El cibercrimen en el ámbito económico y patrimonial

Prof. Dr. iur Dr. med. Carlos María Romeo Casabona
Prof. Dr. Iñigo de Miguel Beriain

Tema 3º

Accesos no autorizados a los sistemas y ficheros informáticos (I).

La protección penal de los datos y de las comunicaciones personales a través de la red. El caso de las personas jurídicas (empresas) Comunicaciones privadas en el ámbito laboral de la empresa.

10. LOS ACCESOS NO AUTORIZADOS A LOS SISTEMAS Y FICHEROS INFORMÁTICOS (I)

10.1. Aspectos generales

Son constantes las nuevas formas en que pueden verse afectados datos de diversa naturaleza (de carácter personal, con valor económico, que interesen a la seguridad del Estado, etc.) y los sistemas informáticos, accediendo a ellos a través de la red. Estos actos constituyen en primer lugar accesos no autorizados y por tal motivo ilícitos, por lo que en ocasiones se les denomina también como intrusismo, e intrusos a sus autores (*hackers* en la terminología anglosajona).

En efecto, es indudable la trascendencia que pueden tener para la vida privada, para las relaciones económicas y financieras, así como para la seguridad tanto de entidades públicas como privadas actividades que se encuentran en vías de generalización, como son la comunicación a través del correo electrónico; las conversaciones escritas u orales a través de la red (*chat*), las transacciones comerciales (compras a través de la red), en este caso, tanto en relación con el interés económico de la operación en cuanto tal –pues puede ser relevante desde el punto de vista penal- como también por lo que pueda revelar sobre la vida privada del autor de la operación. De modo semejante el mero acceso a la ingente, variadísima, dispersa y fluida información disponible en la red (páginas *web*); los archivos y bases de datos o los propios sistemas informáticos accesibles a través de la red; la necesidad de atender a la petición de información por parte de de los prestadores de servicios de la red para poder acceder a ella. Teóricamente todas estas actividades pueden ser interceptadas como también puede accederse a la información archivada, y de hecho lo son en no pocas ocasiones.

Por otra parte, se han ido desplegando situaciones nuevas de difícil encuadramiento jurídico. Así, la introducción de rutinas en el equipo terminal del usuario, donde se instalan y permanecen durante un tiempo determinado, de meses, incluso años, recopilando información sobre el ordenador y en ocasiones sobre los sitios que visita el usuario, devolviendo esa información del usuario receptor al proveedor de servicios remitente de las mismas (*cookies*) cuando se navega a través de ellos, a pesar de que haya podido prestar su consentimiento (normalmente como condición previa para conseguir el acceso a ciertos contenidos de la red); o la recepción masiva de correo electrónico, generalmente publicidad no solicitada (*spam* o *spamming*), sin capacidad de control real por parte del usuario. Estos casos, mencionados a modo de ejemplo, pueden configurar otras formas de intromisión en la vida privada, aunque en el segundo supuesto ya no se trate, evidentemente, de la intimidad, al menos en el sentido en que suele entenderse en relación con la información personal de carácter reservado, sino como invasión en la vida privada, de una forma que recuerda de algún modo al allanamiento de morada.

Puede convenirse en que la mayor parte de las actividades acabadas de mencionar deben quedar bajo alguna forma de tutela jurídica o ser reguladas para controlar su alcance, evitando que se rebasen ciertos límites, que también hay que precisar. De hecho

algunas de ellas ya lo son en el ordenamiento jurídico español, incluso penalmente. Pero como podrá comprobarse a lo largo de este Capítulo, del siguiente y, en cierta medida, de algunos más, la protección penal se sustancia en relación con la agresión que estos accesos ilícitos o no autorizados pueden comportar para bienes jurídicos concretos.

10.2. El delito de acceso a bases de datos o programas vulnerando medidas de seguridad

Hasta hace poco tiempo estos actos de intrusismo en cuanto tales no eran objeto de persecución penal en el Derecho español: sólo había delito si el acceso no autorizado se realizaba con intención de perjudicar a otro –en los términos que se estudiarán más abajo- o si la obtención subsiguiente de información personal comportaba ya su descubrimiento en su sentido jurídico-penal. Pero antes de presentar la novedad introducida en el CP en relación con estos hechos, conviene proceder a una breve exposición de lo que ofrece el panorama internacional.

El Convenio del Consejo de Europa sobre Cibercrimen ha optado por una vía mixta. La primera opción que se ofrece a los Estados Parte en él consiste en criminalizar cualquier acceso no autorizado. Esta vía se suaviza después con una opción alternativa más restrictiva, de acuerdo con la cual los Estados Parte podrán exigir (esto es, incluir en la figura de delito correspondiente) que el autor haya actuado movido por una finalidad determinada:

> "Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático" (art. 2º)

La adopción de una u otra solución implica, por ejemplo, castigar o no como delito el llamado "intrusismo blanco", es decir, aquel acceso, por supuesto sin autorización del titular del sistema informático, con el que únicamente se pretende burlar los mecanismos informáticos de protección de dicho sistema, precisamente frente a accesos no autorizados, sin que el autor pretenda acceder a ningún dato en particular, ni copiarlo, inutilizarlo o alterarlo.

Nos encontramos aquí con opciones político-criminales muy diferentes, pues la primera de ellas comporta que la intervención del Derecho Penal se adelante considerablemente, incluso aunque no se ponga en peligro bien jurídico alguno (estos delitos tendrían entonces la estructura de delitos de simple actividad, en concreto de peligro abstracto). Algunos autores han criticado este enfoque, porque pone en entredicho el principio de mínima intervención del Derecho Penal, conforme al cual el Derecho Penal debe reservarse para los atentados más graves a bienes jurídicos especialmente valiosos.

En este contexto debe mencionarse la figura delictiva introducida por la LO 5/2010, de 22 de junio, de modificación del CP, la cual se ha promulgado en los siguientes términos:

> "El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. Cuando e acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado m7 del artículo 33" (art. 197 nº 3).

Parece ser que el legislador ha querido seguir las previsiones de armonización establecidas en la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, que exige de los Estados miembros de la Unión Europea la adopción de las medidas necesarias para sancionar penalmente el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información (art. 2º).

Sin tomar en consideración la agravación prevista en relación con las personas jurídicas (la LO 5/2010 ha introducido la responsabilidad penal de las personas jurídicas, y el art. 197.8 establece un tipo agravado cuando el hecho se haya cometido en el seno de una organización o grupo criminales), podemos comprobar que se incluye un elemento objetivo en el tipo que limita la punibilidad a los accesos que comporten la vulneración de las medidas de seguridad establecidas para impedirlo; por consiguiente, no se incluyen los accesos que se hayan realizado sin vulnerar dichas medidas de seguridad. Pero, además, es

necesario haber accedido sin estar autorizado. La autorización, para que excluya el tipo, deberá haber venido de la persona, física o jurídica, titular del fichero en el que se acogen los datos a los que se ha accedido o del programa informático, o de la persona con atribuciones otorgadas en este sentido por el referido titular.

Al referirse al acceso a datos (no necesariamente personales), y a programas informáticos, el *bien jurídico* que ha pretendido proteger el legislador parece querer ir más allá (pueden ser datos con interés económico, p. ej.) del que se protege en el conjunto del Capítulo en el que se inserta este delito, esto es, la intimidad y los datos de carácter personal; pero, al mismo tiempo, en ocasiones será inevitable un solapamiento con el delito del art. 197.2, al menos cuando se trate de accesos no autorizados a datos personales; en todo caso, exigirá un esfuerzo de delimitación del ámbito de ambos delitos. Por ello, la ubicación de este delito no es adecuada, pues podría hacerse una interpretación restrictiva del alcance del delito, pues siendo la intimidad y los datos de carácter personal reservados el bien jurídico al que se quiere dar cobertura penal en el capítulo del CP en el que se ha insertado, podría argumentarse que están excluidos del tipo accesos que pueden poner en peligro bienes jurídicos de naturaleza diferente (p. ej., el secreto de empresa, secretos relacionados con la Defensa o con la seguridad del Estado; etc.), y ello sin perjuicio de ser conscientes de que con este delito se pretende castigar los accesos ilegales cualquiera que sea la naturaleza de los datos, incluyendo los programas.

Por lo que se refiere a la *conducta típica* ésta es doble, pero presenta un carácter alternativo, es decir, basta con realizar una u otra para que se realice plenamente el tipo.

La primera de ellas consiste en la acción de acceder a los datos o programas.

La otra conducta típica recogida como alternativa, esto es, mantenerse dentro de un sistema informático o en parte del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, es una conducta omisiva –no abandonar el sistema informático- y presupone que el sujeto del delito se introdujo en tal sistema legítimamente, o lo que es lo mismo, con la autorización correspondiente, pero que ésta ha sido retirada con posterioridad.

Se incluye un elemento objetivo en el tipo que limita la punibilidad a los hechos que comporten la vulneración de las medidas de seguridad establecidas para impedirlo. Por consiguiente, no se incluyen en el ámbito punitivo los accesos que se hayan realizado sin vulnerar dichas medidas de seguridad, aunque se haya accedido sin la autorización pertinente. De entrada nada hay que limite la presencia de este requisito típico a uno de los comportamientos mencionados como alternativos (acceder o mantenerse); alcanza a ambos.

Mientras que normalmente no habrá dificultades para comprobar la existencia de este elemento típico respecto a la conducta de acceder, esta exigencia del tipo no se prevé de fácil cumplimiento a quien se mantiene dentro del sistema, aunque inicialmente haya accedido lícitamente al mismo, pero después le ha sido retirada la autorización o ésta ha caducado, situándose entonces en el entorno del segundo tipo alternativo mencionado, pues no parece que ese mantenerse en el sistema una vez perdida la autorización vaya a hacerse vulnerando medidas de seguridad (si se vulnerasen tales medidas sería probablemente con el fin de volver a entrar, esta vez ilícitamente, adonde se había accedido previamente de forma lícita); no obstante, son admisibles hipótesis compatibles con esta exigencia del tipo en relación con el comportamiento omisivo (p. ej., anular el procedimiento de cierre del acceso lícito una vez pasado un cierto período de tiempo previamente establecido). Por consiguiente, aunque sea discutible su acierto, no hay base para excluir de esta segunda modalidad típica la necesidad de haber vulnerado las medidas de seguridad que se hayan interpuesto para prevenir cualquier acceso no consentido por el titular de los datos o del programa.

Es necesario, además, haber accedido sin estar autorizado. La autorización, para que excluya el tipo, deberá haber venido de la persona, física o jurídica, titular del fichero en el que se acogen los datos a los que se ha accedido, o del programa informático. También es admisible que la requerida autorización venga de la persona con atribuciones otorgadas en este sentido por el referido titular. Hipotéticamente, también podría venir autorizado por la ley.

En cuanto al *tipo subjetivo* es necesario, pero suficiente, el dolo, esto es, la conciencia y voluntad de haber accedido a los datos o programas informáticos vulnerando las medidas de seguridad y sin la autorización correspondiente (o sea, de que concurren, o es

previsible que así sea, todos los elementos del tipo objetivo), o de permanecer en ellos habiendo concluido la autorización correspondiente. No es exigible al presencia de ningún otro elemento subjetivo de lo injusto, ni se ha previsto la sanción penal del hecho si se ha cometido por imprudencia, exclusión de todo punto correcta.

En resumen, se trata de un delito que hubiera merecido una más atenta reflexión respecto al cómo de su inclusión en el CP, si consideramos que la Decisión Marco referida impone al legislador español su tipificación penal, pues se mantiene la duda político-criminal sobre la conveniencia de su sanción mencionada más arriba.

La cuestión de la protección penal de los datos de carácter personal nos la planteamos aquí en tanto que las intromisiones indebidas en esta clase de datos pueden afectar de algún modo, como señalábamos más arriba, a las relaciones comerciales, financieras y económicas en general, tanto en relación con personas físicas como jurídicas, pues ha de tenerse presente que el CP también protege los datos reservados de éstas últimas (art. 200), según se indicará más abajo.

11. LA PROTECCIÓN PENAL DE LOS DATOS PERSONALES: SU TRASCENDENCIA EN EL ÁMBITO EMPRESARIAL

Los problemas jurídicos que plantean los atentados a la intimidad y a los datos de carácter personal en conexión con su tratamiento informático o su comunicación a través de las redes telemáticas requieren una creciente atención por parte de Derecho. Y más ahora, que se ha producido una insospechada expansión del recurso a los medios telemáticos, con la posibilidad de accesos casi infinitos -en el sentido de inmensurables-, a información en archivos virtuales sin límites fronterizos y con apenas un marco jurídico que lo redefina.

Cuando se halla involucrada la tutela jurídica de la intimidad en relación con sistemas informáticos y telemáticos, tenemos que distinguir 1) la intimidad, por un lado, y 2) los datos de carácter personal reservados, por otro, tengan o no éstos un carácter íntimo. Esta bifurcación es esencial desde el punto de vista penal, pues de ella podrán derivarse el o –mejor- los bienes jurídicos protegidos.

11.1. El marco normativo

La Constitución española (CE), después del reconocimiento de la intimidad individual y familiar como derecho fundamental (art. 18.1), declara que

> "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (art. 18.4).

Por consiguiente, la CE reconoce que el uso de la informática afecta a la intimidad, pero puede trascender incluso la misma, al poder verse implicados otros derechos de los ciudadanos, su pleno ejercicio.

El primer paso significativo en nuestro ordenamiento jurídico lo supuso la ratificación por España del Convenio del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, que constituye derecho interno, aunque fuera discutible su aplicabilidad directa de al menos algunos de sus preceptos más significativos. En cualquier caso, el TC ha señalado que constituye un instrumento interpretativo-informador del contenido básico esencial del derecho reconocido en el art. 18.4 CE (*habeas data*).

El siguiente hito legislativo lo fue la promulgación de la LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal desarrollada por el RD 1332/1994, de 20 de junio, y por el RD 994/1999, de 11 de junio. Dicha ley ha sido derogada y sustituida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que dio cumplimiento a la transposición en el derecho interno de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. Esta ley, al igual que ocurrió con la anterior durante su período de vigencia, constituye la norma de referencia interpretativa de algunos tipos penales, como se indicará más abajo y, desde luego, la ley básica sobre el régimen de uso de los datos de carácter personal, así como sobre la protección integral extrapenal de los mismos.

Finalmente, hay que señalar el CP de 1995, que dio por fin cabida, después de reiterados intentos fallidos, a la protección penal

expresa de la intimidad y de los datos en el contexto de la informática y otros sistemas de telecomunicación (art. 197).

11.2. El Código Penal: sistemática legal y consideraciones político-criminales

Estos delitos aparecen recogidos en el Capítulo I ("Del descubrimiento y revelación de secretos"), del Título X ("Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio") del CP (arts. 197 a 201).

Es la primera vez que la intimidad figura explícitamente en una rúbrica del CP como bien jurídico: "delitos contra la intimidad...".

Es uno de los títulos con más novedades del CP de 1995, por el que hay que felicitarse, sin perjuicio de las críticas que pueda merecer. Es indudable que su antecesor requería una importante actualización y revisión con el fin de alcanzar varios objetivos, en particular, reforzar la protección de la intimidad como tal y del secreto; incluir la protección penal del secreto profesional; incorporar la protección de los datos de carácter personal, lo que se ha hecho con los que son de carácter reservado; trasladar a otro lugar del CP -en atención a la especificidad del bien jurídico protegido- la infracción del deber de secreto de carácter económico empresarial, esto es, el secreto de empresa; y responder mejor, en definitiva, a las necesidades legislativas derivadas de los derechos fundamentales de este tenor reconocidos en la CE.

La rúbrica que encabeza el Capítulo I no es correcta ("descubrimiento y revelación de secretos"), pues hay conductas tipificadas que no protegen el deber secreto en si mismo, sino la integridad de los datos reservados, que no son necesariamente secretos.

11.3. El bien jurídico protegido: Los datos de carácter personal (la libertad e identidad informáticas)

El bien jurídico protegido por estos delitos son los datos reservados, tanto de las personas físicas como jurídicas, -pero en este último caso, siempre que no tengan trascendencia económica directa, pues en este caso habrá que plantearse la aplicación de otros delitos de naturaleza patrimonial o socio-económica-, bien para garantizar su confidencialidad, bien para proteger su

integridad (libertad e identidad informática sobre los datos). Destaca, por consiguiente, la importancia de los conceptos de libertad e identidad informáticas, que se refieren al control de los datos personales por parte del interesado (sobre su exactitud, pertinencia, actualización, destino, cesión y uso, etc.), tengan o no carácter íntimo, por lo que conviene tener presente que son dos intereses de protección -bienes jurídicos- diferenciados, aunque en ocasiones se solapen y confluyan, en gran parte como consecuencia de las facultades de control que suelen ser reconocidas al respecto.

La legislación no penal sobre protección de datos personales ha de cumplir una función eminentemente preventiva de abusos en relación con la utilización indebida o inadecuada de aquéllos, fundamentalmente, lo que implica la adopción de medidas sobre la obtención, tratamiento, utilización y cesión de los datos. A este respecto, las actuales legislaciones sobre protección de datos de carácter personal suelen tener presentes estos bienes jurídicos: intimidad (intimidad informática, diríamos), libertad e identidad informáticas, además del libre y pleno ejercicio de los derechos de las personas. La primera faceta, la protección de la intimidad en relación con los datos, se sustenta sobre todo en el reconocimiento del carácter reservado de los mismos, lo que conduce a la consagración específica del deber de secreto y al establecimiento de infracciones relativas al incumplimiento de tal deber. La segunda faceta hemos visto que se desprende del reconocimiento a los afectados del derecho de información y acceso a los datos y del derecho de rectificación y cancelación, así como de los principios relativos a la calidad de los datos, a la información sobre su recogida, al consentimiento, a la seguridad y a la cesión de los mismos. Y, finalmente, con todo este arsenal de garantías y derechos se establece un marco para que el tratamiento automatizado de los datos de carácter personal, cuando resulte necesario, no menoscabe el libre y pleno ejercicio de otros derechos cívicos o políticos de las personas normalmente reconocidos por los textos constitucionales.

Ahora bien, es preciso hacer dos acotaciones sobre el alcance necesariamente limitado del Derecho Penal en esta materia, tanto desde la perspectiva de los principios fundamentales que inspiran su intervención, como a la luz de la peculiar naturaleza del bien jurídico: la constatación de que es imposible una protección global de la intimidad, sino fragmentaria, de algunas de sus manifestaciones más importantes. Aquí también debe regir el

carácter fragmentario y de *ultima ratio* del Derecho Penal, pues contamos además de la penal, con una protección desde los Derechos Civil y Administrativo.

Para lograr la intimidad e identidad informáticas en relación con los datos de carácter personal, se derivan de este último derecho, en concreto, los siguientes: el derecho a estar informado de la inclusión en un banco de datos y de los datos que le afectan; derecho a consentir sobre la utilización de determinados datos (los datos especialmente protegidos, llamados 'datos sensibles'); derecho al acceso a ellos, a su supresión o a su cancelación pasado un cierto tiempo; derecho a la rectificación de los datos erróneos; derecho a conocer el uso a que van a ser dedicados los datos personales; derecho a la confidencialidad; limitaciones tanto en la recogida como en la utilización de los datos; adopción por el responsable del banco de datos de medidas que garanticen el no acceso a los datos por parte de personas no autorizadas, a la vez que aseguren su no destrucción o modificación indebidas, etc.

Sólo algunos de estos aspectos han merecido protección penal, mientras que otros lo son a través de la LOPD, como infracciones administrativas (art. 44).

En cuanto al bien jurídico específicamente protegido en el art. 197.2, las conductas de "apoderarse" y "utilizar", así como las de "acceder" y "utilizar", que delimitan las acciones típicas en sendos tipos delictivos, suponen un atentado a la intimidad del sujeto pasivo –el titular de los datos. Por su parte, las acciones que comportan "modificar" o "alterar", que configuran asimismo conductas típicas en los respectivos tipos aludidos, suponen un atentado a un bien jurídico diferente, que es la identidad informática o integridad de los datos o libertad informática.

12. EL DELITO RELATIVO A LOS DATOS RESERVADOS DE CARÁCTER PERSONAL DE PERSONAS FÍSICAS O JURÍDICAS

El art. 197.2 del CP castiga con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses:

> "al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

> Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".

Consecuentemente de la lectura del precepto la primera observación es la de que se establecen dos tipos diferenciados, que comportan la misma intensidad punitiva.

12.1. El objeto material de la acción

El objeto material del delito: en los dos tipos delictivos que integran el art. 197.2 la acción ha de recaer necesariamente sobre datos reservados de carácter personal o familiar de otro.

En primer lugar, han de ser siempre datos *de otro*, es decir, de persona distinta de la que realiza la acción, lo que significa que el titular de los datos no puede ser sujeto activo respecto a sus propios datos.

En segundo lugar, por datos de carácter personal podemos entender los que así define la ley, añadiendo que también pueden pertenecer al ámbito familiar. Por consiguiente, ha de ser información concerniente a cualquier persona física, pero también jurídica (tampoco figuran éstas en la definición legal), a la vista de lo que señala el art. 200 CP, que también protege los datos reservados de personas jurídicas frente a su descubrimiento, revelación o cesión sin el consentimiento de sus representantes.

Por reservados habrá que entender aquellos datos personales que son de acceso o conocimiento limitado para terceros ajenos al fichero, aunque no sean íntimos en sentido estricto, es decir, que no están al alcance de terceras personas ajenas a su tratamiento autorizado.

En cuarto lugar, no es preciso que se trate de datos procesados automatizadamente, pueden haberlo sido por cualquier otro procedimiento.

Y, por último, han de estar recogidos en ficheros o soportes informáticos, electrónicos o telemáticos, pero también pueden estarlo en cualquier otro tipo de archivo o registro (es decir, manual o convencional) público o privado. La duda que se plantea aquí consiste en si se refiere a información heterogénea y no ordenada (esto es, recogida en ficheros o archivos) cuando se

trata de soportes informáticos, electrónicos o telemáticos, o ha de tratarse también de datos sistematizados en estos soportes pero a modo de fichero o archivo. Creo que se impone esta segunda interpretación, con el fin de poder delimitar mejor el ámbito típico de este delito con el del art. 197.1, cuando se refiere a interceptación y a apoderamiento.

12.1.1. Estructura típica de conductas alternativas

En resumen, son imaginables varias alternativas comisivas.

1) En primer lugar, que alguien realice la acción sobre los datos de otra persona con intención de perjudicar a un tercero (supuesto en el que entran en juego tres personas: el sujeto activo del delito, el titular de los datos sobre los que recae la acción y el tercero perjudicado, distinto del anterior, p. ej., modificar los datos registrales de defunción de una persona con el fin de que su viuda no disfrute de la pensión de la que es acreedora o disminuya la cuantía de disfrute). Realmente es éste un supuesto que parece poco frecuente, pero es admisible y se adecua claramente a la dinámica de ambos tipos penales, configurando espacios propios para cada uno de ellos.

2) En segundo lugar, el sujeto activo puede realizar la acción sobre los datos de otra persona con el fin de perjudicar a esa misma persona (por tanto, el titular de los datos y el perjudicado coinciden).

3) En tercer lugar, la realización de la conducta por el titular de los datos sobre los suyos propios con intención de perjudicar a tercero (así, alterar el puesto de uno mismo en el escalafón profesional, adelantándolo a un puesto superior) no es punible. Este criterio político-criminal es discutible (por supuesto, carecería de interés político-criminal si lo hiciera con intención de perjudicarse a sí mismo, que sería la cuarta hipótesis imaginable).

12.1.1.1. *La confusión descriptiva de las conductas típicas*

El primer problema que plantea este delito, que, como se ve, se refiere a ciertos atentados a los datos reservados de carácter personal o familiar, es la delimitación de las dos conductas típicas que se incluyen en el art. 197.2, pues, aparentemente, en parte indican lo mismo: utilizar y modificar (o alterar), en ambos casos "sin estar autorizado"; la diferencia radica tan sólo en las acciones

de "apoderarse" y "acceder", respectivamente y en actuar en perjuicio de tercero o de éste o del titular de los datos.

La diferencia entre ambos tipos delictivos debe encontrarse en algo más que una mera yuxtaposición de conductas, la cual por lo demás no tendría sentido, pues, en tal caso hubiera bastado con una integración de ambos tipos delictivos en uno solo.

A lo anterior hay que añadir que la LO 5/2010 ha introducido otro tipo delictivo de acceso no autorizado independiente de los dos anteriores (art. 197.3), lo que, probablemente, generará nuevos problemas interpretativos, en particular definir el ámbito típico de las tres modalidades comisivas (véase sobre este delito lo expuesto más arriba).

Por momento vayamos a ver qué puede entenderse del art. 197.2 CP.

12.1.1.2. El acceso autorizado

En el primer supuesto, el autor del hecho está legitimado para acceder al fichero, lo cual pudo estar en la *mens legislatoris* y puede ser más importante como explicación de tal dualidad en la estructura de los tipos. Esta legitimación inicial no concurre en el segundo tipo, por cuya razón en este último caso ya el mero acceso es penalmente ilícito.

Por tanto, quien estando autorizado para acceder al fichero se excede de dicha autorización, apoderándose de los datos a los que ya tiene acceso, o modificándolos más allá de sus funciones legítimas o utilizándolos para fines ajenos a los de su competencia o autorización, incurre en el delito, en su primer inciso. De ahí que sea necesario el apoderamiento de los datos mediante su aprehensión física o cualquier otro procedimiento de copia o reproducción, no bastando el mero acceso a ellos. Cuando con posterioridad al acceso y tratamiento lícito de los datos, el sujeto decide revelarlos a un tercero, no concurrirá el tipo de este delito, aunque podrá reprimirse penalmente a través de otro tipo penal (art. 199).

12.1.1.3. El acceso no autorizado

Por su parte, el segundo tipo del art. 197.2 incrimina a quien no estando autorizado para acceder a los datos lo hace "por

cualquier medio": acceso físico desde el propio sistema que los contiene, bien venciendo los mecanismos lógicos y físicos de seguridad, bien con engaño del encargado o responsable del fichero, por procedimientos telemáticos, etc. En este caso es suficiente con la captación intelectual de los datos, su visión, sin que sea necesaria la aprehensión física -apoderamiento- o reproducción de los mismos. El acceso a los datos ha de ser en todo caso directo por parte del sujeto activo, es decir, sin la mediatización de otras personas interpuestas. De concurrir la interposición de una persona, el que cede los datos incurrirá en el delito del art. 197.4 párr. 1º, y el que los recibe y después los difunde, por el art. 197.4 párr. 2º, siempre que tenga conocimiento de su origen ilícito y no haya tomado parte en el descubrimiento.

Son asimismo conductas alternativas del tipo la alteración de los datos –que es equivalente a modificar, como en el primer inciso- en el propio fichero, pues es irrelevante cualquier modificación de los datos que no se incorpore al fichero (p. ej., una vez copiados de éste), mediante la supresión, ocultación, bloqueo, sustitución o adición de otros, de modo que no reflejen la realidad de la que daban constancia o no sean ya útiles u operativos para el fin al que estuvieran destinados; y su utilización, incluso aunque no los haya percibido o visualizado, de modo que no haya llegado a captar su contenido en estos casos, pero conociendo su contenido global relativo a datos de carácter personal o familiar reservados. El delito existe, aunque el acceso a los datos se realice desde otro ordenador, una vez sustraídos los datos en un disquete.

12.1.1.4. El tipo subjetivo

Ha de actuarse con la intención de perjudicar a un tercero, o a éste o al titular de los datos.

13. LA PROTECCIÓN PENAL DE LOS MENSAJES DE CORREO ELECTRÓNICO Y DE OTRAS COMUNICACIONES DE CARÁCTER PERSONAL A TRAVÉS DE LA RED

13.1.La necesidad de la protección jurídico-penal de las comunicaciones a través de las redes telemáticas

La circulación de información por las redes telemáticas (internet) se ha convertido en un creciente y útil vehículo de comunicación interpersonal, de creación, difusión y acceso a la información.

Al mismo tiempo, el uso de este todavía nuevo procedimiento de comunicación electrónica o telemática comporta la generación de nuevas formas de vulnerabilidad de la intimidad y de los datos de carácter personal en torno a la red, en particular en relación con el anonimato o confidencialidad con que deben estar presididas estas actividades en relación con terceros ajenos a la comunicación, con la integridad de la información producida y con el acceso no consentido a las terminales privadas desde donde los ciudadanos se introducen en la red. Téngase en cuenta, además, que cada acto de recepción o remisión de comunicación o de acceso a sitios de la red dejan su huella o traza digital, que es susceptible de seguimiento e identificación.

A nuestro entender los bienes jurídicos implicados en las comunicaciones personales a través de las redes telemáticas dignos de protección jurídico-penal no se agotan en la intimidad y los datos personales. Esta consideración me ha llevado a pronunciarme también acerca de la oportunidad político-criminal de proteger penalmente de forma integrada y autónoma el pacifico uso y disfrute de tales redes en las relaciones privadas o, dicho de otro modo, la *comunicación pacífica a través de redes telemáticas*, con independencia de las garantías y protección que correspondan a otras formas de manifestación de la intimidad y de los datos de carácter personal.

En efecto, con este nuevo perfil, se quiere llamar la atención sobre la necesidad de ofrecer una protección jurídica más intensa –pero no exclusiva o principalmente penal- a las comunicaciones personales en cuanto tales, así como a las actividades de producción y de consumo de información en las redes, con independencia de que se generen datos personales o no.

13.2.La protección penal de las comunicaciones a través de la red, en particular de los mensajes de correo electrónico

Al consistir los mensajes de correo electrónico y otras telecomunicaciones realizadas a través de las redes telemáticas en una forma de comunicación privada debe reconocérseles en principio el mismo tratamiento jurídico que el ordenamiento jurídico reconoce a ésta. Es oportuno mencionar, en primer lugar, la protección constitucional que se garantiza al secreto de las comunicaciones, salvo resolución judicial, en el art. 18.3 CE, y que la misma naturaleza jurídico-constitucional que a las postales,

telegráficas y telefónicas que menciona ejemplificativamente hay que reconocer a cualquier otra forma de comunicación a través de la red.

Valga recordar la doctrina del Tribunal Constitucional sobre el alcance constitucional de la protección de las comunicaciones en general, que abarca tanto al proceso y al soporte de la comunicación como a su contenido mismo.

El bien constitucionalmente protegido es así, la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto como por el simple conocimiento antijurídico de lo comunicado.

Con posterioridad el Tribunal Constitucional ha realizado también una aproximación a la cuestión que nos ocupa en la línea sugerida más arriba, al entender que el referido precepto constitucional ha de extenderse asimismo a las nuevas tecnologías: "Ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE".

La Ley General de Telecomunicaciones establece por su parte la protección no penal del secreto de las telecomunicaciones y de los datos personales en el sector.

En el art. 197 del CP encontramos varias modalidades típicas básicas, una de las cuales gira en torno al apoderamiento de papeles y cartas, en línea muy semejante a su predecesor, aunque incluyendo ahora otros objetos materiales novedosos, tributarios de las nuevas tecnologías de la comunicación, como lo es el correo electrónico, o que simplemente pretenden cumplir una función de escoba o de recogida en relación con los objetos anteriores.

En el art. 197.1 se incluyen algunas conductas en las que pueden estar implicados sistemas informáticos o telemáticos, en concreto, las comunicaciones personales a través de la red:

> "El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha,

> transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".

En este tipo delictivo podemos distinguir los siguiente grupos de tipicidad: 1º los actos de apoderamiento; 2º interceptar las telecomunicaciones de otro; y 3º utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación.

Finalmente, como se vio más arriba, se incorporan como delito diversas conductas relacionadas con los datos reservados de carácter personal y familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado (art. 197.2).

En principio, en este lugar vamos a centrarnos sobre las posibilidades de protección penal que ofrece el art. 197.2 del CP respecto a las comunicaciones a través de internet.

En cuanto a la naturaleza jurídico-penal de este delito puede calificarse como *de acción peligrosa* (es decir, de peligro abstracto-concreto), pues es preciso que la acción sea en si misma peligrosa para el bien jurídico (de conformidad con el art. 16 CP), es decir, para la intimidad de otra persona. Significa esto que no es necesario que se haya producido la lesión del bien jurídico ni que haya corrido un efectivo peligro (delito de peligro o de peligro concreto). Por consiguiente, es evidente que el tipo básico no es de resultado material.

13.3.El objeto material del delito

El objeto material de este delito es múltiple y variado. Todos ellos se caracterizan por consistir en soportes físicos con capacidad para recoger, incorporar o reproducir hechos, datos, manifestaciones de voluntad, etc. que constituyan un secreto para alguien y afecten a su intimidad o que sin ser secreto involucren a dicha intimidad; esto es, esos soportes han de incorporar aspectos que afecten a la intimidad de otra persona. Están integrados, en primer lugar, por papeles y cartas. Además, por mensajes de correo electrónico, documentos y efectos personales. Lógicamente, en este estudio sólo voy a referirme a los mensajes de correo electrónico.

El CP no proporciona una definición de mensaje de correo electrónico. Sin embargo, el Derecho comunitario ha incluido una propia, que seguramente será incorporada al Derecho interno una vez que el legislador español haya procedido a la oportuna transposición de la disposición jurídica correspondiente: "Todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que pueda accederse al mismo". Puede aceptarse la anterior definición a título orientativo. Sin embargo, si atendemos a los propósitos específicos del Derecho Penal, dirigidos a la protección de un determinado bien jurídico, la definición comunitaria que, no debe olvidarse, está subordinada a los propósitos sectoriales en los que se enmarca, puede ser parcialmente inadecuada. En efecto, en cuanto tal definición es al mismo tiempo demasiado restrictiva y demasiado amplia. Lo primero lo encontramos en la limitación a mensajes cursados a través de redes de comunicación públicas y, sin embargo, no debe excluirse la intervención jurídico-penal allí donde existen comunicaciones que deben ser salvaguardadas del alcance ajeno, con independencia del carácter público o privado que tenga la red. Por otro lado, al Derecho Penal sólo interesan las comunicaciones electrónicas que sean personales.

A los solos efectos penales, por mensaje de correo electrónico puede entenderse una modalidad de comunicación, por lo general de carácter personal, que incorpora texto, voz, sonido o imagen y que se sirve de las redes telemáticas como tecnología de transmisión y de los sistemas informáticos (ordenadores y el *software* o sistema lógico correspondiente) como instrumentos de remisión y de recepción entre dos o más comunicantes y, en su caso, de almacenamiento de los mensajes. Conforme a lo indicado más arriba, a los efectos del presente estudio es necesario que la comunicación sea de carácter personal.

13.4.La adecuación típica de las diversas modalidades comisivas

El CP de 1995 introdujo de forma expresa como delito el apoderamiento de los mensajes de correo electrónico, así como la interceptación de las telecomunicaciones de otra persona. Sin perjuicio de las precisiones que se introducirán más abajo, puede adelantarse ya que en el primer caso se trata de conductas que pueden afectar al mensaje de correo electrónico o a cualquier otra comunicación a través de la red asimilable que se encuentra en

una situación estática, esto es, guardados en un fichero una vez recibido, pendiente de recepción y guardado en el sistema del prestador de servicios o guardado en el terminal de remitente cuando se halla pendiente de remisión. Mientras que las segundas –las telecomunicaciones- se refieren a conductas que afectan a cualquier mensaje u otra forma de comunicación telemática semejante mientras se encuentran en el proceso de transmisión (y, en ocasiones, de creación), es decir, en "movimiento". Sin perjuicio de que comporten situaciones diferentes, en todas ellas puede accederse a la comunicación privando a sus destinatarios o a alguno de ellos de su contenido o sin privar del mismo.

Las acciones de privación del mensaje o de cualquier otra comunicación a través de la red mediante su obstrucción, alteración o destrucción estarían más próximas en todo caso a los delitos de daños que a la finalidad que anima al tipo de descubrir los secretos o vulnerar la intimidad de otro, que difícilmente puede verse afectada por meros actos obstructivos o impeditivos de la comunicación entre terceras personas. De todos modos, en su caso, podría verse afectada la integridad de los datos de carácter personal, y puesto que éstos constituyen un bien jurídico autónomo, podría dar lugar a la aplicación del delito establecido en el art. 197.2 del CP, donde se protegen estos datos frente a su alteración o modificación no autorizada en perjuicio de terceros, además de frente a su acceso o utilización también no autorizados.

13.4.1. El apoderamiento de mensajes de correo electrónico

La primera acción típica en la que vamos a detener nuestra atención está constituida por el apoderamiento de mensajes de correo electrónico y de otras formas de telecomunicación. Para tal propósito habrá que abordar el alcance que tiene la acción de apoderarse en el conjunto del tipo en el que se inserta.

La acción típica viene expresada en el art. 197.1 del CP como *apoderarse* de los objetos que se enumeran en el tipo, entre ellos los mensajes de correo electrónico.

1) La primera acepción, que gira en torno a su expresión literal, consiste en entender que el acto de apoderamiento comporta el desplazamiento o *traslación física de la cosa* -del soporte en el que se encuentra la información o el hecho secreto o íntimo- por parte

del sujeto activo del delito a su propio ámbito de dominio o de control, en sentido similar, en consecuencia, al que suele interpretarse esta misma expresión en los delitos contra el patrimonio de apoderamiento. Sin embargo, no debe olvidarse en ningún momento la diferente orientación de cada unos de ellos en relación con el bien jurídico que están llamados a proteger los respectivos delitos. En consecuencia, esa traslación física en el delito de descubrimiento y revelación de secretos habrá que entenderla como suficiente –típica- desde el momento en que capacita al sujeto activo para acceder al contenido del objeto material trasladado a su control. La acción típica quedaría plenamente realizada con el mero hecho material descrito, sin que sea precisa la captación o aprehensión intelectual del contenido del soporte de la información o circunstancia íntima. Esta interpretación es casi unánime en la doctrina y debe aceptarse como una interpretación válida.

2) Otro significado es fruto del criterio jurisprudencial, ya antiguo, del que se hacen eco algunos autores, conforme al cual el apoderamiento también puede verse encarnado en la retención de lo recibido por error (en concreto, una carta postal remitida por error a un destinatario equivocado por parte del servicio de correos). En el tema que nos ocupa aquí consistiría, por ejemplo, en la recepción de un mensaje de correo electrónico enviado por el remitente a persona distinta del destinatario al que se quería dirigir en realidad y su subsiguiente apertura por el receptor. Desde luego, debe aceptarse que la apertura y subsiguiente aprehensión de su contenido ha podido ser accidental como consecuencia de un error inicial ajeno, con mayor motivo si se trata de un mensaje telemático, en el que el autor del error será normalmente el propio remitente. En tales situaciones es aceptable la exclusión del dolo en relación con lo realizado, según se verá más abajo, y considerar consecuentemente atípico el hecho. Sin embargo, cabría preguntarse si el tipo quedaría constituido si el receptor accidental procede a la copia del mensaje con el fin de vulnerar la intimidad de tercero (p. ej., para divulgarlo), una vez descubierto el error, dado el sentido que se asigna más abajo a la acción de copiar.

Como efecto de estos argumentos, podemos extraer dos conclusiones: una, que ya no es necesario en todos los casos que el acto de traslación haya sido realizado por el sujeto activo o por un tercero que obre con dolo, basta con un acto de dominio sobre el

soporte, una vez que éste ha llegado a su esfera de acción. Asimismo, está excluida la comisión de estos hechos por omisión.

3) A la conducta de apoderamiento hay que asimilar, según los casos, el hecho de copiar (mensaje de correo o de fax electrónicos), fotocopiar o fotografiar el soporte material (papel, documento o efecto personal) en el que se encuentra la información secreta o íntima, o incluso únicamente el contenido del soporte y no éste (piénsese, p. ej., en el mensaje de correo electrónico que es impreso en papel o copiado en un disquete, disco compacto u otro soporte informático), si por ese medio aquélla –la información- se hace accesible.

4) Una ulterior acepción de la acción típica incluiría el conocimiento del contenido del documento o efecto personal sin que esté precedido o acompañado por el apoderamiento material de dicho soporte. Ahora bien, incluso en este caso cabe contemplar varias hipótesis diferentes.

a. La primera de ellas se refiere a cuando el sujeto activo necesita realizar un acto previo que le permita la visualización del contenido

Así, encender el terminal del ordenador, acceder a la carpeta donde figuran los mensajes ya leídos –o no- por su destinatario y visualizarlos a continuación. A este respecto es significativo el acto de colocar un obstáculo, por muy leve que sea éste, por parte del sujeto pasivo al eventual acceso visual de terceros (apagar la pantalla del terminal, cerrar la puerta del despacho, etc.), pues constituye un reflejo *objetivo* de la voluntad de aquél de guardar o proteger el secreto o de mantenerlo fuera del alcance de otros, por lo que de acuerdo con esta interpretación cualquier acto encaminado a levantar o remover ese impedimento se adecuaría a las exigencias del tipo.

b. La otra hipótesis o paso quedaría integrado cuando el sujeto accede directamente a la visualización del contenido, sin necesidad de eliminar o remover impedimento alguno, ni tan siquiera de tocar físicamente el objeto, ni, por supuesto, de desplazamiento ilegítimo. Por ejemplo, leyendo el documento de un tercero situado a la vista sobre la mesa de éste mismo, o un texto –un mensaje de correo electrónico que haya sido impreso previamente- o imagen visualizables sobre la pantalla de un terminal de ordenador.

Para que sea admisible la conclusión de la adecuación típica de esta diferente dimensión de la referida expresión de apoderarse es preciso reconocer a la misma un significado o alcance todavía más espiritualizado que en los supuestos mencionados con anterioridad, pues supone un notable alejamiento de la interpretación que resulta más evidente, como traslación física del soporte del secreto o información íntima (p. ej., un papel o carta) desde el círculo de su propietario al autor del hecho, quedando desposeído aquél de dichos objetos; supone entender la acción típica, además –pero no siempre-, como la pura y simple aprehensión intelectual del contenido que aquéllos incorporan, así como los comportamientos intermedios. Por consiguiente, el último criterio interpretativo apuntado resulta ya discutible desde el punto de vista de su adecuación típica, pues es dudoso que se pueda forzar tanto el proceso de "desmaterialización" –espiritualización- del tipo, pues éste exige en todo caso –probablemente con dudoso acierto- un comportamiento material vinculado con los soportes que menciona. En cualquier caso, es revelador señalar que la doctrina se encuentra muy dividida sobre este particular.

Sin perjuicio de las consideraciones hermenéuticas presentadas hasta el momento, el apoderamiento de los mensajes de correo electrónico requiere todavía un examen detallado. Para algunos autores el hecho típico está caracterizado por el acto de apoderarse del correo electrónico de otro, por ejemplo, del mensaje una vez impreso sobre papel o soporte similar. Sin embargo, no me parece suficiente, pues esto no es lo específico y diferencial del mensaje de correo electrónico, y en consecuencia no puede ser el motivo que impulsara al legislador a incluirlo expresamente en la ley. El legislador supuestamente debió pretender cubrir alguna posible laguna de la descripción típica del CP anterior, y ya se ha visto cómo no sería éste el caso si lo limitamos al supuesto acabado de mencionar sugerido por un sector doctrinal. Por consiguiente, es preciso buscar otras propuestas más acordes con el verdadero sentido de la ley.

b_1) Acceder al mensaje que se visualiza directamente sobre la pantalla de un terminal, sin realizar ningún tipo de maniobra: en coherencia con lo apuntado anteriormente sobre otros documentos informáticos diferentes al mensaje de correo electrónico, debe excluirse tal conducta del ámbito de la tipicidad de este delito.

b_2) Abrir una carpeta no destinada en principio a estos mensajes: el hecho inicial, de ser accidental, sería también atípico, pero de aprovechar tal circunstancia persistiendo en la captación de la información, sería típica, por concurrir ya en este supuesto el dolo. De no ser accidental el acceso, se trataría de un supuesto asimilable al que se estudia a continuación.

b_3) Acceder al buzón -informático- de un tercero, en el que se encuentran almacenados todos los correos electrónicos recibidos por un mismo destinatario (p. ej., abrir e introducirse en la llamada "bandeja de entrada" del programa de correo electrónico), captando así el autor el contenido de los mensajes, pero sin desposeer de ellos a su titular: configura un supuesto similar a los mencionados más arriba como subsumibles en el tipo, en los que se remueve un obstáculo con el fin de poder acceder a los mensajes ya recibidos y archivados sin que se produzca un desplazamiento físico ilegítimo de los mismos.

En conclusión, no constituye una interpretación analógica en perjuicio del reo, contraria a las estrictas exigencias del principio de legalidad, entender que la palabra apoderamiento admite la traslación física o material del soporte, la reproducción de éste junto con el contenido que incorpora, la reproducción únicamente del contenido sobre un soporte diferente o, incluso, la captación directa de su contenido, siempre que haya un comportamiento previo que facilite el acceso al objeto material. Cualquiera de las variantes analizadas integra la acción típica que estamos estudiando. De todos modos, esta conclusión no impide insistir en el desacierto de mantener la expresión legal comentada -apoderarse-, puesto que ofrece un rendimiento muy trabajoso para lograr cubrir la variedad de aspectos –nuevos y no tan nuevos- mediante de los cuales puede presentarse la acción en la vida real.

A la vista de las reflexiones y propuestas anteriores se comprenderá lo excesivamente rígida y angosta –y por ello rechazable- que resulta la hipótesis, defendida minoritariamente por la doctrina, de que el tipo exige no sólo apoderarse del objeto o soporte que contiene la información secreta, sino además que llegue a conocerse también su contenido. Esta interpretación cuenta con un soporte legal todavía menos claro que del que pudiera disponer alguna de las anteriores propuestas interpretativas y, desde luego, no se compadece con la evolución

inherente a este tipo en atención en parte, precisamente, a los nuevos objetos materiales que incorpora.

13.4.2. La interceptación de las telecomunicaciones de otro a través de la red

La segunda variante típica está constituida por la interceptación de las telecomunicaciones de otro. Puesto que sobre el significado del objeto material (las telecomunicaciones) ya nos hemos ocupado más arriba, queda ahora centrarnos en el alcance dela acción típica: interceptar.

Interceptar desde un punto de vista lingüístico puede consistir en desviar, obstruir o acceder, en este caso a una telecomunicación, pero en atención a la estructura compleja que presenta el art. 197.1 y al bien jurídico protegido, procede realizar varias precisiones.

En efecto, la primera acepción debe ser descartada de todo punto en este lugar, puesto que de lo contrario no permitiría establecer ninguna forma de distinción con el primer inciso del art. 197.1 del CP.

Nos queda, por consiguiente, como significado más conforme con la naturaleza del delito el de acceder a la comunicación de otros sin interferir en su prosecución. En consecuencia, satisfaría los requerimientos de este segundo inciso ('interceptar' como equivalente a intromisión) y no del primero ('apoderarse'), en virtud de lo ya argumentado, si el sujeto activo logra acceder a un mensaje de correo electrónico durante el proceso de su transmisión, mientras está circulando por la red, captando su contenido sin desviarlo de su destino. Sería aplicable entonces este segundo inciso del art. 197.1 del CP. Ahora bien, si el sujeto activo lograra reenviar una copia a su propia terminal, podría incluirse en ambos incisos del art. 197.1 indistintamente, dado que hemos admitido como adecuadas típicamente al primero de ellos las acciones de copiar un documento sin privar al mismo tiempo de él a su propietario o tenedor.

En conclusión, en relación con el objeto de interés de este estudio es típica conforme al inciso segundo del art. 197.1 del CP la acción de interceptar los mensajes de correo electrónico o cualquier otra forma de comunicación telemática sostenida a través de la red en el sentido de acceder a la comunicación realizada por terceros,

siempre que esto se sustancie sin impedir la llegada del mensaje a su destino o el efectivo intercambio de mensajes.

13.4.3. La desviación de una telecomunicación

La acción puede consistir, finalmente, en la desviación del mensaje a un tercer terminal (p. ej., desde el que opera el sujeto activo o a otro diferente) durante el período de transmisión desde el equipo terminal del remitente al del destinatario, siempre que se prive a éste de su recepción. Nos encontramos aquí con una conducta que participa de elementos de los dos tipos referidos en los apartados anteriores, puesto que se actúa en el proceso de la transmisión, pero se priva al mismo tiempo de su recepción al destinatario o destinatarios. Entiendo que será punible de acuerdo con el primer inciso del art. 197.1, en el sentido de apoderamiento que he propuesto más arriba, pues si el mensaje llegase a pesar de ello a su destino estaríamos ante el supuesto de interceptación de las comunicaciones de otro que menciona el segundo inciso del art. 197.1.

En efecto, lo que aquí ocurre es que se intercepta un mensaje de correo electrónico, en el sentido de "apoderase de una cosa antes de que llegue al lugar o a la persona a la que se destina" que le otorga la RAE, sin acceder necesariamente al contenido del mensaje. La acción se asemeja con cierta fidelidad al efecto traslativo que adjudicamos inicialmente a la palabra apoderarse, pero con la significativa diferencia de que no se produce el traslado material de ningún soporte, sino del contenido mismo del mensaje. Consecuentemente, la adecuada interpretación de "apoderarse de… mensajes de correo electrónico" no ha de limitarse al sentido material o físico de los supuestos analizados con anterioridad, incluso los entendidos más laxamente, porque el estado "natural" de estos mensajes que estamos analizando ahora –los mensajes de correo electrónico- es virtual, sin ningún soporte material que los contenga. Por otro lado, la posibilidad de acceder a un mensaje de correo electrónico desde diferentes puntos o terminales, y no sólo desde el terminal habitual abunda a favor de esta propuesta interpretativa.

Debe dejarse claro inmediatamente que, por consiguiente, la palabra interceptar según se está utilizando ahora no guarda relación semántica con la que se utiliza en el segundo inciso del art. 197.1 ("interceptar las telecomunicaciones de otro"), y por ello

no puede ser integrada en esa modalidad del tipo, sino en la de apoderamiento, pues como se indicó más arriba, en aquella estructura típica no se produce una traslación-privación del dominio de la comunicación, que es lo que ocurre en nuestro caso, sino una mera intromisión cognoscitiva en la comunicación de terceros.

En conclusión, la anterior interpretación sí parece responder más certeramente a las características propias de los mensajes virtuales y probablemente también a la preocupación del legislador por despejar cualquier duda sobre la incriminación de las conductas mencionadas, recurriendo por ello a la mención explícita de estos mensajes en la descripción de los objetos materiales sobre los que puede recaer la acción típica.

13.4.4. El apoderamiento de trazas de acceso a la red

Como es sabido tanto las comunicaciones a través de la red como el mero acceso a determinados sitios de la misma (páginas *web*), suele dejar huellas de los mismos (páginas visitadas, hora de acceso, etc.), como ocurre en el propio historial de la navegación efectuada por la red, así como con los llamados *cachés*, pues ambos quedan registrados en el equipo terminal. En particular, algunos sitios de la red introducen en el equipo terminal como condición previa a permitir el acceso al mismo un fichero (*cookie*) que suministra información sobre el propio usuario. Sin entrar ahora en el estudio de este procedimiento, que requeriría un abordaje específico, lo cierto es que accediendo a las *cookies*, como también a los demás rastros, se puede obtener también información sobre los accesos realizados por el usuario, lo que afecta sin duda a su vida privada.

¿Cómo podría calificarse entonces si alguien accede al terminal de un tercero y se apodera o copia dichas *cookies* u otros rastros de las sucesivas navegaciones?

Lo cierto es que el objeto material a duras penas encaja en las previsiones actuales del CP, pues aunque podría aceptarse que el acto constituye un apoderamiento típico, no se trata de papel o carta, ni de documento en el sentido del CP (art. 26), ni es un mensaje de coreo electrónico ni tampoco un efecto personal. El hecho no tiene por qué comportar la interceptación de una comunicación (aunque podría serlo), por lo que surgen en un

primer plano dudas sobre la tipicidad del acceso o apoderamiento de estas informaciones.

La cuestión es si esa información cabe ser considerada como dato reservado de carácter personal, pues en ese caso el art. 197.2 del CP al abarcar como objeto material esos datos bastará con que estén registrados en soportes informáticos, electrónicos o telemáticos, que lo que ocurre con el caso que nos ocupa (esta información se halla en el equipo terminal u ordenador del usuario). La LOPD define los datos de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables (art. 3, a). Por consiguiente, a partir de una definición tan amplia (en este caso en relación con la expresión "cualquier información concerniente"), y al no ser preciso que formen parte de un fichero en sentido estricto cuando encuentran registrados en un soporte como el indicado, éste sería entonces el camino para sancionar penalmente el acceso a esta clase de información residual pero tan reveladora potencialmente de la intimidad del sujeto que ha generado esa información en su propio equipo terminal.

13.4.5. Otros elementos del tipo

13.4.5.1. Realización del hecho sin el consentimiento del interesado

En todas las variantes examinadas es necesario que el sujeto activo realice la acción correspondiente sin el consentimiento del sujeto pasivo. Por consiguiente, el consentimiento de cada uno de los participantes en la comunicación se configura como el eje sobre el que se vertebra el marco de licitud de aquélla en relación con terceras personas.

El consentimiento del interesado excluye, desde luego, la tipicidad del hecho, es decir, de las diversas conductas que han sido estudiadas más arriba. En este delito el consentimiento opera como causa de exclusión del tipo y no de la antijuricidad, porque cuando se produce la mediación del mismo (previa o simultáneamente al hecho) no se sustancia ningún menoscabo fáctico del bien jurídico. Esto es así porque este delito pertenece al grupo en los que junto al bien jurídico en cuanto tal se protege la libre disposición del mismo por parte de su titular.

Cuando se trata de la comunicación simultánea entre dos o más personas y una de ellas revela a terceros ajenos a tal comunicación el contenido de la misma o procede a su grabación o registro mediante artificios técnicos o a copiar una imagen, de consistir en un procedimiento audiovisual de comunicación, no concurre el tipo, puesto que el interlocutor es cotitular de la información reservada y está legitimado para hacer uso de ella, salvo que a su vez tenga una obligación previa de secreto laboral o profesional, pero entonces se trataría de un tipo delictivo diferente (art. 199 CP).

Más clara me parece la respuesta al supuesto de captaciones del sonido o la imagen de otro u otros por una persona ajena a la comunicación, pero que cuenta para ello con el consentimiento de uno o varios de los interlocutores. En estos casos, tal consentimiento no excluye la tipicidad, puesto que el partícipe en la comunicación está involucrando a un tercero sin que tal circunstancia sea conocida por los demás, y pueda ser consentida implícitamente.

13.4.5.2. El tipo subjetivo

El tipo subjetivo está comprendido, en primer lugar, por el dolo en cualquiera de sus variantes (directo de primer o segundo grado o eventual), el cual implica la conciencia y voluntad de la realización de todos los elementos objetivos del tipo.

Además, es necesaria la concurrencia de un específico elemento subjetivo de lo injusto, como elemento típico común –al igual que el dolo- para las diversas modalidades típicas ya estudiadas en su vertiente objetiva, consistente en la intencionalidad de "[para] descubrir los secretos o vulnerar la intimidad de otro". Sobre el alcance de ambos componentes subjetivos, que se presentan como exigencia típica alternativa, por lo que se refiere a 1) "descubrir", alude a la captación intelectual del contenido del soporte, a su conocimiento, pero en este caso tal captación ha de recaer sobre un secreto de carácter personal, esto es, sobre un hecho que su titular ha querido dejar fuera del alcance de los demás o tan sólo accesible a un número limitado de personas. 2) En el segundo caso ha de concurrir la intención de vulnerar la intimidad de un tercero, aunque no afecte a un secreto ajeno, conclusión que abunda en la idea de lo superfluo de la referencia expresa al secreto y a su descubrimiento, pues bastaba con la segunda –

vulnerar la intimidad de otro-, que se proyecta explícitamente sobre el bien jurídico protegido y en ella quedaría ya incluida la primera.

Es por ello un delito de intención mutilado de dos actos, el primero de los cuales configura ciertamente la acción típica –apoderarse, interceptar, etc.-, pero quedando el segundo de ellos ya fuera del tipo (el efectivo descubrimiento del secreto o vulneración de la intimidad), cuya comisión quedará en principio en manos del sujeto activo, sin perjuicio de que se pretenda que el descubrimiento lo realice un tercero al que se entrega el soporte correspondiente sin haber entrado en conocimiento de su contenido, lo que podrá dar lugar a su vez a un tipo delictivo distinto (art. 197.3 CP).

La comisión por imprudencia no está tipificada expresamente, por lo que no resulta punible, de acuerdo con la exigencia del art. 12 del CP.

Asimismo, las intromisiones accidentales quedan fuera de la cobertura de este delito.

Así, la STS (2ª) de 30 de abril de 2007:

> "El Tribunal ha explicado que en instancia se negó adecuadamente el carácter típico de la conducta enjuiciada fundamentalmente sobre la base de la ausencia del elemento subjetivo. Aunque es cierto que se accedió a un archivo de correo electrónico y también lo es que existió apoderamiento del contenido de un mensaje concreto dirigido al querellante, no es posible entender que en el ordenador donde se almacenaban físicamente los datos y al que accedieron los acusados era el lugar idóneo para el archivo o almacenamiento de datos relativos a la intimidad personal del querellante, porque se trataba de un instrumento de titularidad pública, adscrito al organismo municipal, y porque además, los dos funcionarios a que se refiere la sentencia lo usaban circunstancialmente y conocían la clave de acceso."

14. TIPOS AGRAVADOS EN RELACIÓN CON LOS ANTERIORES GRUPOS DE DELITOS

Los diversos delitos integrados en los apartados 1 y 2 del art. 197 del CP, ya vistos anteriormente, esto es, contra los datos reservados de carácter personal, contra los mensajes de correo electrónico, interceptación de las comunicaciones y desviación de las mismas, pueden dar lugar a otros delitos más graves (tipos agravados), siempre que concurran las circunstancias que

describe el propio CP en los demás apartados de ese mismo art. 197.

14.1.Por revelación de la información obtenida

Según el art. 197.4.1:

> "Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.
>
> Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior".

Por lo tanto, la acción consiste, alternativamente, en difundir, revelar o ceder a terceras personas los datos o hechos descubiertos o las imágenes captadas.

14.2.Por razón de la calidad o condición del sujeto activo

1. Descubrimiento por los encargados o responsables de los ficheros

El art. 197.5 dispone:

> "Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior".

La calidad que ha de poseer el sujeto activo le convierte en un delito especial. En cuanto al responsable del fichero, es un concepto jurídico que viene determinado en la LOPD. Respecto al encargado, lo será el que asume esas funciones por cuenta del responsable del tratamiento.

Responsable y encargado, según la LOPD, puede serlo también una persona jurídica, y desde 2010 en nuestro sistema jurídico-penal se ha introducido la responsabilidad penal de las personas jurídicas (art. 31 bis).

Podemos distinguir tres tipos delictivos. 1) En cuanto al primer tipo objetivo, la acción será la(s) descrita(s) en el art. 197.1. La

agravación resulta difícilmente concebible en relación con este tipo básico.

2) Respecto al segundo tipo, se refiere a la comisión por el encargado o responsable del fichero de los hechos recogidos en el art. 197.2.

3) El tercer tipo delictivo (superagravado), común a los dos anteriores, consiste en difundir, ceder o revelar la información a la que se ha tenido acceso.

2. Comisión del delito en el seno de organizaciones o grupos criminales.

> "Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado" (art. 197.8).

Este tipo agravado ha sido introducido por la LO 5/2010, y supone reconocer la importancia creciente que están teniendo como sujetos activos de estos delitos las organizaciones –o grupos- criminales.

3. Cometido por funcionario público o autoridad

> "La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años" (art. 198).

No cabe duda, pues, de que estamos ante un tipo agravado.

Sujeto activo lo es, la autoridad o funcionario, que habrá que interpretar con el alcance que otorga a ambos el art. 24 del CP a los efectos penales.

14.3.Por la especial vulnerabilidad del sujeto pasivo

De acuerdo con el art. 197.6 (inciso final):

> "Igualmente, cuando... la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior".

Por menor de edad deberá entenderse el que lo sea de acuerdo con la legislación civil; y por incapaz la definición que establece el art. 25 del CP.

14.4.Por razón de la calidad o vulnerabilidad de la información

Este tipo agravado aparece descrito en el art. 197.6:

> "Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o..."

Es común la opinión de aceptar que entran de lleno en el núcleo de la intimidad los datos referidos a la salud y al origen racial de las personas, los cuales, junto con otros, configuran los llamados datos sensibles o supersensibles, (así, también, los relativos al origen étnico, opiniones políticas, adscripciones sindicales, convicciones religiosas u otras convicciones, la vida sexual). Su calificación como datos supersensibles implica el establecimiento de garantías reforzadas de protección, como es vedar el acceso a la información y a su tratamiento en archivos automatizados si no media el consentimiento del afectado, o limitar en otro caso -por lo general con reserva de ley-, tal acceso y su utilización.

Por su parte, la Directiva de la Unión Europea sobre la misma materia, de 1995, dedica una atención especial a esta clase de datos.

14.5. Cometer el delito con intención de lucro

En realidad son dos los tipos delictivos agravados cuando la acción está presidida por el propósito de lucro, dando lugar a un tipo superagravado si a ese propósito se une un determinado objeto material sobre el que recae la acción o se dirige contra determinado sujeto pasivo.

Art. 197.7:

> "Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años".

Basta la finalidad lucrativa, no es necesario para la consumación del delito haber obtenido efectivamente un lucro.

14.6.Tipo autónomo

Consiste este delito en la revelación de la información obtenida por terceros.

Art. 197.4.2:

> "Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior".

El tipo objetivo consiste en difundir, revelar o ceder a terceros, siempre que esa información no haya sido descubierta previamente por el mismo autor.

El tipo subjetivo, requiere, además del dolo, el conocimiento del origen ilícito de los datos -o hechos- descubiertos -o imágenes captadas.

15. LAS PERSONAS JURÍDICAS, SUJETOS PASIVOS DE ESTOS DELITOS

Las personas jurídicas no sólo pueden ser sujetos activos o autoras de estos delitos (desde 2010), sino que también pueden ser sujetos pasivos o víctimas de los delitos anteriores, puesto que de todos los delitos recogidos en este mismo Capítulo se las considera legalmente sujetos pasivos. La protección de los datos reservados de las personas jurídicas constituye una novedad del CP 1995.

De todos modos, no todas las formas ataque contra la confidencialidad o la intimidad recogidas en estos tipos delictivos son protegidas penalmente en relación con las personas jurídicas. En primer lugar, únicamente aquéllas que afectan a la confidencialidad de los datos reservados de las mismas frente a las conductas de revelación, descubrimiento o cesión.

Por otro lado, dada su peculiar condición, no cabe duda de que no les afectan los datos reservados de carácter familiar y personal, como tampoco todos los que figuran como sensibles en el art. 197.5, sino tan sólo algunos de ellos, como los que se refieren a la ideología, religión o creencias.

16. LAS COMUNICACIONES PRIVADAS EN EL ÁMBITO LABORAL DE LA EMPRESA

En el seno de la empresa se plantean varios problemas en relación con el acceso a los mensajes de correo electrónico de los empleados y a otros accesos y comunicaciones semejantes a través de la red realizados por aquéllos. En resumen, se trata de hipotéticos comportamientos en los que se plantea el acceso al correo del trabajador para comprobar si está utilizando el servicio de correo electrónico y el acceso a la red con fines particulares u otros abusivos.

En cuanto al acceso al correo electrónico privado del trabajador la cuestión es ciertamente compleja. No cabe duda de que, como se vio más arriba, a él se extiende el derecho al secreto de las comunicaciones. En resumen, se trata de información personal de carácter reservado que puede entrar asimismo en el ámbito de protección de la norma penal que estamos estudiando. Por su parte, el empresario puede estar movido por diversos intereses aparentemente legítimos para acceder al correo electrónico de sus empleados, como podría serlo la obtención de elementos de prueba para un despido, o con el fin de comprobar si el trabajador está haciendo uso privado del correo electrónico, y además si lo hace en horas de trabajo, aspectos ambos que podrían comportar un perjuicio económico para la empresa, o cuando sospecha que el correo está siendo usado para la comisión de un delito. Entonces se trata de ver si el empresario puede actuar amparado por una causa de justificación, en concreto la del ejercicio legítimo de un derecho.

La escasa jurisprudencia existente sobre estas situaciones, en todo caso no penal, ha exigido como primer requisito la proporcionalidad entre el objetivo buscado por el empresario y el acceso al correo del empleado, habiendo negado su concurrencia cuando aquél únicamente pretendía acopiar pruebas para fundamentar como procedente un despido.

La Dirección General del Mercado Interno de la Unión y el Grupo de trabajo de la Comisión Europea sobre protección de datos se han pronunciado sobre este asunto, admitiendo la posibilidad de acceso a los mensajes de correo de los trabajadores, siempre y cuando se den una serie de garantías entre las que destacan: a) la necesidad de un propósito especificado, explícito y legítimo; b) que la supervisión sea una respuesta proporcionada sobre un patrón de riesgo, y c) la mínima repercusión sobre los derechos a la intimidad de los trabajadores afectados.

Si existe la sospecha de que el trabajador está cometiendo un delito por medio del correo electrónico u otras comunicaciones por medio de la red deberá ser la autoridad judicial quien tome la decisión de autorizar la intervención de esta correspondencia o comunicación.

Un asunto distinto es el acceso al correo de un trabajador o empleado por otro compañero, cuando se limita a mensajes directamente relacionados con la actividad laboral, sin tener carácter privado, sino institucional (p. ej., acceder a los mensajes de un compañero que contienen información relativa al trabajo y tiene interés general). EL TS entiende que en estos casos se trata de un acceso lícito que no comporta un atentado a la intimidad de la persona cuyos mensajes han sido abiertos (STS 10 de junio de 2011: absolvió al procesado, profesor de Derecho, de los delitos de descubrimiento y revelación de secretos y del delito contra la propiedad intelectual que le imputaba, y que habría cometido al acceder indebidamente a las cuentas de correo electrónico de otros profesores desde ordenadores de la Facultad en la que trabajaba. En cuanto al delito de descubrimiento y revelación de secretos, el TS declara que la conducta denunciada no se corresponde con la tipificada en el art. 197.1, 2 o 5 CP, al tratarse de correos institucionales, de utilización para fines no estrictamente personales, y que eran ajenos a la intimidad o privacidad de sus titulares).

Por otro lado, el TC declara vulnerado el derecho a la libertad sindical (art. 28.1 CE) en relación con el uso del correo electrónico de la empresa para la comunicación sindical.

> En efecto, el derecho a informar a los representados forma parte del contenido esencial de la libertad sindical. Eso implica que podrá hacerla efectiva por los cauces previstos en la ley y por otros que libremente adopte siempre que respete la normalidad productiva. Si bien el empresario no tiene la obligación de dotarse de infraestructura informática para uso sindical, si esa infraestructura existe deberá ponerla a disposición del uso sindical, siempre y cuando se respeten las siguientes reglas y normas de uso, a saber: que la comunicación no perturbe la actividad normal de la empresa, que no se pretenda que prevalezca el uso sindical y que no ocasione gravámenes económicos al empresario (STC 7 de noviembre de 2005).

17. EL CONTROL JURISDICCIONAL DE LA INTERCEPTACIÓN DE LAS COMUNICACIONES

PERSONALES ELECTRÓNICAS CON FINES DE INVESTIGACIÓN PENAL

El sistema legal (más exactamente: las regulaciones introducidas o en camino de serlo mediante ley) introducido en España para el control jurisdiccional de las comunicaciones, que afecta al derecho fundamental al secreto de las comunicaciones, ha sido objeto de diversas críticas.

No es pacífica la consideración de los límites de las intervenciones de las comunicaciones mediante procedimientos tecnológicos. Así, se ha discutido en relación con el Sistema Integrado de Interceptación de las Telecomunicaciones, SITEL, sistema de intervención de terminales móviles automatizado, perteneciente al Ministerio del Interior.

La jurisprudencia se ha ocupado sobre la legalidad de estas técnicas, pero no parece haber encontrado problemas mayores sobre la misma; ha realizado asimismo esfuerzos para establecer los criterios conforme a los que la interceptación de las comunicaciones privadas es conforme a derecho.

> Así, la STS (2ª) de 19 de diciembre de 2008 dice: "respecto de la utilización de herramientas electrónicas, sistema GPS, que pudieran producir injerencias, no autorizadas, en la intimidad del investigado, al permitir, entre otras utilidades, que fuera espacialmente ubicado, el propio Tribunal de instancia, con todo acierto, se encarga de replicar este extremo afirmando que, en efecto, podría asistirle la razón al recurrente si esa localización (SITEL o Sistema de Intervención Telefónica) permitiera conocer el lugar exacto en el que el comunicante se encontraba, pero que, cuando como en este caso, esa ubicación sólo puede concretarse con una aproximación de varios cientos de metros, que es la zona cubierta por la BTS o estación repetidora que capta la señal, en modo alguno puede considerarse afectado, al menos de forma relevante, el derecho a la intimidad del sometido a la práctica de la diligencia". Mencionan o tratan sobre SITEL también las SsTS de 12 (que entra en detalle en los datos que se obtienen y manejan así como en el cumplimiento de una serie de principios y garantías, que a juicio del TS son satisfechos), 13 y 23 de marzo de 2009, que lo califican como un sistema garantista. Por su parte, la STS de 13 de marzo de 2009, f.j. 1º, explica con detalle cómo funciona este sistema y qué tipo de información puede captar y registrar.
>
> Finalmente, la STS (2ª) de 12 de marzo de 2009 menciona cuál era la información solicitada en el caso: los listados de llamadas entrantes y salientes del referido teléfono, así como la titularidad del mismo, si se tratar de contrato y no de tarjeta de prepago; contenido de las carpetas de audio o llamadas; contenido de los mensajes de texto o SMS; contenido de las comunicaciones mantenidas vía fax o Internet;

> identificación y localización de los repetidores; identificación del número que interacciona con el intervenido (llamante y llamado) aunque sean secretos; IMEIS correspondientes a los teléfonos intervinientes; identidad del titular de los teléfonos que interactúan, aunque sean secretos.

Frente a la actitud jurisprudencial, favorable a la legalidad de estas interceptaciones, se objeta contra este sistema y otros similares que pudieran implantarse que en muchas ocasiones dan lugar a la acumulación de muy abundante y variada información, incluida la localización geográfica aproximada del sujeto intervenido, muchas veces innecesaria para la investigación criminal concreta y, en consecuencia, se entiende que se rebasarían los márgenes que marca el principio de proporcionalidad.

Lo cierto es que dada la abundante información privada que recoge este sistema, la injerencia en el derecho fundamental al secreto de las comunicaciones es extremadamente elevada. Por este motivo, la decisión judicial de autorizar la intervención de la comunicación, de prorrogarla y sobre qué contenidos, debe apoyarse en una motivación muy razonada y ponderada, en particular en relación con la pertinencia de la interceptación de la comunicación en atención a la gravedad del delito o delitos objeto de persecución y en atención a la razonabilidad de los indicios disponibles sobre el sujeto cuyas comunicaciones van a ser intervenidas, evitando de este modo resoluciones rutinarias. Asimismo, deberán tomarse medidas muy estrictas sobre el uso, acceso, custodia y destino (en particular la cancelación) de esa información una vez concluida la investigación policial o, en su caso, el proceso judicial.

Sobre estos detalles tan importantes no parece pronunciarse la ley, por lo que el sistema descansa básicamente en la resolución motivada dictada por el juez, el cual, a su vez, con bastante frecuencia, da por buenas las razones de los investigadores policiales sin otras comprobaciones, exigencias y garantías.