EGUZKILORE
Número 21.
San Sebastián
Diciembre 2007
185 - 199

EL SENTIDO DE LA PRIVACIDAD, LA INTIMIDAD Y LA SEGURIDAD EN EL MUNDO DIGITAL: ÁMBITOS Y LÍMITES

Enrique STERN

Fiscal del Tribunal Superior de
Justicia de La Rioja

Resumen: La utilización de los servicios informáticos como medio de comunicación conlleva la exigencia del respeto de un margen de privacidad por parte del Estado: el derecho al uso pacífico de los sistemas informáticos, con la garantía de no ser perturbado por terceros no autorizados. Tras exponer la normativa internacional, se analiza la legislación interna en relación a estas cuestiones, haciendo especial hincapié en la protección penal de la intimidad y de los datos personales, al utilizar el correo electrónico u otras formas de comunicación de carácter personal al través de Internet.

Laburpena: Informatika zerbitzuak komunikazio modura erabiltzen baditugu, pribatutasun marjina exijitu diezaiokegu estatuari. Hau da, informatika zerbitzuen erabilera baketsua baimendugabeko hirugarrenen nahasmendurik gabe. Nazio mailako arautegia aurkeztu eta gero, barne legeria aztertzen da gai hauen inguruan, intimitatearen eta datu pertsonalen babes penala bereziki kontutan harturik, bai posta elektronikoa erabiltzerakoan edota internet bidez egindako beste komunikazio pertsonalekin.

Résumé: L'utilisation des services informatiques comme moyen de communication implique le respect par l'Etat d'une marge d'intimité: le droit à l'utilisation pacifique des systèmes informatiques, avec la garantie de ne pas être troublé par des tierces personnes non autorisés. Après avoir exposé la réglementation internationale, on analyse la législation interne par rapport à ces questions, en soulignant surtout la protection pénale de l'intimité et des données personnelles, lors de l'utilisation du courrier électronique ou d'autres formes de communication à caractère personnel à travers Internet.

Summary: The use of computer services, as a way of communication, requires the respect of a certain frame of privacy by the State: the right to the normal use of computer systems, with the guarantee of not being disturbed by unauthorized third parties. After explaining the international norms, the internal legislation regarding this matter is analyzed, with a special emphasis on the penal protection of privacy and personal data, when using the electronic mail or other personal communication modalities by Internet.

Palabras clave: Derecho a la intimidad, Servicios informáticos, Derecho penal, Delitos, Protección penal de la intimidad.

(Nota): Contribución a la Jornada sobre "Protección penal de la privacidad en entornos digitales", San Sebastián, 29 noviembre 2007 (subvencionada por el Proyecto DITESEC del programa SAIOTEK, Dpto. de Industria, Comercio y Turismo del Gobierno Vasco).

Gako hitzak: Intimitaterako eskubidea, informatika zerbitzuak, Zigor zuzenbidea, delituak, intimitatearen babes penala.

Mots clef: Droit à l'intimité, Services informatiques, Droit pénal, Délits, Protection pénale de l'intimité.

Key words: Right to privacy, Computer services, Penal Law, Crimes, Penal protection of privacy.

No es preciso ser un sujeto especialmente reflexivo para darse cuenta de que, cuando navegamos por la Red y pasamos de una página a otra radicada en extremos opuestos del mundo, y nos embarga una sensación de intimidad, de secreto y de absoluta soledad, en la seguridad de que nadie es testigo de las páginas que visitamos, nos encontramos en realidad ante una sensación totalmente falsa. Desde la inocente "cookie" hasta el peligroso troyano, el "bug" o el "spy", estamos ofreciendo al mundo en general una cantidad sustancial de información sin que seamos muy conscientes de ello. Si en un mensaje de correo electrónico se incluyen, por ejemplo, fotografías de pornografía infantil, podemos tener la sospecha de que en algún centro de información alguien lo captará; si en el asunto de nuestro correo tecleamos, por ejemplo "Bin Laden", sin duda serán varias las alarmas internacionales que se dispararán.

Sin embargo, es obvio que cuando utilizamos los servicios informáticos para comunicarnos, algún margen de privacidad tenemos derecho a exigir, al menos en un Estado democrático y de derecho. Esto es, el ciudadano tiene derecho al uso pacífico de los sistemas informáticos, utilizando sus posibilidades en la garantía de no ser perturbado por terceros no autorizados.

En el caso español, el derecho que nos protege viene dado tanto desde el ámbito interno como desde el que nos da la pertenencia a la Comunidad Europea. Así, es variada la normativa europea relativa a la protección de los sistemas de información, desde la Decisión Marco relativa a los ataques de los que son objeto los sistema de información, hecha en Bruselas el 19 de abril del 2002 (COM 2002, número 73 final 2002/0086 CNS) cuyo objeto es reforzar la cooperación entre autoridades judiciales y policiales mediante la aproximación de las legislaciones penales de los Estados miembros en materia de ataques contra los sistemas de información, hasta la Decisión Marco 2005/222/JAI del Consejo de Europa, de 24 de febrero, relativa a estos mismos ataques, en los que se unifican las definiciones de lo que debe entenderse por intromisión ilegal, circunstancias agravantes, responsabilidad de las personas jurídicas y competencia judicial para conocer sobre estas infracciones, pasando por infinidad de Decisiones, Convenios y Directrices que protegen el comercio entre personas físicas o jurídicas con independencia del lugar en el que se encuentren, la Directiva sobre Comercio electrónico de 8 de junio de 2000 (Directiva 2000/31/CE, la Directiva sobre Firma electrónica de 13 de diciembre de 2000 (Directiva 1999/93/CE) o la Directiva sobre protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, de 24 de octubre de 1995 (Directiva 95/46/CE).

Dentro del ámbito interno, las normas de garantía se encuentran en la protección que la Constitución Española otorga tanto a la intimidad personal como al secreto de las comunicaciones recogidos en el artículo 18[1] y que se ven desarrolladas tanto en

1. La Constitución Española hace referencia a las comunicaciones postales, telegráficas o telefónicas, pero nadie pone en duda su extensión a todo tipo de comunicaciones privadas cualquiera que sea el medio utilizado (chats privados, correo electrónico, etc.).

el Código Penal como en la Ley de Enjuiciamiento Criminal fundamentalmente, sin perjuicio de que también otras normas procuran su amparo, como por ejemplo, la Ley 32/03 de 3 de noviembre General de Telecomunicaciones, la Ley 34/2002 de 11 de julio de servicios de la sociedad de la información y de comercio electrónico, que desarrolla la Directiva 2000/31/Ce o la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (modificada tanto por la Sentencia del Tribunal Constitucional –Pleno– número 292/2000 de 30 de noviembre, como por la Ley 62/2003 de 30 de diciembre de medidas fiscales, administrativas y del orden social), el Reglamento de Medidas de Seguridad de 11 de junio de 1999 sobre ficheros automatizados que contengan datos de carácter personal.

Dado que la intromisión en datos personales ajenos afecta a derechos fundamentales y conlleva consecuencias penales, es preciso definir previamente los conceptos que se van a utilizar, que en numerosas ocasiones vienen dados por la propia normativa internacional.

Así, por **correo electrónico** la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) entiende que es "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 éste acceda al mismo".

Por "**intromisión ilegal**", la Propuesta de Decisión Marco dada en Bruselas el 19 de abril de 2002 (COM 2002, 173 final)[2] entiende cualquiera de las siguientes acciones:

a) el hecho de obstaculizar o interrumpir de manera significativa sin autorización el funcionamiento de un sistema de información introduciendo, transmitiendo, perjudicando, borrando, deteriorando, alterando o suprimiendo datos informáticos.

b) El hecho de borrar, deteriorar, alterar, suprimir o hacer inaccesibles los datos informáticos en un sistema de información cuando es cometido con la intención de causar un daño a una persona física o jurídica.

Por acceso "**sin autorización**", la Decisión Marco 2005/222/JAI de 24 de febrero señala que será aquel "acceso o la intromisión no autorizados por el propietario o titular de otro tipo de derecho sobre el sistema o parte del mismo no permitidos por la legislación nacional".

El término "**documento**" encuentra dentro del propio Código Penal una definición legal en el artículo 26, a tenor del cual se considera documento "*todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica*". Es ciertamente una definición amplia y abierta, determinada por la finalidad o la aptitud para soportar pruebas de cualquier clase. Sin embargo, la definición legal sigue exigiendo un soporte material, lo cual no siempre existe cuando se trata de documentos virtuales; el documento no se refiere a

2. *http://eur-lex.europa.eu/LexUriServ/site/es/com/2002/com2002_0173es01.pdf*

ese soporte –el disco duro, disquette, servidor, etc.– sino al propio documento en sí sin precisión de soporte alguno, o en todo caso, la visualización de una pantalla del monitor. Es por ello que no se explica[3] que el legislador no haya recogido el criterio de documento que ya señalaba nada menos que en 1985, fecha en la que hablamos de la prehistoria de la informática, cuando la Ley de Patrimonio Histórico 13/1985 en su artículo 49, 1º señalaba que "*Se entiende por documento toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos*", mostrando entonces una clarividencia para las posibilidades de la cibernética que en aquel entonces apenas si se apuntaban con imaginación. Máxime cuando el propio Código Penal los incluye de forma expresa, como susceptibles de ser destruidos, en su artículo 264 dedicado al sabotaje informático. Igualmente, la L.O.P.J. en su artículo 230 amplía el concepto de elemento susceptible de ser utilizado como medio de prueba, cualquiera que fuera el soporte en el que se presente.

En otras ocasiones las definiciones de los términos pertenecen al acervo común, y así, por **secreto** entenderemos como todo aquello que haya querido ser excluido por su titular del conocimiento de terceros, teniendo tal consideración con independencia del contenido de ese mensaje pues la protección del derecho de las comunicaciones tiene una entidad propia, ya que las comunicaciones deberán resultar protegidas con independencia de su contenido, esto es, ya se trate de comunicaciones de carácter íntimo o de otro género. De esta forma, el derecho al secreto de las comunicaciones adquiere un significado propio separado del derecho a la intimidad configurándose, pues, como un derecho autónomo, si bien debe tener un contenido que afecte a la intimidad de quien lo posee, pues en definitiva ése es el bien jurídico protegido en el Código Penal en su artículo 197. Además, ese secreto debe ser actual, no pudiendo ser objeto de protección aquel que ha sido abandonado[4], por ejemplo si tras imprimirlo se tira a la basura, demostrando así su titular que la preservación de ese secreto ha dejado de tener interés para él, abandono que debe ser distinguido del descuido en su conservación, por ejemplo dejando el mensaje en el monitor y ausentándose momentáneamente del lugar donde se encuentra el ordenador.

Debe además, tenerse en cuenta que el correo electrónico ofrece información vestibular[5], sin necesidad de acceder a su contenido: cualquiera que sea el programa utilizado para la remisión o recepción del correo, éste recoge datos del remitente y a quien se ha remitido; los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión. También pueden referirse al formato en que la red conduce la comunicación, la existencia de archivos

3. José Manuel Maza Martín, "La necesaria reforma del Código Penal en materia de delincuencia informática", en *Estudios jurídicos del Ministerio Fiscal*, II del 2003, pág. 305.

4. Carlos María Romeo Casabona, "La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras formas de comunicaciones de carácter personal a través de internet y problemas sobre la ley penal aplicable", en *Estudios jurídicos del Ministerio Fiscal,* II del 2003 pág. 78.

5. Manuel Marchena, Dimensión jurídico penal del correo electrónico, XX premio LA LEY

adjuntos, etc. (campos de cabecera o propiedades del documento), pudiendo acceder incluso a la agenda –o libreta de direcciones– en la que cada usuario recoge las direcciones de correo más frecuentes. Estos datos, que no son garantizados por el secreto a las comunicaciones, sí se encuadran dentro del derecho a la intimidad de la forma en que lo protege el artículo 8 del Convenio Europeo de Derechos Humanos. Así, el Tribunal Europeo[6] ha entendido que los informes generados en el proceso de remisión de los datos se encuentran también protegidos como parte del derecho a la intimidad de las personas y la Directiva 2002/58/CE de 12 de Julio ya citada[7] garantiza el tratamiento confidencial de estos datos.

Sin embargo, el concepto de secreto debe tener una interpretación restringida desde el momento en que el legislador no ha pretendido sancionar al "usuario no autorizado", sino a quien pretenda descubrir los secretos de otro, por lo que quedarán fuera del tipo penal aquellos "hackers" que se limiten al escaneado de los puertos de un ordenador desde otro con control remoto, si bien se planteará la duda de aquellos que, una vez accedido a la computadora, observan la estructura del disco duro contemplando sus archivos; se puede concluir que, el mero visionado de los directorios de un disco duro no conllevará descubrimiento de secreto alguno, pero sí que podrá incidir en el tipo penal el hecho de entrar en las ramas del disco abriendo las diferentes carpetas, conducta que, por lo demás, tiene una difícil justificación en aras a evitar la ilicitud de la finalidad de la intromisión. Parece que la "sustracción" de las contraseñas o passwords empleados no deben ser considerados como secretos por sí mismos[8], sin perjuicio de considerarlos como actos preparatorios de otro tipo de actividad delictiva.

Siguiendo con el problema de las definiciones de los términos empleados, nos encontramos con la palabra "**interceptar**"[9], que según el Diccionario de la Lengua Española significa "*apoderarse de una cosa antes de que llegue al lugar o a la persona a la que se destina, obstruir una vía de comunicación o acceder a la comunicación de otros sin obstruir o interrumpir esa comunicación*". El sentido de interceptación que sugiere el artículo 197 del Código Penal hace referencia a aquellos accesos a la comunicación entre otras personas que no la interrumpen ni impiden que llegue a su destinatario, si bien conociendo su contenido u observando la relación entre remitente y remitido; las comunicaciones bien pueden ser escritas, telegráficas, telefónicas o por medios técnicos del correo electrónico, ya sea cuando el mensaje se halle en el servidor, ya cuando haya accedido al ordenador del destinatario, con independencia de que

---

6. STEDH de 2 de agosto de 1984 –caso Malone- y de 30 de julio de 1998 –caso Valenzuela Contreras–.

7. Artículo 5 Confidencialidad de las comunicaciones 1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad.

8. Jose Manuel Maza Martín, "La necesaria reforma del Código Penal en materia de delincuencia informática", en *Estudios jurídicos del Ministerio Fiscal*, II del 2003, pág. 301.

9. Carlos María Romeo Casabona, op. Cit. Pág. 85

éste lo haya ya abierto o no. Por tanto, no concurre dicha interceptación cuando es uno de los comunicantes[10], ya sea el emisor o el receptor, quien guarda, graba o copia el mensaje, y su difusión no vulnerará el derecho al secreto de comunicaciones salvo cuando expresamente se encuentre sancionado[11], como son los supuestos de secretos profesionales o laborales del artículo 199 del Código Penal.

A diferencia de lo que ocurre con la interceptación de las conversaciones telefónicas, en las que la actividad se produce mientras dicha conversación se está llevando a cabo, la del mensaje o del correo electrónico puede llevarse a cabo tanto antes de que llegue a su destino, mientras se halla en la "bandeja de salida" del remitente, como cuando éste se encuentre en el servidor, al igual que también puede darse cuando el destinatario ya lo haya recibido y conservado en su poder o incluso enviado a la bandeja de elementos eliminados, en la creencia de que con ello destruía el documento.

De la misma manera, el término "interceptación" impide que la mera escucha de una conversación telefónica por hallarse en las inmediaciones sin utilizar ningún medio técnico o electrónico pueda considerarse vulneración de secreto[12].

Para que exista difusión ilícita, ésta tendrá que haber sido realizada "**sin autorización**" de su titular. Ya la propuesta de decisión marco del consejo de Europa de 19 de abril del 2002 en su artículo 2º g) señalaba que el término "sin autorización" es amplio y deja libertad a los Estados miembros para definir de manera concreta el delito, que ha pasado al artículo 2 d) de la Decisión marco 2005/222/JAI de 24 de febrero al entender que será sin autorización "el acceso o la intromisión no autorizados por el propietario o titular de otro tipo de derecho sobre el sistema o parte del mismo o no permitidos por la legislación nacional". Por tanto, para valorar el consentimiento de su titular, ya explícito o ya tácito, es válida la doctrina civilista acerca del mismo, si bien se deja claro que existen intervenciones legítimas por parte del Estado en las comunicaciones a través de la red, como son los supuestos de prevención para la comisión de determinados delitos (por ejemplo, pornografía infantil, incitación a la xenofobia, terrorismo, etc.), así como la obligación que se impone a los prestadores de servicios de interrumpir la prestación en cuanto detecten que vulneran determinados principios singularmente protegidos (el orden público, la defensa nacional, la salud pública, etc.). El hecho de acceder a información con conocimiento de su titular será no una causa de justificación, sino un supuesto de atipicidad de la acción, al exigirlo así el tipo penal del artículo 197.

En el reino del derecho penal, las acciones objeto de sanción vienen determinadas siempre por el verbo rector que define la conducta como delito. Por lo que respecta a la ofensa a la intimidad, el Código Penal se refiere "*al que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento,* ***se apodere*** *de sus papeles,*

---

10. El levantamiento del secreto por uno de los intervinientes no se consideraría violación del artículo 18.3 CE, sino, en su caso, vulneración del derecho a la intimidad (art. 18. 1 CE) o, según lo expresaba la STC 114/1984, sobre los comunicantes pesa, en todo caso, " un posible 'deber de reserva' que –de existir– tendría un contenido estrictamente material, en razón de cual fuese el contenido mismo de lo comunicado".

11. Carlos María Romeo Casabona, op. Cit. Pág. 90.

12. Sentencia de la AP de Guipúzcoa de 17 de febrero de 2000, no existe interceptación al escuchar una conversación a través de una cabina telefónica situada en un lugar público.

cartas…", etc. Lo cierto es que la redacción del Código Penal actual en su artículo 197 tiene como único elemento original el haber incluido expresamente los mensajes de correo electrónico entre los documentos susceptibles de poseer secretos; sin embargo, el resto de su articulado es semejante al artículo 497 del anterior Código Penal de 1944 (Texto Refundido de 1.973), incluido el verbo "apoderarse"[13], y ello pese a que han sido varias las críticas vertidas por la doctrina. Con mayor razón actualmente, este verbo debe ser interpretado de una forma más espiritualizada que antes dado que el apoderamiento de los mensajes de correo electrónico puede efectuarse sin que el mensaje en sí sufra la más mínima intromisión, pudiendo realizarse, por ejemplo, librando una copia desde el servidor hasta un tercero no autorizado, o recuperarse una vez destruido por el destinatario.

Este verbo ha sido especialmente desarrollado por la doctrina cuando ha tratado los delitos contra el patrimonio. Así, el Código Penal emplea este mismo verbo en el delito de robo, para distinguirlo precisamente del hurto, en el que el verbo "tomar" hace referencia a una sustracción astuta y no percibida por la víctima, a diferencia del robo, en el que la conducta del apoderamiento ha sido entendida como el vencimiento de un impedimento colocado por el titular del objeto, ya con violencia o intimidación, ya venciendo los sistemas de protección existentes en el exterior continente para obtener el objeto apetecido (contenido). Cierto es que ya el Código de 1995 imponía una interpretación integradora de la fuerza del apoderamiento al incluir el descubrimiento de las claves (238,3º) o la inutilización de sistemas de alarma o guarda (238,5º) aunque fueran formas inteligentes y no violentas sobre los objetos, pero cuando nos enfrentamos al apoderamiento de secretos viene a ser necesaria una vuelta de tuerca más para su interpretación correcta.

Está claro que el apoderamiento de secretos no exige ni fuerza material ni violencia de ningún género; que puede realizarse incluso sin tener dominio de ningún tipo sobre el mensaje, por ejemplo remitiendo copias desde el servidor mismo, y que la fuerza empleada es únicamente de forma técnica, por ejemplo abriendo el correo en un ordenador encendido, en el que el correo aparece sin ningún sistema de cifrado ni de clave, y tampoco precisa de ningún desplazamiento o traslación del mismo ni siquiera efectuado de forma electrónica.

Sin embargo, la espiritualización del verbo apoderarse no puede llevarse a extremos absolutos, siendo imprescindible que se venza de cualquier modo la oposición del titular, por insignificante que sea su gesto de discreción, por ejemplo, cuando el titular minimiza la pantalla con el mensaje abierto, o cuando, una vez impreso, lo guarda o le da la vuelta con el inequívoco afán de impedir nuestra visión: en estos casos, restaurar la pantalla o voltear la hoja impresa para conocer el contenido del mensaje constituyen verdaderos actos de apoderamiento, tal como lo constituye el acto de quien extrae una carta que no le pertenece de un sobre aun cuando esté previamente abierto. No lo serán, tal y como se señaló anteriormente, la recogida de las hojas arrojadas a la basura cuando el titular ha hecho un efectivo abandono a su suerte del secreto, si no ha tomado las medidas imprescindibles para su destrucción. No es equiparable al abandono implícito, el hecho de

13. Carlos María Romeo Casabona, "La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras formas de comunicaciones de carácter personal a través de internet y problemas sobre la ley penal aplicable", en *Estudios jurídicos del Ministerio Fiscal,* II del 2003 pág. 79.

que el destinatario haya remitido los mensajes a la "bandeja de elementos eliminados" o a la "papelera de reciclaje", que, si bien informáticamente sólo son archivos distintos en el disco duro de un ordenador, perfectamente recuperables mediante simples movimientos de ratón, sin embargo muestran la voluntad inequívoca del sujeto de evitar que dichos documentos puedan ser contemplados por otro sujeto distinto.

No es necesario el uso de sistemas de desencriptación del mensaje ni de descubrimiento de las claves de acceso que, en caso de ser utilizados, redundan claramente en el concepto de uso de apoderamiento forzado. El mensaje goza de protección legal aun cuando se haya remitido sin hacer uso de ningún sistema de cifrado de sus datos. Es igualmente indiferente para la comisión del delito el terminal desde el cual se obtiene la información, pudiendo ser tanto el propio sistema informático del destinatario como la interceptación del mismo desde un tercer sistema ajeno y lejano para la comisión del tipo.

Cuestión distinta sería la apertura del correo recibido por error, ya porque se envió a varios sistemas informáticos, ya porque el mensaje fue posteriormente reenviado a otras personas, alguna de ellas no autorizadas. Dado que el sentido del verbo apoderarse requiere de una conducta positiva, una conducta de hacer, no lo cometerá quien recibe el mensaje y lo abre en un sistema para cuyo acceso está autorizado.

De la misma forma, si el apoderamiento precisa la remoción de un obstáculo[14], por mínima que sea la conducta desplegada por el agente, el hecho de visualizar pasivamente el contenido del mensaje que aparece en la pantalla, por ejemplo leyendo por encima del hombro de quien resulta ser su destinatario, tampoco puede entenderse como constitutivo de infracción al secreto de comunicaciones.

Desde luego no son aplicables las teorías sobre la consumación del apoderamiento existentes para el delito de robo: éstas varían desde las posiciones extremas, bien siendo suficiente para la consumación el mero contacto con el objeto o bien precisando que sea extraído del poder de su dueño para la consumación, hasta las intermedias en las que bastaría la individualización del objeto o la mera disponibilidad, aun cuando fuera de manera ideal, del objeto para su consumación, entendiendo que el delito quedaría en tentativa en los demás supuestos. Al ser el delito de descubrimiento de secretos un delito intencional y de resultado cortado, será bastante para su consumación el hecho de copiar o de reenviar el mensaje aun sin ser preciso en ningún caso que el sujeto activo haya llegado a conocer su contenido.

En conclusión, todo parece indicar que el término utilizado de "apoderarse" no es el idóneo para englobar la totalidad de las conductas que el Código Penal pretende sancionar en materia de revelación de secretos, hallándonos ante una alarmante interpretación amplia –espiritualizada– de dicho verbo, y por ello el informe que sobre el anteproyecto de Ley Orgánica de modificación de la L.O. 10/95 de 23 de noviembre, del Código Penal emitió el Consejo Fiscal acerca de la redacción del Título X del Libro II propuso incorporar un nuevo tipo penal que tuviese como finalidad el proteger la intimidad a través del castigo expreso de la conducta de quien acceda a datos o programas contenidos en sistemas informáticos, tratando además, de dar respuesta a las normas armonizadoras de la U.E. y concretamente cumpliendo la obligación exigida en la De-

14. Carlos María Romeo Casabona, op. Cit. pág. 82.

cisión Marco 2005/222/JAI, de 24 de febrero, ya citada, interesando la creación de un nuevo párrafo tercero con el siguiente contenido: "*3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, será castigado con pena de prisión de seis meses a tres años*".[15]

La revelación de secretos es un delito doloso, no solamente porque no existe un paralelo culposo en su redacción (artículo 12 del Código Penal), sino también porque exige un elemento subjetivo de injusto, consistente en ese afán de descubrir los secretos ajenos o vulnerar su intimidad, finalidad que debe regir la conducta del agente.

Habiendo dejado sentado que el uso de un ordenador personal constituye un acto que se halla dentro de la intimidad de las personas, que en su interior se guardan datos que pertenecen al arcano secreto de sus poseedores y que un ataque al mismo constituye una infracción penal, será también preciso señalar que ese secreto que garantiza puede ser utilizado para la comisión de ilícitos penales o guardar datos relevantes para su descubrimiento o evitación, y en ocasiones será preciso el acceso a sus datos con o sin el consentimiento de su titular. Aquí el problema que se presenta es la deficiente regulación legal. Así, nuestra Ley de Enjuiciamiento Criminal (cuyo texto provisional data de 1882), obviamente nada recoge que haga referencia al trato que merecen las computadoras. El problema es que, pese a las reiteradas reformas acaecidas incluso por motivos de menor entidad, sigue sin señalar con claridad la forma en que la aprehensión y el acceso a un ordenador o la interceptación de los mensajes que se transmiten efectuado por los agentes de policía pueda servir de prueba en un juicio penal sin el riesgo de ser declarada nula por aplicación de artículo 11 de la L.O.P.J., y no sólo esa diligencia probatoria sino además todas aquellas que de ella traigan consecuencia (teoría de los frutos del árbol envenenado, que de ascendencia anglosajona, ha venido al derecho continental en todo su esplendor).

Para ello nos veremos obligados a servirnos de las reglas de la analogía sin que ni aun así queden suficientemente aclarados los requisitos obligados: así, si en el concepto "correo electrónico" incidimos en la primera de estas palabras[16], el término "correo" hará inclinarnos por aplicar las normas que la Ley rituaria establece para la "apertura de la correspondencia escrita y telegráfica" ubicada en el Título VIII del Libro II (Del

---

15. "*La Decisión Marco arriba mencionada y que inspira el nuevo precepto, permite a los Estados, conforme a lo dispuesto en el apartado 2 de su artículo 2, la libertad de opción entre sancionar de una forma general y amplia toda conducta de acceso a los datos contenidos en un sistema de información o bien tipificar únicamente la conducta de acceso cuando se realice con vulneración de medidas de seguridad.*

Entre estas dos posibilidades, castigar cualquier conducta de acceso sin autorización o sólo la más grave acción de quien para llegar a los datos requiere una actividad más clara y directa de vulneración de la intimidad en cuanto que para obtener la información debe realizar actuaciones dirigidas a superar la barrera de seguridad impuesta por los titulares o gestores de los datos, el prelegislador español opta por imponer sólo la sanción penal a quien para obtener los datos debe superar alguna medida de seguridad.

Es ésta una opción que el Consejo de la Unión deja al legislador, por lo que tratándose de una decisión de política criminal no merece comentario técnico-jurídico, si bien de cara a la evaluación y respuesta ante la UE convendría justificar las razones de la opción en la Exposición de Motivos".

16. Manuel Marchena Gómez, *op. cit.*

Sumario), artículo 579, 1º[17] así como los siguientes hasta el artículo 588, mientras que si hacemos hincapié en el término "electrónico", más parece que la normativa aplicable sería la propia para las interceptaciones telefónicas.

Sin embargo, ninguna de las dos puede ser aplicada en bloque: la apertura de correspondencia exige, además de lo reglamentado en los artículos 563 y 564 (artículo 580) relativos a la entrada en lugar cerrado, en primer lugar, que los mensajes sean enviados inmediatamente al Juez de Instrucción de la causa (artículo 581), así como a la citación del interesado, el cual podrá presenciar por sí mismo la apertura de su correspondencia, o designar a otra persona que actúe en su lugar (artículo 584), debiendo el Juez abrir por sí mismo la correspondencia para que, después de leerla para sí, aparte la que haga referencia a los hechos de la causa para conservarla, devolviendo la restante (artículo 586 y 587), haciendo constar por diligencia cuanto haya ocurrido, diligencia de la que levantará Acta el Secretario firmando todos los asistentes (artículo 588). Obviamente la normativa plena relativa a la apertura de correspondencia no puede ser aplicable en bloque bajo pena de hacerla artificiosamente complicada.

Otro tanto puede decirse por lo que respecta a la interceptación de las conversaciones telefónicas, recogido en el artículo 579 párrafos 2º y 3º[18]. Téngase en cuenta el hecho de que en muchas ocasiones la comunicación no se ha producido, pudiendo haber sido simplemente enviada y todavía no recibida por el destinatario, por ejemplo localizándola en el servidor, o por el contrario, será más frecuente que dicha comunicación haya cesado hace ya tiempo, y se encuentre en el disco duro del ordenador como elemento recibido, ya haya sido leído o todavía no haya logrado abrirlo, o incluso lo haya ya eliminado de la bandeja de entrada, por lo que carece de sentido la aplicación de los postulados que jurisprudencialmente han venido a ser exigidos para las interceptaciones telefónicas (totalidad, indemnidad de las grabaciones, cintas originales, transcripción bajo fe del Secretario judicial, etc). De hecho, la legislación comunitaria más parece inclinarse por proteger la intimidad (artículo 1º de la Directiva 2002/58/CE de 12 de julio de 2002[19], señalando incluso en su Considerando 27 la conveniencia de destruir y eliminar los datos del tráfico en el momento exacto en el que termina una comunicación salvo a efectos de facturación, y no para garantizar el secreto de las comunicaciones, que no tiene sentido cuando éstas ya han terminado.

---

17. "*1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa*"**.**

18. *2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.*

*3. "De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos"***.**

19. Artículo 1 **Ámbito de aplicación y objetivo** 1. "*La presente Directiva armoniza las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular,* ***del derecho a la intimidad****, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad*".

De todas formas, la aplicación de las más elementales normas de garantía constitucional[20] imponen la obligada observancia de los principios generales aplicables a toda intromisión en un derecho fundamental[21]: en primer lugar, que sea absolutamente necesario para la investigación dentro de un procedimiento penal ya incoado, dando preferencia a otros medios menos invasivos de la intimidad cuando fuera posible, precisando de una causa grave que justifique el acto de injerencia. En segundo lugar, que la prueba del hecho se derive de la intervención como causa a efecto, esto es, que de la intervención se pretenda obtener pruebas sobre el hecho investigado. En tercer lugar, que se trate de investigar un hecho grave, no siendo suficiente la intervención por infracciones administrativas ni tampoco por infracciones veniales. La gravedad puede venir determinada por varias circunstancias, siendo de entre ellas una fundamental la pena que el Código Penal imponga al delito que se pretende descubrir. Por último, debe aplicarse el principio de transparencia, de modo que la intervención, el "volcado" de los datos y el examen de su contenido no queden bajo secreto sino a la luz de la garantía judicial y con la fe del Secretario judicial.

Siempre será preciso una Resolución judicial que deberá revestir forma de Auto, suficientemente motivada y que individualice lo mejor posible el sujeto a investigar de manera que no deje duda sobre su identidad, la sede o domicilio donde se encuentre el equipo informático, los sistemas y soportes de todo tipo que deberán ser requisados y cuantas circunstancias sirvan para dirigir a los agentes de policía a la mayor concreción de los objetos apetecidos y no otros.

El examen de un disco duro, más que una apertura de correspondencia debe ser considerado como un acto pericial[22], por lo que le será de aplicación lo dispuesto en el artículo 336[23], permitiéndose al imputado no sólo su presencia sino también su participación activa en el sentido de poder designar a otro perito a su costa para que presencie el examen y en su caso, confeccione su propio informe que pueda contradecir al oficial en el desarrollo de juicio oral.

Para ello, el examen se realizará en dependencias generalmente ajenas al Juzgado, por lo que será preciso proceder a un volcado del disco duro en otro aportado para la ocasión, sobre el que se efectuarán los análisis correspondientes, permaneciendo el disco original en la sede judicial y bajo la salvaguarda de la tutela del Secretario judicial, quien garantizará la indemnidad del mismo, otorgando la fe pública judicial en la exactitud e integridad de las copias efectuadas y entregadas a la policía y a las partes para su trabajo.

---

20. Francisco Alexis Bañuls Gómez, "Las intervenciones telefónicas a la luz de la jurisprudencia más reciente", en *Noticias jurídicas*, febrero 2007.

21. Manuel Marchena Gómez, *op. cit.*

22. Manuel Marchena Gómez, *op. cit.*

23. **Artículo 336: "***En los casos de los dos artículos anteriores ordenará también el Juez el reconocimiento por peritos, siempre que esté indicado para apreciar mejor la relación con el delito, de los lugares, armas, instrumentos y efectos a que dichos Artículos se refieren, haciéndose constar por diligencia el reconocimiento y el informe pericial.*

*A esta diligencia podrán asistir también el procesado y su defensor en los términos expresados en el artículo 333"***.**

Una vez sentada la exigencia de resolución judicial motivada, es preciso concretar cuál de entre todos será el Juez competente para ordenar el examen de los ordenadores. La competencia funcional corresponderá a la de un órgano que actúe en una primera instancia, sin perjuicio de que sus resoluciones puedan ser susceptibles de recurso de apelación ante un órgano superior, que será la Audiencia Provincial. Tampoco arroja dudas la competencia objetiva pues, tratándose de la investigación de las causas por delito la competencia recae sobre los Juzgados de Instrucción (artículo 14, 2º LECrim.), ya lo sea el del lugar donde el delito se hubiere cometido o ya el Central de instrucción de la Audiencia Nacional para la Instrucción de los delitos cuyo conocimiento y fallo correspondan por ley a la Audiencia Nacional.

Sin embargo, la atribución territorial sí que puede plantear problemas, dada la simpleza empleada por este artículo para la aplicación de su competencia por razón del territorio, y así, la competencia del Juzgado "*del lugar donde el delito se hubiere cometido*" del artículo 14, se ve completada por el artículo 15 de la LEcrim[24]., en el que se establecen fueros subsidiarios correlativamente de atribución de la competencia en los casos de dificultad para localizar el lugar de comisión del ilícito. Es precisamente en los delitos cometidos por medios cibernéticos donde mayor complejidad puede plantear la identificación del Juzgado competente.

Una primera aproximación indica que el lugar de comisión del delito será aquel donde radica el sujeto que da la orden a su sistema (el hacker) para interceptar o penetrar en el ordenador vulnerado, propio de la teoría de la actividad, tan habitualmente utilizada en el derecho penal. Normalmente, este ordenador víctima se encontrará en cualquier otro punto del planeta, sin añadir incluso que puede ser utilizado un servidor en un tercer país tan alejado del primero como del segundo, por lo que no nos servirá como indicativo la distancia a la que se encuentre, máxime teniendo en cuenta que la agresión puede dirigirse de manera idéntica a una pluralidad de sistemas situados en los emplazamientos geográficos más dispares. En estos casos, el problema ya ni siquiera es de competencia sino que puede alcanzar una pluralidad de jurisdicciones diversas, por lo que el primero de los problemas a dilucidar será precisamente si corresponde o no a los Tribunales Españoles la investigación. Téngase en cuenta que las posibilidades de conocimiento de la jurisdicción española por delitos cometidos fuera de las fronteras

---

24. **Artículo 15**

Cuando no conste el lugar en que se haya cometido una falta o delito, serán Jueces y Tribunales competentes en su caso para conocer de la causa o juicio:

1º) El del término municipal, partido o circunscripción en que se hayan descubierto pruebas materiales del delito.

2º) El del término municipal, partido o circunscripción, en que el presunto reo haya sido aprehendido.

3º) El de la residencia del reo presunto.

4º) Cualquiera que hubiese tenido noticia del delito.

Si se suscitase competencia entre estos Jueces o Tribunales, se decidirá dando la preferencia por el orden con que están expresados en los números que preceden.

Tan luego como conste el lugar en que se hubiese cometido el delito, se remitirán las diligencias al Juez o Tribunal a cuya demarcación corresponda, poniendo a su disposición a los detenidos y efectos ocupados.

de España se halla recogido en el artículo 23 de la L.O.P.J[25]., y entre el elenco de los graves delitos allí enumerados, no hallaremos los atentados contra la intimidad que estamos tratando, por lo que si el fuero exclusivo de competencia fuera el del lugar donde se encuentre localizado el sistema agresor, habría que concluir que sólo sería competente la justicia española cuando dicho sistema se encuentre localizado en el interior de nuestras fronteras, dando lugar en caso contrario, no a una falta de competencia sino a una verdadera ausencia de jurisdicción para conocer del asunto aun cuando uno, varios o incluso la totalidad de los perjudicados se encontraran en su interior.

Para resolver esta cuestión, no siendo bastante explícito el fuero subsidiario del artículo 15, 4º de la LECrim, y para evitar la zona de impunidad que algunos supuestos fácilmente imaginables ocasionan, la Sala Segunda del Tribunal Supremo llegó al Acuerdo no jurisdiccional en Pleno –y por tanto obligatorio– de fecha 3 de febrero de 2005[26] en el que el Alto Tribunal se inclina por la teoría de la ubicuidad en materia de represión penal, fijando incluso en dicho Acuerdo el término "jurisdicciones", con lo que facilita la interpretación que permite asumir la competencia española en el caso de uno solo de los actos criminales haya producido un resultado en España al poder reputarlo cometido en nuestro país. Sin embargo, la mera ubicación del servidor en España no parece que pueda ser considerado como suficiente para entender cometido

---

25. Y ello pese a que por L.O. 13/2007 de 19 de noviembre de 2007 (B.O.E. 278 de 20 de noviembre), acaba de ser reformado en materia de persecución extraterritorial del tráfico ilegal o la inmigración clandestina de personas en el sentido de incluir otros delitos en el sentido siguiente:

Artículo primero. Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial:

Uno. Se modifica el apartado 4 del artículo 23 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que quedará redactado como sigue:

4. Igualmente será competente la jurisdicción española para conocer de los hechos cometidos por españoles o extranjeros fuera del territorio nacional susceptibles de tipificarse, según la ley penal española, como alguno de los siguientes delitos:

a. Genocidio.

b. Terrorismo.

c. Piratería y apoderamiento ilícito de aeronaves.

d. Falsificación de moneda extranjera.

e. Los delitos relativos a la prostitución y los de corrupción de menores o incapaces.

f. Tráfico ilegal de drogas psicotrópicas, tóxicas y estupefacientes.

g. Tráfico ilegal o inmigración clandestina de personas, sean o no trabajadores.

h. Los relativos a la mutilación genital femenina, siempre que los responsables se encuentren en España.

i. Y cualquier otro que, según los tratados o convenios internacionales, deba ser perseguido en España.

26. Acuerdo no jurisdiccional del Pleno de la Sala 2ª del T.S. de fecha 3 de febrero de 2005: "*El delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa*".

en España alguno de los elementos del tipo al ser el nodo un mero cajón desde donde se va a distribuir el programa invasor.

Por último, es preciso señalar que en ocasiones se plantean supuestos en los que la previa intervención judicial puede ser puesta en tela de juicio; estos son los supuestos en los que el ordenador, o incluso la totalidad del sistema informático pertenece a un tercero que autoriza a otro para utilizarlo bajo determinadas condiciones: son los casos en los que el empresario cede su material para que el operario en su tiempo de trabajo utilice el ordenador para desempeñar su trabajo.

De una parte, debe partirse del hecho de que la intimidad de una persona se ejerce no sólo cuando se encuentra en su domicilio, y que el lugar de trabajo también deja el reducto necesario para el desarrollo de esa intimidad a la que toda persona tiene su parcela de derecho, así como que el artículo 197 no hace distinción alguna a este respecto.

De otra parte, también es preciso señalar que el empresario tiene derecho al acceso de los datos relativos a la empresa que se encuentren en sus ordenadores, y que para que constituya infracción penal dicho acceso debe ser ilegítimo; que tiene igualmente derecho a la inspección sobre los instrumentos y herramientas de trabajo de su propiedad cedidos a los empleados para el desempeño de su labor, que el trabajador en general actuará dentro de la empresa y en sus relaciones frente a terceros como mandatario de empresario, quedando reflejados en el ordenador los mensajes relativos a los pedidos, las facturas, las conversaciones referentes a los pagos, recepción de materiales, etc. que son propios de la empresa y cuyo conocimiento no puede ser restringido al empresario.

Sin embargo, el acceso al correo electrónico propio del trabajador[27], así como al historial mismo de las páginas que ha visitado desde ese terminal de ordenador para controlar el posible abuso en el ejercicio de su trabajo, o la utilización de programas ajenos a la empresa, no puede efectuarla aquél por su propia autoridad para utilizarla en contra del trabajador, por ejemplo, para presentar una denuncia ante la Inspección de trabajo o para fundamentar un despido o el inicio de un expediente disciplinario. Desde el momento en que las comunicaciones son secretas, no cabe que so pretexto de interés empresarial, el empresario acceda a la totalidad de la información del sistema pues daría como consecuencia un abuso desproporcionado de su poder, debiendo recabar en todo caso la autorización judicial para el acceso.

En cualquier caso, es precipitado el dar una solución única a este problema, que deberá resolverse caso por caso y teniendo siempre presente el pacto existente entre el empresario y el trabajador, la naturaleza del trabajo y el tipo de contrato que les una. Así, será difícil impedir el acceso del empresario al ordenador del empleado contable para controlar la contabilidad de la empresa, o el correo electrónico propio de la empresa con el que ésta se comunica habitualmente con su clientela, recibe sus pedidos y contesta a los requerimientos de los clientes, al menos en lo que se refiere al uso del correo en la dirección oficial de la empresa, la que utiliza en el mundo del tráfico mercantil. No así cuando se trata del correo particular del trabajador, aun cuando utilice el mismo sistema informático.

---

27. Carlos María Romeo Casabona, *op. cit*., Pág. 97

BIBLIOGRAFÍA

ARIAS POU, MARIA, "El consentimiento en la contratación electrónica a través de internet", *Diario LA LEY* número 6540.

BAÑULS GÓMEZ, FRANCISCO ALEXIS, "Las intervenciones telefónicas a la luz de la jurisprudencia más reciente", en *Noticias jurídicas*, febrero 2007.

ELVIRA PERALES, ASCENSIÓN, "El derecho al secreto de las comunicaciones, *IUSTEL*, 2007.

MARCHENA GOMEZ, MANUEL, "Dimensión jurídico penal del correo electrónico", XX premio LA LEY.

MAZA MARTIN, JOSE MANUEL, "La necesaria reforma del Código Penal en materia de delincuencia informática", en *Estudios jurídicos del Ministerio Fiscal* II-2003, págs. 285 a 318.

ROMEO CASABONA, CARLOS MARIA, "La protección penal de la intimidad y de los datos personales en sistemas informáticos y en redes telemáticas", en *Estudios jurídicos del Ministerio Fiscal,* III-2001 págs. 273 a 311.

SÁNCHEZ ALMEIDA, CARLOS, "La investigación policial de los delitos relacionados con nuevas tecnologías", en *Estudios jurídicos del Ministerio Fiscal,* III-2001 págs. 585 a 612.

DECISIÓN MARCO 2005/222/JAI del Consejo de Europa de 24 de febrero de 2005.

PROPUESTA DE DECISIÓN MARCO del Consejo de Europa relativa a los ataques de los que son objeto los sistemas de información hecho en Bruselas el 19 de abril del 2002.

DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA.