Riesgos de los delitos relacionados con las tecnologías de la información y las comunicaciones

JUANA MARÍA DOMAICA MAROTO

ABOGADO

En la base de estas conductas, de manipulación y abuso, se encuentra indiscutiblemente un problema de seguridad de la información. Seguridad de la información en un triple aspecto: físico, lógico y jurídico. La seguridad física, quizá al ser la más palpable y cercana, es la que cuenta en nuestro país con un mayor grado de atención a nivel institucional y empresarial.

Introducción

Procede, desde una perspectiva jurídica, acercarse a una realidad que ha ido creciendo y desarrollándose de forma paralela a la extensión e implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en nuestra vida de relación, nos referimos a los riesgos de conductas delictivas relacionadas con las TIC.

Dentro del amplio espectro de estas conductas, aquellas en las que la manipulación de un sistema (como elemento físico), o de un proceso informático (como elemento lógico), produce un desplazamiento patrimonial en favor del autor de la manipulación y en perjuicio de un tercero, serán objeto central del presente estudio.

La aprobación por Ley Orgánica 10/1995, de 23 de noviembre, del nuevo Código Penal español ha dado acogida a nuevas formas de delincuencia, introduciendo entre los delitos contra el orden socioeconómico el de estafa producida mediante manipulación informática

o artificio semejante. Esta nueva regulación incluye a la legislación española entre aquellas que de forma explícita establecen consecuencias penales, la respuesta más contundente del ordenamiento de cada Estado al uso abusivo o manipulación de un sistema informático.

En la base de estas conductas, de manipulación y abuso, se encuentra indiscutiblemente un problema de seguridad de la información. Seguridad de la información en un triple aspecto: físico, lógico y jurídico. La seguridad física, quizá al ser la más palpable y cercana, es la que cuenta en nuestro país con un mayor grado de atención a nivel institucional y empresarial. Sin embargo el responsable de seguridad sabe que de la adecuada respuesta a las exigencias de la seguridad lógica del sistema de información depende, en buena medida, la propia subsistencia del mismo.

Los tres aspectos de la seguridad indicados (físico, lógico y jurídico) son complementarios y en modo alguno excluyentes entre sí. El efecto preventivo que la existencia de una amenaza penal representa, la represión efectiva posterior a la comisión del hecho delictivo y el recurso al sector asegurador constituyen las principales medidas de seguridad jurídica implantadas en el Derecho Español. Sin embargo, la indemnización de la aseguradora, si es que se ha tenido la precaución de contratar un seguro, puede no ser la solución plena si se llega a perder la viabilidad de la propia empresa, organismo o institución. La implementación de medidas de seguridad preventivas, se configura hoy como una necesidad más de todo sistema de información abierto al exterior. Es cada vez más habitual la utilización del sistema informático en una red de comunicación, la expansión en el uso de la red mundial Internet es una realidad incontestable. Los sistemas informáticos han dejado de ser una isla para convertirse en lugares de paso, de recepción y transmisión de información. Desde este planteamiento no puede descuidarse el control de acceso al sistema ni la información que sale de él. La integridad, confidencialidad, disponibilidad, autentificación y el no repudio del envío o recepción de un mensaje son exigencias sin las cuales la indudable potencialidad comercial, económica, educativa y otros usos que la comunicación de los sistemas informáticos proporciona puede llegar a vaciarse de contenido.

La cuestión de la tipificación del delito informático

Antes de la entrada en vigor del nuevo Código Penal español era sostenible defender la dicotomía entre la categoría criminológica y delictual en relación con el conjunto de conductas a las que se hará referencia, diciendo que éstas podían encajar en la condición de conductas criminógenas, pero no eran en puridad delitos. No eran delitos puesto que no estaban tipificadas como tales en la legislación penal. En definitiva, cabía concluir que esas conductas eran factores criminógenos, de alto riesgo, que precisamente por la peligrosidad social que entrañaban exigían una regulación por la legislación penal, como último instrumento de control social, pero que en derecho positivo carecían de reflejo alguno.

Es decir, hasta la aprobación del nuevo Código Penal español ¿dónde se encontraba el obstáculo que impedía hablar con rigor de conductas delictivas? Evidentemente en la tipicidad. Las conductas englobadas dentro del concepto de criminalidad informática, no ofrecía duda, eran antijurídicas, culpables, concurriendo en ellas las circunstancias objetivas de punibilidad, merecedoras de una pena, pero no existía tal pena puesto que no estaban tipificadas, no eran conductas típicas recogidas y reflejadas como tales en el Código Penal o en la legislación penal especial.

La falta de tipicidad impedía hablar de delitos informáticos y dejaba inmersas estas acciones en la nebulosa de los indiferentes penales.

Sin embargo la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal modifica esta situación. El mencionado Código ha optado por atender a la naturaleza del bien jurídico lesionado, para dar cobertura jurídica a aquellas conductas relacionadas con la informática donde ésta aparece como medio o como objeto de la agresión. Así, el nuevo Código utiliza los tipos tradicionales de la estafa, robo, daños, protección de la intimidad... para dar entrada a los ilícitos informáticos. No obstante, algunos tipos dejan traslucir la protección de un nuevo bien jurídico, la información tratada automáticamente, aunque sea a través de un tipo tradicional.

Los nuevos tipos penales de delitos informáticos

El nuevo Código Penal al definir los delitos y faltas define los presupuestos de la aplicación de la forma suprema que puede revestir el poder coactivo del Estado, es decir, la pena criminal.

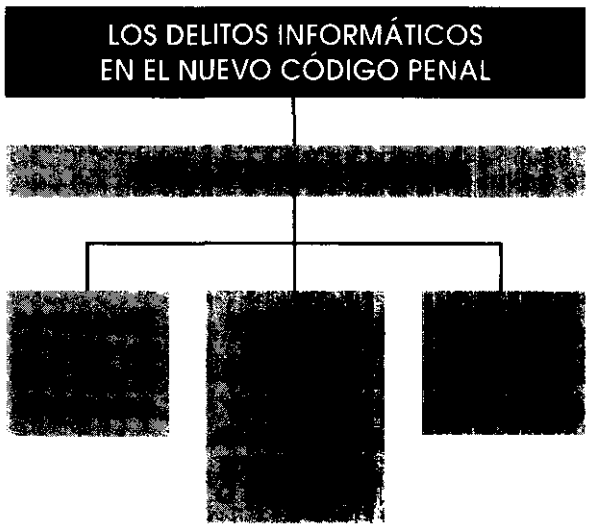
Como la propia Exposición de Motivos que el nuevo Código recoge, se ha afrontado la antinomia entre el principio de intervención mínima del Derecho Penal y las crecientes necesidades de tutela en una sociedad cada vez más compleja. Así, tienen cabida en el nuevo texto formas de criminalidad hasta ahora huérfanas de regulación, como por ejemplo nuevos delitos contra el orden socioeconómico, en concreto la estafa cometida a través de una manipulación informática o artificio semejante.

Esquemáticamente, a continuación, se recogen las figuras delictivas del nuevo Código Penal cometidas con la intervención del medio informático o en las que bienes o derechos relacionados con el tratamiento automático de la información son objeto de agresión. En ambos casos con posibles derivaciones perjudiciales en el ámbito patrimonial y/o de la intimidad personal de las víctimas.

Delitos contra la intimidad con intervención de medios informáticos o telemáticos

La intimidad y el derecho a la propia imagen están penalmente protegidos cuando los datos relativos a tales ámbitos y derechos se encuentren en soporte o medio informático o incorporados a un fichero susceptible de tratamiento informatizado (artículos 197 y 198 del nuevo Código Penal). Brevemente, las conductas tipificadas son éstas:

- Ataques pasivos: apoderarse de mensajes de correo electrónico, interceptar telecomunicaciones, utilizar cualquier artificio técnico de grabación o reproducción de una señal de comunicación.
- Ataques activos: utilización o modificación de datos reservados de carácter personal registrados en ficheros o soportes informáticos, electrónicos o telemáticos, acceso no autorizado a ficheros informáticos que contengan datos personales, difusión, revelación o cesión a terceros de los datos o hechos descubiertos por los métodos mencionados.



El mismo artículo establece agravaciones de las penas para aquellos supuestos en los que las conductas se lleven a cabo por personas encargadas o responsables de los ficheros informáticos, así como cuando los hechos descubiertos afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuera un menor de edad o un incapaz, o se lleven a cabo estas conductas con ánimo de lucro.

El artículo 198 del Código Penal recoge las conductas descritas pero realizadas por autoridad o funcionario público, que fuera de los casos permitidos por la ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, las lleve a efecto.

Por primera vez en Derecho español se plasma en un Código Penal el medio informático, telemático o electrónico como posible instrumento de ataque y soporte del bien jurídico intimidad. Así mismo se crea un título específico «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», remarcando el bien jurídico objeto de protección específica. Con respecto a la regulación anterior se ha producido una clara ampliación del ámbito incriminatorio, ya que se recoge como soporte de los secretos e intimidad de los individuos sus papeles, cartas, mensajes de correo electrónico, o cualesquiera otros documentos o efectos personales. La alusión al medio informático es clara, así como la apertura a futuros soportes de la intimidad de las personas que el avance tecnológico incorpore. Por último, apuntar que se ha producido un incremento de las penas respecto de la regulación contenida en el Código derogado y una penalización de conductas que hasta ahora sólo se consideraban infracción administrativa.

Delitos contra el Patrimonio y el Orden Socioeconómico

El bien jurídico del **Patrimonio y el Orden Socioeconómico** queda protegido frente a los ataques informáticos en el Libro II, Título XIII, en los capítulos II y VI, del nuevo Código Penal. Junto a la consideración de la informática como medio de ataque al patrimonio también se protegen, en el mencionado Título XIII, bienes y derechos relacionados con la informática a través de los delitos de daños y de los relativos a la propiedad intelectual. Así, la informática aparece, en este Título del nuevo Código, como medio de comisión de delitos y también como objeto de protección. De esta forma, se distinguen los siguientes delitos:

- **Robo con fuerza en las cosas**

El Capítulo II, De los Robos, tipificada en los artículos 238 y 239 como **robo con fuerza en las cosas** el uso de tarjetas magnéticas o perforadas perdidas u obtenidas por un medio que constituya infracción penal.

El nuevo Código establece responsabilidades penales por el uso por tercero de tarjeta robada o substraída. De acuerdo con la normativa comunitaria cabe afirmar la exoneración de responsabilidad del titular de tarjeta substraída por los cargos realizados con posterioridad a la denuncia del hecho de la substracción y la limitación de su responsabilidad a 150 euros por las disposiciones anteriores a la denuncia. Pero si se concreta o determina la responsabilidad penal será el responsable penal el que, siguiendo las disposiciones del nuevo Código Penal en relación a la responsabilidad civil derivada de los delitos, deba reparar todos los daños y perjuicios causados.

El vigente artículo 239 determina que a los efectos del presente artículo se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Analizando este precepto, (239 in fine) la utilización ilícita de tarjetas con banda magnética, se subsume claramente en el tipo de robo con fuerza en las cosas. Por tanto los hechos consistentes en la substracción de una tarjeta o la utilización de una tarjeta perdida por

quien no es titular, constituirán un delito de robo con fuerza en las cosas. La tipificación de estas conductas ya había sido propuesta por la doctrina y por la Fiscalía General del Estado.

Sin embargo este precepto, para parte de la doctrina, presenta algunos inconvenientes. La equiparación, en el mismo, del uso ilícito de las tarjetas de crédito o de débito con las tarjetas electromagnéticas en general puede producir un tratamiento equivalente de conductas totalmente distintas.

Así, algunos autores sostienen que en el supuesto de sustracción y utilización de una tarjeta magnética ajena (por ejemplo: tarjetas para apertura de puertas en hoteles), el agente supera el obstáculo puesto por el dueño para la protección de su propiedad, utilizando la tarjeta como si de una llave falsa se tratara. Pero un supuesto totalmente distinto es aquél en el que *el agente utilizando la tarjeta magnética y el número de identificación personal correspondiente accede a los fondos existentes en la cuenta corriente de un cliente de un banco u otra entidad de crédito.* En este caso es el banco o la entidad financiera, la que facilita la disposición patrimonial porque previamente se ha producido un «engaño» que ha conducido a una creencia errónea de que el usuario de la tarjeta era el verdadero titular. *Este segundo supuesto de hecho encaja más dentro del tipo de las defraudaciones y sin embargo se le da un tratamiento equivalente al del robo con fuerza en las cosas.*

Los que utilizan esta vía de razonamiento defienden que *el uso fraudulento por un tercero de las tarjetas de crédito o de débito legítimas substraídas a su titular debe ser castigado no a través del delito de robo con fuerza en las cosas, sino a través del delito de estafa.*

Sin embargo, mantenemos como más adecuada la tipificación como delito de robo con fuerza en las cosas, la utilización de tarjeta legítima por un tercero. En estas conductas aunque existe un engaño a la entidad depositaria de los fondos no se produce una manipulación de un proceso informático, elemento necesario para apreciar la existencia del delito de estafa. Es únicamente la utilización de una tarjeta falsificada, alterada en alguno de sus elementos físicos o lógicos intencionalmente, la que constituye una manipulación del «input». Por tanto, una de las formas de defraudación o manipulación informática propias del delito de estafa. Con la consiguiente transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Hasta aquí la situación queda ordenada si se concreta la responsabilidad penal en uno o varios sujetos, éstos responderán civilmente de todos los daños y perjuicios que su actuación haya ocasionado. El problema surge cuando no se llega a determinar la responsabilidad penal, que indudablemente existe como ya hemos expuesto en la utilización ilegítima de tarjetas electrónicas. ¿Quién soportará el detrimento económico del hecho delictivo: la entidad o el titular de la tarjeta? Ciertamente los fondos se detraerán de la cuenta de cargo asociada en tarjetas de débito o en tarjetas monedero, o bien se efectuará el correspondiente apunte en la cuenta de crédito en tarjetas de esta modalidad. Pero el titular, que observando la diligencia exigida en la custodia del instrumento de pago sufre un robo, hurto o extravío del mismo, no interviene en nada en la acción posterior y son las instalaciones (ATM, cajeros) de la entidad las que sufren el ataque haciendo que dicha entidad falte a uno de sus deberes básicos con su cliente, el deber de custodia del numerario.

Para estos supuestos el artículo 1.101 del Código Civil es claro al establecer que: «*quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de*

sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren el tenor de aquéllas». La entidad tiene obligación de custodiar un numerario del que es propietaria cuando el cliente lo deposita en una cuenta corriente, libreta u otro producto de pasivo, y con más claridad en una cuenta de crédito. Por tanto, la víctima es la entidad emisora debiendo quedar, a nuestro juicio, totalmente ajeno a la acción delictiva el titular de la tarjeta.

El problema fundamental gravita en torno al descubrimiento del delincuente. Algunas entidades emisoras de instrumentos de pago, conscientes de esta dificultad, descargan la responsabilidad sobre el titular de la tarjeta si la disposición se llevó a cabo **con uso NIP** (Número de Identificación Personal). Este es el punto de inflexión utilizado en la mayoría de los contratos de uso de tarjetas, de débito y algunas de crédito, para atribuir responsabilidad en la operación fraudulenta al titular del instrumento. Pero realmente el criterio de atribución de responsabilidad (uso del NIP) no reúne las garantías jurídicas exigibles para apoyar una inversión de la carga de la prueba. Si el artículo 1.214, del Código civil, impone la carga de la prueba de las obligaciones al que reclama su cumplimiento, qué base jurídica asiste a aquellas cláusulas contractuales en la que si una operación con tarjeta se ha efectuado con uso de NIP el que tiene que probar que esa operación no se efectuó es el titular de la tarjeta, cuando resulta que el sistema implementado de uso de NIP no identifica a ese titular. No creemos que se pueda acudir a la autonomía de la voluntad de las partes (1.255 del Cc) cuando se trata de contratos de adhesión. Cabría plantear, por tanto, la existencia de una situación de desequilibrio entre el titular de tarjetas que soporta una sobrecarga o un *plus* de responsabilidad sobre las deficiencias de un sistema, el de cajeros automáticos, que no ha puesto en funcionamiento y del que es un mero usuario y las entidades emisoras y gestoras del sistema. En un justo equilibrio de las obligaciones (como así exige la Ley de Defensa de los Consumidores y Usuarios) en las relaciones entre cliente y entidad si se descarga la responsabilidad en el usuario por transacciones efectuadas con el NIP, en justa reciprocidad, la entidad debería proporcionar una infraestructura de cajero que realmente permitiera identificar a todo aquel que usa la red.

- **Estafas**

El Capítulo VI **«De las Defraudaciones»**, Sección 1.ª **«De las Estafas»** contiene un artículo, el 248.2, que dispone:

> ***«También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero».***

Con este artículo queda tipificado como delito de estafa tradicional el «fraude informático». Para ello se ha sustituido el término «engaño» propio del delito de estafa, por el de «manipulación», evitando así las críticas o dificultades que mostraba el tipo de la estafa para considerar producido el mismo sobre una máquina y no directamente sobre una persona. Esta «manipulación», como más adelante tendremos ocasión de analizar, se puede producir en el *input* o entrada de los datos, en el proceso de los mismos, o bien, en el *output* o salida. En cualquier caso, las conductas tipificadas en este párrafo 2.º del artículo 248 plantearán cada vez con más frecuencia, con la generalización en el uso de la red Internet, el problema de la ley penal aplicable. Nos estamos refiriendo a las denominadas manipulaciones a distancia en las que el lugar de comisión de los hechos delictivos (manipulación) no coincide con el lugar donde se produce el resultado dañoso (transferencia fraudulenta). La aplicación del derecho penal dominada por el principio de la territorialidad hará necesario acuerdos internacionales con soluciones al respecto.

El artículo 249 del nuevo Código Penal fija una serie de pautas a las que tendrá que sujetarse el juzgador para la fijación de la pena en el delito de estafa. Así este artículo 249 dispone que:

> *«Los reos de estafa serán castigados con la pena de prisión de seis meses a cuatro años, si la cuantía de lo defraudado excediere de cincuenta mil pesetas. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los MEDIOS empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción».*

Aunque el artículo termina con la referencia amplia «y cuantas otras circunstancias», la doctrina opina que la redacción del precepto obliga al Juez o Tribunal a motivar la pena que imponga.

Hemos destacado, en mayúsculas, un elemento que puede tomarse en orden a la graduación de la pena, los MEDIOS empleados en la comisión de la estafa, ya que entendemos que la estafa cometida a través de medios informáticos debe resultar afectada por este elemento de graduación.

Pero en la determinación de la pena aplicable a un supuesto delito de estafa cometida por medios informáticos no sólo debe tenerse en cuenta este artículo 249, sino también, el artículo 250.1.7.º que establece:

> *«250.1. El delito de estafa será castigado con las penas de prisión de uno a seis años y multa de seis a doce meses, cuando:*
>
> *(...)*
>
> *7.º Se cometa abuso de las relaciones personales existentes entre víctimas y defraudador, o aproveche éste su credibilidad empresarial o profesional».*

La agravación que recoge este artículo 250 presenta dos escalones:

- uno para el caso de que concurra una única circunstancia de agravación, como por ejemplo la del número 7.º y,
- otro que recoge el mismo artículo 250.2 para el caso de que concurran juntamente las agravantes de los números 6.º o 7.º con la 1.ª. En estos casos la pena a imponer será de prisión de cuatro a ocho años y multa de doce a veinticuatro meses.

Creemos que en las conductas de estafa informática podrá apreciarse en muchas ocasiones este segundo tramo en la agravación, ya que, si la estafa recae sobre sueldos, salarios, depósitos u otros activos de la víctima y, revistiendo especial gravedad la defraudación, coloca a aquélla en una comprometida situación económica, la pena puede llegar a los ocho años de prisión y multa de hasta veinticuatro meses.

- **Daños**

Dentro del mismo Título XIII, por tanto dentro del ámbito de protección penal del mismo bien jurídico (Patrimonio y Orden Socioeconómico), el Capítulo IX **«De los Daños»** para aquellos que excedan de cincuenta mil pesetas, el artículo 264.2 dispone:

> *«La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.*

La protección que otorga este artículo recae directamente sobre la información tratada de forma automática entendiendo que su destrucción lleva aparejados menoscabos importantes en el patrimonio de sus propietarios.

- **Piratería de «software»**

El Capítulo XI, del ya citado Título XIII, bajo el título **«De los Delitos relativos a la Propiedad Intelectual e Industrial al Mercado y a los**

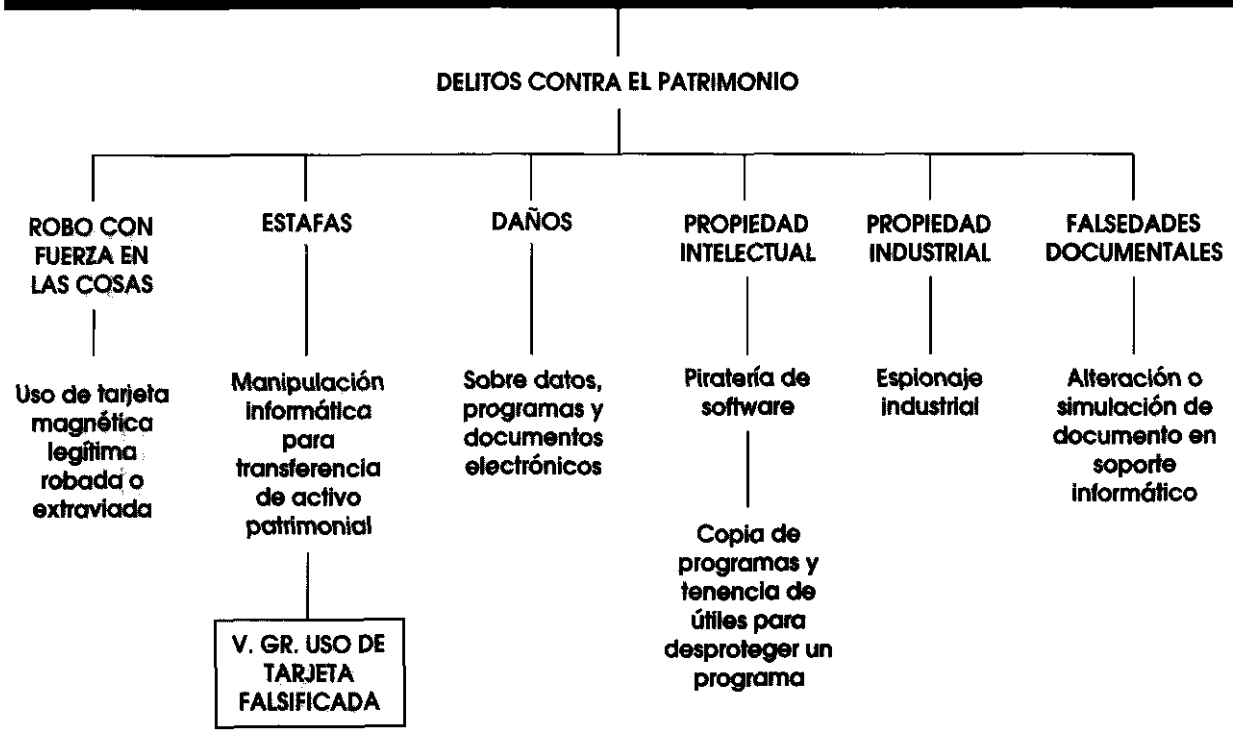
Consumidores» recoge en el artículo 270 la protección penal al titular de derechos de propiedad intelectual sobre programas de ordenador. Las penas previstas en este artículo son de prisión o multa. En el caso de la prisión oscila de seis meses a dos años, y en el caso de la multa de seis a veinticuatro meses. Como en el Código Penal anterior, el nuevo castiga, con las penas transcritas, la copia no autorizada (piratería) de programas de ordenador (software). Esta protección penal deviene de la consideración por la Ley de Propiedad Intelectual, de 11-11-87 (22/87), a los programas de ordenador como objetos de Propiedad Intelectual.

El artículo 270.1 exige para la aplicación del tipo el ánimo de lucro en el autor y el perjuicio de tercero. Sin embargo el párrafo segundo del mismo artículo 270 exige únicamente una acción intencionada (sin hablar de ánimo de lucro ni de perjuicio de tercero) de importación, exportación o almacenaje de las obras objeto de protección en el artículo. Con ello entendemos quedan comprendidas las conductas de los denominados «Hakers» que almacenan estas obras o producciones o ejecuciones sin autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. En estas conductas es indiferente la existencia o no de ánimo de lucro.

Como innovación frente a la regulación anterior ha de destacarse el párrafo final de este artículo 270 que dice:

> *«Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador».*

LOS DELITOS INFORMÁTICOS EN EL NUEVO CÓDIGO PENAL



Este párrafo inserto en sede de protección penal de los derechos de propiedad intelectual sobre programas de ordenador hace pensar que la sanción se establece para aquellas conductas que neutralizando los sistemas lógicos de protección de un programa consiguen la copia del mismo y su posterior reproducción. Sin embargo, la dicción de este párrafo no circunscribe la conducta de neutralización a la finalidad de copia y reproducción, por lo que cabría sostener la penalización de aquellas otras conductas de neutralización de la protección lógica de programas que dejen expedita, o permitan, la entrada en sistemas de información. Estamos considerando una serie de conductas en las que la finalidad del autor no sea copiar el programa cuyas medidas de seguridad lógicas han quedado neutralizadas, sino conseguir el acceso al sistema informático que precisamente el programa neutralizado impedía. La fabricación y puesta en circulación de medios destinados a facilitar la supresión de medidas de protección de programas de ordenador creemos puede tener un ámbito de aplicación mucho más amplio que el que quizá, ante una primera lectura, cabe deducir de este artículo 270 *in fine*.

Si en los hechos concurre, junto a la conducta exigida en el tipo básico (por ejemplo, copia de un programa de ordenador con ánimo de lucro y en perjuicio de tercero), alguna de las circunstancias recogidas en el párrafo segundo y tercero del artículo 270 (almacenaje de diseños de páginas web de Internet, tenencia de un medio para desproteger un programa de ordenador) viene en aplicación el tipo agravado (artículo 271). En estos casos el Juez puede decretar el cierre temporal o definitivo de la industria o establecimiento del condenado.

En cuanto al régimen de la responsabilidad civil derivada de estos delitos se mantiene igual que en la regulación del anterior Código, remitiéndose a las disposiciones en la materia de la Ley de Propiedad Intelectual en relación con el cese de la actividad ilícita y la indemnización de los daños y perjuicios.

Así mismo, el artículo 272.2 prevé, en el supuesto de sentencia condenatoria, que el Juez o Tribunal pueda decretar la publicación de la sentencia, a costa del infractor, en un periódico oficial.

Así mismo, el artículo 272.2 prevé, en el supuesto de sentencia condenatoria, que el Juez o Tribunal pueda decretar la publicación de la sentencia, a costa del infractor, en un periódico oficial. Cabría en este punto apuntar que quizá la publicación de la sentencia en un periódico de tirada nacional, u otros medios de difusión de más generalizado acceso, se avenga mejor con la finalidad de resarcimiento y defensa de los intereses del titular del derecho de autor vulnerado y, así mismo, sea una eficaz medida de publicidad de la efectividad en la aplicación de la norma penal.

- **Espionaje industrial**

La Sección 3.ª **«De los delitos relativos al mercado y a los consumidores»** del mismo Capítulo XI «De los Delitos Relativos a la Propiedad Intelectual e Industrial al Mercado y a los Consumidores» recoge en el artículo 278 una referencia a documentos escritos o electrónicos y soportes informáticos y una remisión a los medios e instrumentos señalados en el apartado 1 del artículo 197, manipulación de las telecomunicaciones..., como medios idóneos para la comisión de un delito de espionaje industrial.

- **Falsedades documentales**

Dentro del Título XVIII **«De las Falsedades»** el Capítulo II **«De las Falsedades Documentales»**, en su Sección 1.ª recoge un artículo, el 390, que castiga la falsificación de documentos debiendo considerarse incluido dentro del con-

cepto de documento aquellos que se encuentren en soporte electrónico dada la claridad con la que el artículo 26, del mismo cuerpo legal, define lo que a los efectos del nuevo Código Penal ha de considerarse por documento:

> *«Artículo 26. A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica».*

No se encuentra precedente de este artículo en el anterior Código Penal, y dada la amplitud de su formulación es indudable que cabe considerar (incluidos en el concepto de documento aquellos que se encuentren en soporte electrónico.

- **Programas informáticos para la falsificación**

Dentro del mismo Título XVIII, el Capítulo III, artículo 400 sanciona la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores (falsificación de moneda y efectos timbrados y falsedades documentales). La dicción del presente artículo es amplia aunque si se tiene en cuenta la restricción del concepto de moneda, artículo 387, las actuaciones delictivas en torno a lo que se denomina dinero electrónico quedarían fuera del ámbito de aplicación de los tipos de falsificación de moneda y por tanto del ámbito del artículo 400.

- **Violación de las telecomunicaciones**

Por último, el Título XXI «Delitos contra la Constitución», del Libro I del nuevo Código Penal, recoge en su Sección 2.ª «De los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad», en el artículo 536 el delito de violación de las telecomunicaciones por parte de una autoridad o funcionario, con infracción de las garantías constitucionales o legales, aunque medie causa por delito.

- **Faltas informáticas**

En cuanto a las faltas cometidas por medio de o contra elementos informáticos, comentaremos las cometidas contra el patrimonio. El nuevo Código Penal define las faltas en el artículo 13.3 como las infracciones que la ley castiga con pena leve. Centrándonos en las faltas contra el patrimonio el artículo 623.4 establece que:

> *«Los que cometan estafa, apropiación indebida, o defraudación de electricidad, gas, agua u otro elemento, energía o fluido, o en equipos terminales de telecomunicación, en cuantía no superior a cincuenta mil pesetas».*

Serán castigados con arresto de dos a seis fines de semana o multas de uno a dos meses.

El fenómeno INTERNET. Fraudes en la Red

Si hasta aquí hemos recogido la regulación penal del delito informático, no podemos desaprovechar la ocasión para recoger un medio sobre el que muchas de las conductas descritas se están o pueden estar desarrollándose, nos referimos a Internet. El primer problema que nos encontramos es que en Internet no existe una regulación en relación a los usos abusivos que pueden desarrollarse en ella.

En un reciente trabajo publicado por la Comisión de las Comunidad Europeas se pone de manifiesto la gran potencialidad y, al mismo tiempo, la gran «miseria» de esta red de redes. Nos referimos al hecho de que Internet está conducida por los propios usuarios, y que son éstos, y no necesariamente en ejercicio de

actividades de editores establecidos, los que crean y suministran buena parte de los contenidos disponibles a través de la Red. Ésta funciona simultáneamente como medio de publicación y de comunicación, en definitiva, la red Internet difiere de los servicios tradicionales de telecomunicación y, precisamente, del adecuado tratamiento jurídico de esta diferencia depende el éxito de una posible futura regulación de Internet.

La Comisión de las Comunidades reconoce expresamente en el documento que venimos comentando la circulación de contenidos ilícitos y por tanto puede que incluso constitutivos de delito en algunos casos, en Internet. Ante esta situación la Comisión propone una serie de medidas para combatir las fuentes de las que proceden los contenidos delictivos. Como medida básica se configura la necesidad de incrementar la cooperación entre los Estados miembros en orden a intercambiar los datos de que se disponga en cada Estado sobre suministradores de contenidos ilícitos en la Red. Dada la falta de uniformidad entre las legislaciones de los Estados miembros en relación con qué se considera contenido ilícito en Internet se aconseja establecer unos criterios europeos mínimos.

Así mismo, la Comisión propone fomentar la autorregulación alentando el desarrollo de Códigos de Conducta en aquellos Estados miembros que todavía no dispongan de ellos. Pero, sin duda, entendemos que la solución ha de venir abordando la regulación de los ilícitos en Internet desde el punto de vista internacional, es decir, con la firma de un convenio internacional sobre contenidos ilícitos y nocivos.

Recogemos a continuación, brevemente, los posibles delitos que pueden desarrollarse sobre la red.

• Delitos en INTERNET. Especial referencia a Fraudes Informáticos. Medidas de seguridad lógica en la Red

La aproximación a los delitos cometidos dentro de una red como Internet, exige una clasificación de estas conductas. Para ello nos inclinamos por un criterio simple como es la distinción entre **ataques activos** al sistema informático tanto a nivel lógico o de software (manipulación de datos y/o de programas) como a nivel físico o de hardware (destrucción y/o manipulación de elementos físicos del sistema); y los denominados **ataques pasivos** donde se accede de forma ilícita a la información que circula por la Red, o bien, a través de ésta a la información almacenada en un sistema.

Dentro de los que hemos denominado *ataques pasivos* las conductas más frecuentes son los *accesos no autorizados*. Según una corriente generalizada, tanto a nivel legislativo como doctrinal en todo el mundo, debe tipificarse como delito la entrada en un sistema informático sin la autorización del propietario. En estas conductas se produce un acceso inconsentido a un sistema sin alterar, inutilizar, destruir o de cualquier modo manipular los datos o los programas de ese sistema. El nuevo Código Penal español tipifica estas conductas en el artículo 197 pero desde la perspectiva de la defensa del bien jurídico intimidad.

Junto al acceso no autorizado a sistemas informáticos a través de la Red cabe otro tipo de ataques pasivos, igualmente tipificados por el nuevo Código Penal, como son la interceptación de mensajes de correo electrónico (e-mail).

Siguiendo con el criterio clasificador adoptado, los *ataques activos* dentro o a través de la Red se concretan en: la destrucción de datos, las estafas electrónicas, las manipulaciones en transferencias de fondos, la infracción de derechos de autor y falsedades en documentos electrónicos.

• Referencia a ataques reales producidos en la Red

Brevemente recogemos a continuación algunos ejemplos de los ataques más frecuentes y públicamente conocidos producidos en Internet.

Puede identificarse como uno de los factores que han propiciado y propician estas situaciones los propios protocolos de comunicación en Internet. Éstos se diseñaron para que fueran simples, careciendo de mecanismos de seguridad, siendo responsabilidad de cada usuario su implantación. Esta situación ha facilitado la proliferación de los denominados *«sniffers»* que acceden o escuchan los paquetes que viajan por la Red. En 1994 el 80 por ciento de los ataques en Internet se clasificaron en esta categoría. Los autores de estos ataques, denominados *«crackers»*, utilizan una serie de programas que les permiten escuchar los paquetes de datos que viajan por la red sin medidas de protección (un mensaje cifrado utilizando un sistema de encriptación asimétrico estaría a salvo de estos ataques). Así, por ejemplo, se averiguan «passwords» de cuentas bancarias para posteriormente acceder a ellas.

Junto a esta forma de violación de la información ha proliferado la suplantación de personalidad de usuario. Se denomina *«hijacking»* y consiste en tomar el control de una conexión ya establecida. El *«hijacker»* suplanta al usuario que realmente ha establecido la conexión dejándole colgado.

Ante las situaciones descritas se hace necesario adoptar medidas de seguridad que abarquen un doble ámbito, el de la seguridad exterior o perimétrica, que impida a los usuarios situados en el exterior de un sistema acceder a su interior si no se cumplen determinadas condiciones, y el de la seguridad interior o interna que impida a los usuarios interiores incumplir las normas establecidas. Cabría, a nuestro juicio, añadir las medidas de seguridad en la comunicación con el exterior. A ello dedicamos a continuación unas líneas en relación con las medidas de seguridad lógica en Internet.

Junto a los ataques activos y pasivos enumerados en los que el objeto de ataque es un bien o derecho relacionado con el tratamiento automático de la información, la red mundial Internet está sirviendo de campo de desarrollo de delitos tradicionalmente cometidos en el mundo real en oposición al mundo virtual al que nos venimos refiriendo. En concreto, hablamos de delitos de espionaje, terrorismo, narcotráfico, delitos contra la libertad sexual...

• Medidas de seguridad lógica en Internet. Trascendencia jurídica

Brevemente nos referiremos ahora a medidas de protección lógica frente a manipulaciones desautorizadas de mensajes que circulan por la red Internet y que pueden constituir una forma de comisión de fraude informático. El mensaje objeto de una manipulación desautorizada bien puede tratarse de una orden de transferencia de fondos o de pago con tarjeta. Entrarían por tanto estas conductas de lleno dentro del objeto de nuestro interés, manipulación intencionada (con ánimo de lucro) producida sobre o por medios informáticos y con repercusiones negativas en la esfera patrimonial de un individuo.

En opinión de los expertos, los requerimientos de seguridad en redes abiertas como Internet se centran en proporcionar servicios de privacidad, integridad, autentificación y disponibilidad de la información. Así mismo, aconsejan que estas medidas de seguridad se sitúen en los extremos o nodos finales de la red. Las manipulaciones de mensajes, alteración de información, dentro de la red Internet (ataques activos) no pueden ser prevenidos, sólo pueden ser detectados. La adopción de estos mecanismos de seguridad responde en determinados casos en exigencias prácticas de evitación de incidentes y si los mensajes que circulan por la red tienen como fin la conclusión de acuerdos contractuales, aunque ciertamente en de-

«En cualquier caso la criptografía se presenta como el principal mecanismo de seguridad en redes abiertas como Internet.»

recho español rige como principio general la libertad de forma, con el fin de evitar los siempre conflictivos problemas de prueba es recomendable adoptar sistemas de encriptación que doten a los mensajes de los atributos de integridad, confidencialidad, autentificación y no repudio.

Conclusiones

Como consideraciónes finales cabe apuntar:

1.° Que el nuevo marco penal, definido por la Ley Orgánica 10/1995, de 23 de noviembre, no es la panacea que resuelve y da respuesta penal a todos los ilícitos relacionados con el uso abusivo y malintencionado de las Tecnologías de la Información y las Comunicaciones.

2.° Los ilícitos informáticos presentan unas características intrínsecas que dificultan sobremanera su persecución. Así, podemos enumerar, entre otras, las siguientes circunstancias que dificultan la represión: rapidez en su comisión, la facilidad para borrar las pruebas (no debe olvidarse que normalmente el delincuente pertenece a la plantilla de la empresa), la facilidad para encubrir el hecho, la dificultad de la prueba sobre soporte magnético.

3.° Además de estos inconvenientes, pertenecientes al orden de los hechos, las cuestiones de derecho que se suscitan tanto en el plano sustantivo como procesal, en aquellas conductas delictivas cometidas a distancia, plantean problemas de derecho internacional de a veces no fácil solución.

4.° En relación con el nuevo escenario comercial, cultural y social, en general, desarrollado con la extensión de la red Internet sólo cabe apuntar la necesidad de una regulación internacional vinculante que proteja nuestra intimidad y patrimonio de ataques provinientes de cualquier punto del planeta. ■