donde el Alto Tribunal viene desestimando el amparo solicitado por los recurrentes basándose en considerar que se trata de uso de correos corporativos en los que cabía entender que no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial; en las que, además, existía una expresa prohibición, legalmente habilitada para el empresario, del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales, lo que conllevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe; y en las que, finalmente, en la mayoría de los casos, tales comunicaciones venían reflejando una conducta contraria, incluso, a los intereses colectivos de la empresa y de otros trabajadores.

De este modo, está claro que el TC no avala en modo alguno que cualquier empresario pueda “fisgar” cuando y como quiera en las cuestiones personales de los trabajadores transmitidas a través de Internet haciendo uso de los elementos informáticos de la empresa, en cualquiera de sus modalidades (e-mail y redes sociales normalmente), sino que matiza cuándo y cómo, con apoyatura legal para el empresario, y con conocimiento previo del trabajador sobre las condiciones de uso de los mismos, puede aquel acceder, de forma proporcionada y justificada, a aquellos contenidos, con la finalidad de poder advenir el incumplimiento o defectuoso cumplimiento de la relación laboral por parte del trabajador.

Cualquier otra invasión en la intimidad del trabajador o en su derecho fundamental al secreto de las comunicaciones (por ejemplo, el control por el empresario del correo particular del trabajador usado desde el ordenador de la empresa sin otros condicionantes) podría dar pie, sin duda, al amparo del TC, cuando no a una intromisión al derecho fundamental a la intimidad personal protegida por el art. 18.1

José Díaz Cappa. Fiscal.
Delegado de Criminalidad Informática.

www.josediazcappa.es
jose.diaz@fiscal.es

de la CE y en la Ley 1/82 de 5 de mayo, o, incluso, a una infracción penal incluida en el tipo delictivo correspondiente.

De nuevo, se trataría de conocer en detalle el juego de los derechos a la intimidad y secreto de las comunicaciones, haciendo una exégesis a adecuada de su connotación común de confidencialidad, así como separarlos de aquellos supuestos en los que, al amparo del art. 18.4 de la CE, no se trataría sino de una cuestión administrativa a valorar conforme a la correspondiente legislación sobre protección de datos personales. Al respecto, mi artículo en www.josediazcappa.es sobre las diferentes dimensiones de la protección de datos.