Daniel Sánchez Romero

Letrado colegiado en el Ilustre Colegio de Abogados de Jerez de la Frontera, Cádiz, España.
Socio de la FICP.

~Las nuevas tecnologías y los delitos informáticos tras la reforma de la LO 1/2105~

I. INTRODUCCIÓN

Podemos comprobar que la evolución social encaminada a la utilización de las nuevas tecnologías y sobre todo, asociadas al cada vez mayor uso del internet y acceso al ciberespacio, no sólo comporta un gran paso en la evolución social, sino que también supone un gran instrumento al servicio de mentes delictivas y organizaciones criminales que, apoyándose en su enorme capacidad económica que les permite situarse en la cúspide del conocimiento técnico, arremeten contra la población en general aprovechándose de su escasa formación informática.

Ante esta situación que nos presenta esta nueva realidad derivada de la nueva "cultura tecnológica", nuestro ordenamiento jurídico, adecuándose a esta necesidad y realidad social, se ha visto en la obligación de estudiar estas nuevas situaciones sociales aprovechadas por los delincuentes, y avocando en la incorporación de modificaciones sustanciales y relevantes, bien estableciendo nuevas modalidades o subtipos de figuras específicas ya existentes, bien introduciendo y creando ex novo nuevos tipos penales como figuras específicas y autónomas, hasta entonces inexistentes.

La culminación de este proceso de adaptación la encontramos en la **reforma del Código Penal tras la Ley Orgánica 1/2015 de 30 de Marzo.**

Esta nueva realidad ha desembocado en la categorización de una nueva tipificación de los llamados como "delitos informáticos", que tienen como punto en común las nuevas tecnologías como medio, objeto o bien jurídico protegido. Sin embargo, contamos con la implacable evolución tecnológica, que impide la estanqueidad de esta calificación y promueve un continuo desarrollo y avance en la catalogación de esta nueva modalidad delictiva.

II. LOS NUEVOS DELITOS INFORMÁTICOS: EL PHISING Y EL PHARMING Y SU CALIFICACIÓN JURÍDICA; EL HACKING Y EL CRACKING

1. El phising

El **Tribunal Supremo** desde hace años ha analizado éste delito de estafa informática, así destaca la **sentencia de 2 de diciembre de 2014 (RJ 845, 2014)** relativamente reciente en la que el Alto Tribunal encuadra estas conductas de phishing bancario en el artículo 248.2 a) del Código Penal y explica cómo suele actuar el autor de este tipo de delitos de estafa informática.

La conducta básica que encarna este tipo de delitos consiste en el envío de emails fraudulentos desde direcciones supuestamente de entidades bancarias a la dirección de correo electrónico de la víctima, reclamando datos personales de contenido económico, como regla general datos de acceso a las cuentas (usuario y contraseña) que la víctima o víctimas tengan abiertas en la entidad o mediante enlaces a una web casi idéntica o muy similar a la de la entidad bancaria, produciendo así engaño en los usuarios con la finalidad de obtener un beneficio económico ilícito mediante la realización de transferencias a la cuenta del autor o autores del delito.

Destaca también la **SAP de Vizcaya de 10 de noviembre de 2016 (RJ 429, 2016)**, en la cual dicho órgano jurisdiccional concreta que en el "phishing bancario" es habitual que "el internauta reciba un correo en el que se la informe de que debe verificar sus cuentas, seguido por un enlace que parece la página Web oficial de la entidad bancaria."

Otra Sentencia significativa es de la **Audiencia Provincial de Valencia de 25 de enero de 2017 (RJ 37/2017)** que profundiza en los conceptos de phishing y mulero, trata de configurar la responsabilidad del mulero y además analiza un caso en el que Bankia S.A como proveedora de servicios de pago en línea consigue bloquear las transferencias realizadas por el autor del delito, desplegando así la requerida diligencia y no generándose responsabilidad civil contractual por haber adoptado la entidad bancaria las medidas necesarias tendentes a la evitación del delito.

El phishing en sí consiste según la Audiencia como técnica de ingeniería social caracterizada por intentar obtener información confidencial, consistente en datos personales del usuario, de forma fraudulenta, como pueden ser contraseñas o

información sobre tarjetas de crédito u otra información bancaria a través de una técnica consistente en suplantar páginas web o enviar correos electrónicos aparentemente oficiales haciéndose pasar por empresas o entidades de confianza (normalmente Bancos) y solicitando la aportación de datos relativos al usuario y contraseña de acceso a servicios de pago en línea, pues el principal objetivo del autor o autores de estos delitos son los usuarios de servicios de pago en línea.

El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. A partir de la obtención de estos datos confidenciales, el *phiser* procede a apoderarse de los patrimonios ajenos ordenando transferencias bancarias.[1]

La mayoría de los métodos de phishing utilizan alguna forma técnica de engaño en el diseño para mostrar que un enlace en un correo electrónico parezca una copia de la organización por la cual se hace pasar el impostor. La calidad del anzuelo dependerá de la calidad del *phiser* en todos los casos se podrá medir la entidad del *iter criminis* efectuado, al igual que en las estafas siempre suele concurrir cierta negligencia, mayor o menor por parte de la víctima, y habrá que estar a la circunstancias subjetivas que concurran en ella.

Uno de los aspectos más importantes es el blanqueo de dinero. Actualmente empresas ficticias intentan reclutar teletrabajadores por medio de e-mails, chats, irc y otros medios, ofreciéndoles no sólo trabajar desde casa sino también otros jugosos beneficios. Aquellas personas que aceptan la oferta se convierten automáticamente en víctimas que incurren en un grave delito sin saberlo: el denominado “lavado de dinero” obtenido a través del acto fraudulento de phishing. Los intermediarios realizan el traspaso a las cuentas de los estafadores, llevándose éstos las cantidades de dinero y aquéllos, los intermediarios, el porcentaje de la comisión.

2. El pharming

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (*domain name*) a otro ordenador diferente. De esta forma, un usuario que introduzca un determinado nombre de dominio

[1] SJPI Murcia, 69/2007, de 30 de marzo, (RJ 2008/ 44072).

que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

La palabra *pharming* deriva del término "farm" (granja) y está relacionada con el término "phishing", utilizado para nombrar la técnica de ingeniería social que, mediante suplantación de correos electrónicos o páginas web, intenta obtener información confidencial de los usuarios, desde números de tarjetas de crédito hasta contraseñas. La etimología de esta palabra se halla en que una vez que el atacante ha conseguido acceso a un servidor DNS y tomado control de éste, es como si poseyera una "granja" donde puede hacer uso a placer de los recursos que allí se encuentran.

La técnica de *pharming* se utiliza normalmente para realizar ataques de phishing, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

3. Calificación jurídica

a) Tipo objetivo

Como ya sabemos, el *phiser* o *farmer* es la persona que acude a una página web (de una entidad bancaria o de un particular) y se apodera de las claves de acceso a la banca electrónica realizando transferencias no consentidas de dinero a costa de las cuentas corrientes de las víctimas.

Sin embargo, llegamos a un punto controvertido doctrinalmente y es en relación a la concurrencia o no del elemento "engaño". En la **STS de 19 de Abril de 1991**, El tribunal consideró que no hubo estafa, sino apropiación indebida ya que no hubo engaño en las víctimas que les llevara a producirles el error necesario que les indujera a realizar esa disposición patrimonial a favor del autor del delito. La solución dada por esta sentencia, considerada doctrinalmente muy forzada, sostenía en su **FJ 2º**:

> "*La «inducción» a un acto de disposición patrimonial sólo es realizable frente a una persona y no frente a una máquina, implica una dinámica comisiva con acusado substrato ideológico. Con razón se ha destacado que a las máquinas no se las puede engañar, a los ordenadores tampoco, por lo que los casos en los que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce ni el engaño ni el error necesarios para el delito de estafa. Sin engaño, elemento cardinal de la estafa, no puede entenderse producida ésta*".

Por tanto, una de las características principales de la estafa informática es que estructuralmente no es exigible el engaño, pues como argumenta la **STS de 20 de noviembre de 2001**, dado que estamos en una estafa cometida a través de una transferencia no consentida por el perjudicado mediante manipulación informática, no es precisa la concurrencia de engaño alguno por el estafador. Y ello es así porque la asechanza a patrimonios ajenos realizados mediante manipulaciones informáticas actúa con automatismo en perjuicio de tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal.

La Instrucción nº 4/ 2007 del Fiscal Jefe de Madrid distingue los siguientes supuestos:

1) Falseamiento de la página web para la obtención de claves y contraseñas de acceso y utilización de las así obtenidas para detraer dinero de las cuentas corrientes mediante transferencia bancaria.

La instrucción insta a los Fiscales a perseguir este tipo de conductas como un delito de estafa informática del art. 248. 2 del CP y un delito contra la intimidad del art. 197.2 del Código Penal. Sin embargo dado que lo que ocurre un supuesto de concurso de normas (art. 8.1 del CP) se exhorta a calificar exclusivamente como una estafa informática (del art. 248.2 del CP).

2) Falseamiento de la página web para la obtención de página de claves y contraseñas de acceso y sin, realizar transferencias, posteriormente se efectúa la venta o transmisión de dichas claves y contraseñas.

En este caso la Fiscalía entiende que nos encontramos ante un delito de revelación de secretos del art. 197. 2 y 3 del CP.

3) Falseamiento de una página web para la obtención de claves y contraseñas de acceso y utilización de sólo parte de las así obtenidas para detraer dinero de las cuentas corrientes mediante transferencia, conservando el resto o transmitiéndolas a un tercero: se calificará como un delito de estafa informática del art. 248.2 del CP y otro de revelación de secretos del art. 197.2 y 3 del CP en concurso real.

En cuanto a la conducta del "mulero" (persona que abre o "presta" su cuenta corriente para que el phiser haga el ingreso del dinero de las víctimas, normalmente mediante un reparto del botín, bien por una cantidad a tanto alzado o mediante una cuota o porcentaje.

No es impune y se calificará, en función de los casos, o como un delito de estafa informática del art. 248.2 del CP (**STS 533/ 200727, de 12 de junio**) o, como un delito de blanqueo de capitales del art. 301 del CP, atendiendo a las circunstancias concurrentes, singularmente al origen del dinero.

b) Tipo subjetivo

Los principales elementos que lo constituyen son:

- El ánimo de lucro: se refiere a que el sujeto actúe con el deseo o la intención de enriquecerse, de aumentar su patrimonio, en su caso, de eludir una deuda.
- La acción típica es la de valerse de una manipulación informática o artificio semejante. Tras la reforma de la LO 15/ 2003, de 25 de noviembre, desaparece los conceptos de "engaño bastante y error", siendo sustituidos por los de "manipulación". Se corresponde con la conducta de alterar, modificar u ocultar datos informáticos de manera que se realicen operaciones de forma incorrecta o que no se lleven a cabo, y también con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener. De esta forma un sujeto puede introducir instrucciones incorrectas en un programa de contabilidad de manera que no anote cargos a su cuenta corriente por ejemplo, o que desplace a su cuenta bancaria todos los ingresos efectuados un determinado día a las cuentas cuyos números terminen en determinado.

La referencia a «alguna manipulación informática o artificio semejante» parece capaz de acoger todos los casos posibles mediante los que se efectúa una transferencia no consentida de activos patrimoniales en perjuicio de tercero, ya consistan en modificaciones de programas o alteraciones en el procesamiento, ya en manipulaciones en la entrada, salida o transmisión de datos. Como se ha observado, la fórmula legal es muy amplia, aunque tal vez inevitable en este campo, en el que el desarrollo tecnológico es continuo, con el peligro de que una prosa más estricta dejara pronto obsoleto el precepto[2].

La referencia a «artificio semejante» podría hacer pensar que se incluyen también otras maniobras de naturaleza no informática. Sin embargo, el sentido del apartado

[2] QUINTERO OLIVARES, Comentarios a la Parte Especial del Derecho penal, Aranzadi, Pamplona, 1996, p. 491.

obliga a entender que todo él va referido a estos supuestos, por lo que la mención legal debe ser interpretada también desde esa perspectiva.

- La transferencia no consentida del patrimonio de otra persona sin utilizar violencia. Lo que se suele traducir en un desplazamiento del dinero de la cuenta bancaria de la víctima a la cuenta del autor del delito.
- Perjuicio a tercero, ya que no es la propia víctima la que realiza la transferencia económica, sino que es el propio autor del delito el que la lleva a cabo.

En cuanto al elemento subjetivo del injusto, en este delito no cabe la comisión culposa, el sujeto activo actúa dolosamente, es decir, actúa conociendo y queriendo realizar la acción delictiva. El concepto de "manipulación informática" implica por sí mismo la intencionalidad del sujeto activo; es difícil que alguien lleve a cabo actos de alteración, modificación de datos o programas informáticos por error y que además le reportan un beneficio económico, ya que estas acciones requieren conocer los datos o instrucciones correctas y cambiarlos por otros, el sujeto sabe que su actuación constituye una acción contraria a derecho y aún así la lleva a cabo.

4. El hacking

El *hacking* o intrusismo informático, consistente en el acceso no autorizado, por lo general violando los mecanismos de seguridad allí donde los haya, a los archivos y bases de datos contenidos en los sistemas informáticos ajenos, normalmente de grandes empresas o instituciones[3].

Los comportamientos de *hacking*, aunque en sí no tienen por qué ser perniciosos, pues, una vez soslayadas las barreras de protección informática el *hacker* suele salir del sistema sin ulteriores propósitos, no deja de ser cierto que, en no pocas ocasiones, son la antesala de violaciones muy graves contra la intimidad, contra los derechos de propiedad intelectual o industrial o contra los secretos de empresa.

La tipificación penal, allí donde el *hacker* se limita, sin más, a entrometerse es muy confusa, porque si la conducta se mantiene en el estricto ámbito de la intromisión informática, hay que considerarla, desde el punto de vista de su relevancia penal, como impune o atípica. Es más, ni siquiera llega a alcanzar la consideración de una tentativa o de un acto preparatorio (allí donde éste fuera punible), porque no concurre el elemento

[3] Sobre el estudio de las figuras afines al hacking: MORÓN LERMA, Esther, en: Internet y Derecho penal: Hacking y otras conductas ilícitas en la red; Aranzadi, 2002; Capítulo II.

subjetivo, ya que la finalidad del *hacker* no es atentar contra la intimidad o contra la propiedad intelectual como tampoco es dañar los sistemas o los programas informáticos en los que se entromete.

En este sentido, se pronuncia el **Auto de 29 de enero de 2002 del Juzgado de Instrucción nº 2 de Lorca** que destipifica las conductas atendiendo a que no concurre el elemento subjetivo del injusto y declarando en su FJ 2º:

"Las conductas de mero hacking acceso a los a los sistemas informáticos perpetrados con al única finalidad de acceder al password o puerta lógica no son actualmente constitutivos de delito pues carecen del elemento subjetivo del injusto".

Desde el punto de vista político-criminal, esta ausencia de relevancia penal es severamente criticada, por algunos sectores, que no dudan en considerar que el *hacking* debería de contar con un tipo penal específico.

Las manipulaciones más usuales se producen normalmente mediante la introducción de datos falsos, la alteración de los programas o la utilización de bombas lógicas, caballos de Troya, ya analizados, o técnicas como la del salami[4], que provocan la realización automática de transferencias bancarias, ingresos o reconocimiento de créditos en favor de quien realiza la alteración. El medio empleado y la actuación con y sobre máquinas y no sobre personas, junto con el hecho de que la conducta utilice e incida en elementos incorporales, son los caracteres definidores de estos supuestos y los que les dan identidad propia desde el punto de vista penal.

Sin embargo, la preocupación por su desarrollo explica que haya sido objeto de tipificación expresa en algunos ordenamientos[5]. No ocurre así en el Código penal español, que no contiene ninguna previsión que castigue de manera genérica el acceso no autorizado a sistemas informáticos ajenos.

[4] Se denomina así a la introducción de instrucciones para transferir a cuentas propias la acumulación resultante de los céntimos que se desprecian al operar con cuentas corrientes, cálculo de intereses, saldos, operaciones financieras, etc., y que alcanzan montos importantes (vid., CAMACHO LOSA, Luis, Internet y Derecho penal: Hacking y otras conductas ilícitas en la red; Aranzadi, 2002, pp. 41-42 y SNEYERS, Alfredo, El fraude y otros delitos informáticos, Tecnologías de Gerencia y Producción, S.A., Madrid, 1990, p. 112).

[5] MÖHRENSCHLAGER, Manfred, Tendencias de política jurídica en la lucha contra la delincuencia informática, Delincuencia informática, (coord. Mir Puig, Santiago), Ed. PPU, Barcelona, 1992., pp. 60-61.

Como consecuencia, la punición de estos comportamientos sólo será posible en la medida en que vayan referidos a datos que sean objeto de protección particular o impliquen conductas que resulten incluibles en tipos penales genéricos.

Si la finalidad es descubrir las intimidades de un particular concreto parece que serían perfectamente incardinables en el art. 197 del CP. El problema surge cuando no hay una relación aleatoria entre víctima y hacker la incardinación resulta cuando menos conflictiva, debido a la función selectiva y restrictiva del elemento subjetivo del injusto.

Autores como MORALES PRATS[6] sin embargo entienden que la mayoría de las conductas de abusos cibernéticos o contra la libertad informática o *privacy* deben quedar subsumidas en el art. 197.2 del CP (que carece del elemento subjetivo del injusto del párrafo 1º).

Cuando el elemento volitivo va encaminado a descubrir los «secretos de empresa» tal conducta estaría protegida en el art. 278.1, que constituye la referencia básica de estos comportamientos: «El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197»[7].

El precepto se refiere expresamente a «datos, documentos... electrónicos, soportes informáticos...», y por la remisión al 197 a «mensajes de correo electrónico... telecomunicaciones... o... cualquier otra señal de comunicación», lo que lo sitúa de lleno dentro de los supuestos que tratamos en la medida en que el "apoderamiento" de los mismos supone de suyo un acceso no autorizado al sistema o al ordenador en el que los mismos se encuentran.

Para la jurisprudencia no parece ser un elemento decisorio la relevancia del dato aprehendido, así la **STS de 11 de junio de 2004** condena a un funcionario del INEM que meramente se apodera de referencias relacionadas con el lugar de trabajo y domicilio de la empresa respecto a una base de datos perteneciente de la Tesorería General de la Seguridad Social.

No nos parece posible, pues sería demasiado forzado, incardinar la conducta en el art 256 del CP tal como hace algún sector de la doctrina, alegando que valerse

[6] MORALES PRATS, Fermín, en: Comentarios al Nuevo Código Penal, Aranzadi, 4ª Ed., Pamplona, 2005, p. 1063.

[7] GONZÁLEZ RUS, Juan José, Curso de derecho penal, Vol. I, pp. 796 y ss.

subrepticiamente de un aparato ya conectado pues la dicción del tipo parece estar orientada al denominado hurto de uso de tiempo del ordenador o utilización sin autorización o extralimitándose de ella. A su vez, como apuntan VALLE MUÑIZ/ QUINTERO OLIVARES [8] , el Proyecto del Código penal exigía una utilización "subrepticia", elemento típico que fue despreciado ya en el trámite de ponencia.

Ante la insuficiencia legal y el vacío jurídico, no faltan autores[9] que propugnan un adelantamiento de la barrera punitiva (creando delitos obstáculos o barreras al igual que acaeció en Francia) **e**n base a que los ilícitos que se cometen con frecuencia en la denominada zona oscura del ciberespacio suelen ser la antesala de otros ilícitos mayores, dado que el hacker raramente se contenta con allanar el espacio digital del ciudadano afectado y tiende a hacer manifestar su poder intromisivo cometiendo otras nuevas transgresiones.

5. Cracking

También conocido como sabotaje informático. No debemos confundirlo con el *password cracking* o rompimiento o desciframiento de claves (*passwords*) que se asimila al *hacking*.

En el primer sentido, MARCHENA[10] los define como conducta consistente en la destrucción o en la producción generalizada de daños en su sistema, datos, programas informáticos o telemáticos.

Mas, como destacan MATA Y MARTÍN [11] , lo principal de este tipo de comportamientos es que van dirigidos a atacar los elementos lógicos del sistema, es decir, al software en general y a los ficheros o archivos informáticos en los que se recogen datos, información o documentos electrónicos, cualquiera que sea su contenido concreto. Como reseña la doctrina[12], el *modus operandi* concreto (borrado, formateado, virus) es indiferente.

---

[8] VALLE MUÑIZ, José Manuel/QUINTERO OLIVARES, Gonzalo, en: Comentarios al Nuevo Código Penal, Aranzadi, 4ª Ed., Pamplona, 2005, p. 1307.

[9] MORON LERMA, Esther, en: Internet y Derecho penal: Hacking y otras conductas ilícitas en la red; 2002, p. 75.

[10] MARCHENA GÓMEZ, Manuel, El sabotaje informático: entre los delitos de daños y los desórdenes públicos, Actualidad Jurídica Aranzadi, Núm. 40, julio de 2001, p. 7.

[11] MATA Y MARTÍN, Ricardo, Delincuencia informática y Derecho penal, Edisofer, Madrid, 2001, p. 59.

[12] PIÑOL RODRÍGUEZ, José Ramón, Manual de Derecho Penal. Parte. Especial, 4ª Ed, Thomson Civitas, 2006, p. 293.

Dentro de las más graves conductas, resulta destacable, la conducta del *cyberpunker* o *cyberpunking*, que puede ser traducida al castellano como vandalismo electrónico o sabotaje informático, mediante la cual el sujeto activo se dedica a borrar, suprimir o modificar, sin el consentimiento del titular, funciones o datos de un ordenador, con la intención de obstaculizar su funcionamiento normal.

Las formas a través de las que esta conducta se lleva a cabo son, desde el punto de vista de la lógica del funcionamiento de los sistemas y mecanismos informáticos, muy variadas y normalmente, desde el punto de vista terminológico, todas ellas se unifican por referencia a la infección de los sistemas por virus informáticos.

Últimamente cobra cierta peculiaridad el *smurfing* consistente en donde lo que asalta es el encaminador de redes o *router*, sobrecargando el servicio a través de continuos ataques masivos utilizando sistemas esclavos o atacar el sistema con gran cantidad de paquetes con direcciones de IP falsas (*flooding*), bloqueando el sistema y provocando la denegación global del servicio (*DdoS* o *denial of service*).

En ciertas ocasiones la conocida como publicidad vírica o marketing viral (*pop ups*) puede ser incardinable en este tipo, cuando como consecuencia de estas prácticas al menos a titulo de dolo eventual se prevea que va dar lugar a una instalación inconsentida que implique un perjuicio para los sistemas operativos del ordenador afectado.

Como vimos, el *cracking* es pues un concepto informático no material[13], porque los datos incorporados a los soportes físicos dirigidos al hardware o cualquier soporte informático cuyos desperfectos deben ser cobijados en el tipo genérico de daños (art. 263 para el delito y el 625 para la falta).

Para la persecución penal del sabotaje informático se ha creado un tipo específico en el art. 264.2 del Código Penal que cobijaría los daños a los datos previstos en el art. 4 del Convenio de cibercriminalidad. Aunque a juicio de cierto sector de la doctrina44 tal tipificación no era imprescindible pues aparecían ya protegidos en el delito genérico de daños.

[13] GONZÁLEZ RUS, Juan José, Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos, Revista de la Facultad de Derecho de la Universidad Complutense, 12, 1986, pp. 138-142.

Como refiere CREMADES GARCÍA[14] en la exégesis de este art. 264.2 es necesario tener en cuenta para calificar la acción como delito, la utilidad de esos datos y el reflejo de ese menoscabo en la actividad de su titular, además del valor en sí de esos propios datos.

Aunque es preciso recordar que cuando la dimensión del hecho dañoso suponga la destrucción u obstaculización de las instalaciones de telecomunicación cabe aplicarse el art. 560.1 del Código Penal.

Como ha destacado MARCHENA GÓMEZ [15], la destrucción generalizada de programas de gestión de correo electrónico tiene que ser vista como un acto contra el patrimonio del afectado.

El bien jurídico sin embargo es mucho amplio que el patrimonio pues lo dañado no son sólo los datos contenidos en la red sino también la seguridad jurídica en el ciberespacio.

Se trata, bajo mi punto de vista, de un delito pluriofensivo. Los métodos más conocidos para producir la destrucción de los elementos lógicos son los virus, caballos de Troya, sniffers, bombas lógicas y gusanos (*worms*).

6. Competencia territorial

La Red posee una naturaleza muy mutable, transfronteriza y dinámica, a la par que tecnológicamente es una entidad muy compleja. Comporta un cierto lado oscuro que provoca la sensación de "invisibilidad" de las contravenciones cometidas en su seno.

Como bien sostiene HERRERA MORENO[16], esta última característica encuentra su razón de ser en la "relatividad del espacio y tiempo informático", a través de la cual "en un juguetón parpadeo cibernético, el delincuente se inviste con los más absolutos atributos de intemporalidad y ubicuidad".

Este carácter "anónimo" provoca en la víctima la sensación de indefensión, rayana con el desamparo. Contemplando las innumerables autopistas de información que circulan por la red, piensa que la Justicia penal nunca podrá dar con el responsable del

[14] CREMADES GARCÍA, Javier, El fraude de los servicios financieros on line, Estudios Jurídicos del Ministerio Fiscal II, Madrid, 2003, pp. 271-272.

[15] Vid. MARCHENA GÓMEZ, Manuel, Actualidad Jurídica Aranzadi, 40, 2001, p. 9.

[16] HERRERA MORENO, Myriam, El fraude informático en el derecho penal español, Actualidad Penal, 39, La Ley, 2001, pp. 925-964.

ataque en su contra, la víctima siente que se enfrenta a un ser "invisible" frente a cuyos ataques sólo queda resignarse, por lo que pocas veces denuncian los hechos que se dan en su perjuicio. Cuando los ataques delictivo- informáticos son dirigidos contra empresas o corporaciones, la "cifra oculta" de criminalidad encuentra su razón de ser en la "publicidad negativa" que ello significa para las propias empresas atacadas.

Frente a las dificultades que se plantean en la persecución de delitos cometidos a través de la red, fundamentalmente las derivadas del principio de territorialidad, propugna la aplicación de la teoría de la ubicuidad, pudiendo hacerse valer conforme a ella tanto la jurisdicción del lugar de la acción como la del lugar del resultado (esto sin que se tengan en cuenta los "lugares de tránsito" a través de la ruta telemática, que serían irrelevantes). En favor de esta ubicuidad señala decisiones jurisprudenciales como el conocido **Auto del TS de 12 de marzo de 1996.**

Mas esta aparentemente sencilla solución encubre numerosas problemas y dificultades. Con la experiencia existente hasta la fecha, podemos afirmar que la vigencia de principios procesales referidos a la aplicación de la ley penal en el espacio, y el clásico celo que la mayoría de los países tienen antes de autorizar que un tercer país juzgue a un ciudadano propio, está complicando sobremanera la persecución del delito cometido utilizando como medio internet.

Lege ferenda, parece postulable una jurisdicción especializada en este tipo de delitos pues los juzgados de instrucción locales, contemplados aisladamente, carecen de experiencia, pericia y mecanismos logísticos adecuados para enfrentarse a la compleja dinámica delictiva que dimana de la red.

Así, las dificultades se concretan por ejemplo cuando la actividad delictiva tiene su origen en el extranjero y el resultado se produce sin embargo en España; esto es, los que comúnmente se conocen como "delitos a distancia".

La pretensión de las autoridades judiciales españolas de entender cometidos en nuestro país este tipo de delitos y reclamar su correspondiente enjuiciamiento colisiona con la frecuente aplicación de la *teoría de la ubicuidad* por parte de terceros países[17], al ser ésta la más favorable para colmar el afán expansivo de su jurisdicción.

[17] COBO DEL ROSAL, Manuel/VIVES ANTÓN, Tomás S., Derecho penal. Parte general, Tirant lo Blanch, Valencia, 1999, pp. 209 y ss.

Además, en muchas ocasiones, las más importantes conductas delictivas se realizan desde países con legislaciones porosas o flexibles respecto a determinadas infracciones penales, que poseen medios muy limitados, o que no han ratificado ningún tratado de extradición.

III. DELITOS INFORMÁTICOS TRAS LA REFORMA DEL CÓDIGO PENAL DE 2015

A lo largo de todo el Código Penal, especialmente tras la reforma de 2015, aparecen muestras de delitos informáticos, al hacer referencia al medio utilizado para la comisión. Así, por ejemplo, otros delitos de este tipo son:

- El acceso no autorizado a sistemas informáticos, artículo 197 bis
- Los delitos informáticos relativos a la propiedad intelectual e industrial a través de la nueva redacción del artículo 270.
- La producción, venta, distribución, exhibición, o su facilitamiento, e incluso su posesión, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces (art. 189).
- La inducción a la prostitución de menores por cualquier medio (art. 187).
- Las amenazas (arts. 169 y siguientes), así como las calumnias e injurias (sets. 205 y siguientes) efectuadas y difundidas a través de cualquier medio de comunicación.
- Los fraudes informáticos para cuya consecución se manipulen datos o programas (art. 248).
- El sabotaje informático, es decir, la alteración o destrucción de datos, documentos, software que se encuentran almacenados en sistemas o redes informáticas (art. 263).
- La posesión de software informático destinado a cometer delitos de falsedad, por ejemplo, falsificar contratos, el DNI, etcétera.
- Delito de descubrimiento y revelación de secretos a través del acceso y difusión sin consentimiento de sus respectivos titulares de datos registrados en ficheros o soportes informáticos (arts. 197 a 201)

Todos estos delitos tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

IV. CONCLUSIONES

Internet se ha convertido en el motor evolutivo tanto de la economía como de la sociedad y su continuo desarrollo resulta vertiginoso para un futuro no muy lejano, por lo que se ha llegado a configurar como un bien jurídico fundamental para el progreso de la sociedad. Un ciberespacio donde no se pueda circular sin seguridad jurídica merma considerablemente las potencialidades de éste y el desenvolvimiento y desarrollo social.

La ausencia de tipificación concreta de determinadas conductas cibernéticas ha llevado a determinados autores, apoyados en el principio de legalidad *strictu sensu*, a negar la represión penal de numerosas conductas.

En primer lugar, el mantenimiento de los modelos tradicionales de protección ante el nuevo entorno digital es evidente, pues ninguno de ellos comparte las características conjuntas con la consiguiente dificultad en su tipificación.

Es evidente que, al examinar las diversas posibilidades del Código Penal español en este punto, se concluye que las conductas de intrusismo informático no encuentran siempre encaje en los diferentes tipos.

Se denota una insuficiencia de normas y mecanismos administrativos de policía que sancionen y reprendan tanto a los autores de actos de hacking como a los operadores de redes y proveedores de acceso prestadores de servicios que faciliten enlaces que por omisión o negligencia favorecen este tipo de actividades ilícitas.

Sin embargo, sería deseable un derecho penal punitivo que actuase contra aquellas conductas que atenten a la seguridad jurídica que debe regir en el ciberespacio. En otras palabras el planteamiento jurídico represivo debe seguir protagonizado fundamentalmente por la Administración, en virtud de los principios fragmentario y de intervención mínima.

Debemos poner también, especial relieve en el factor prevención. Así la propia tecnología tiende a reaccionar frente a los riesgos que inconscientemente genera: los programas antivirus, anuladores de cookies, los detectores de *webs bugs*, los repetidores de correo (*anonymus remailers*), anonimizadores de navegación, los servidores *proxy*,

las aplicaciones criptográficas y los agentes de software o protocolos de seguridad son ejemplos de esta lucha a favor de la salvaguardia de la intimidad informática, configurándose como la vía más oportuna teniendo un carácter preferente sobre la amenaza penal.

Sin embargo, este tipo de autotutela o de autoprotección del usuario cuentan con la grave desventaja de dejar indefensas a amplias capas de la población que no poseen recursos económicos o técnicos para garantizar su propia protección.

En tercer lugar dado que el ciberespacio se proyecta sobre las fronteras nacionales se hace necesaria una regulación internacional sobre esta materia. La manipulación informática realizada a distancia de los datos suscita el problema de cuál es la ley aplicable cuando no coincide el lugar de la manipulación con el lugar donde se produce el resultado fraudulento.

Finalmente, tampoco parece desdeñable, a título de *lege ferenda*, instar la creación de una jurisdicción especializada en materia de cibercriminalidad. La complicación y enorme dificultad que comporta instruir este tipo de causas hacen necesario descargar a los tribunales locales de su persecución y encomendársela a esta nueva jurisdicción, que proporcione un cierto grado de seguridad jurídica.