EGUZKILORE
Número 21.
San Sebastián
Diciembre 2007
7 - 32

PROBLEMÁTICA DE LA PERSECUCIÓN PENAL DE LOS DENOMINADOS DELITOS INFORMÁTICOS: PARTICULAR REFERENCIA A LA PARTICIPACIÓN CRIMINAL Y AL ÁMBITO ESPACIO TEMPORAL DE COMISIÓN DE LOS HECHOS

Mirentxu CORCOY BIDASOLO

Catedrática de Derecho Penal
Universidad de Barcelona

Resumen: La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, resultando difícil determinar la autoría y el lugar de comisión del delito y, en consecuencia, la competencia para juzgar unos determinados hechos. De otra parte, el particular funcionamiento de los sistemas informáticos y los problemas de definición de la titularidad condicionan la atribución de responsabilidad en los delitos cometidos a través de sistemas informáticos o contra éstos. Así, el problema esencial consiste en determinar la responsabilidad jurídico-penal de los intervinientes, y esclarecer cuál es la responsabilidad de los intermediarios de servicios.

Laburpena: Informatikak berezitasun batzu baditu, eta honek delito mota asko burutzeko egoki bihurtzen du, zaila izanik nor izan den jakitea eta delitua non egin den jakitea ere, eta zaila de epaitzeko konpetentzia nork duen azaltzea. Informatika sistemen funtzionamendu bereziak eta titulartasun arazoak, sistema hauen bidez edo hauen kontra burututako delituen erantzukizunaren eskurantza baldintzatzen dute. Parte hartu dutenen erantzukizun juridiko-penala zehaztean dago gakoa. Kontutan hartu behar da, baita ere, nori egotzi diezaiokegun debekatutako ekintza, eta nortzu diran ekintza hauek erraztu dituztenak eta zerbitzu hauen bitartekarien erantzukizuna zein den ere.

Résumé: L'informatique regroupe des caractéristiques qui font d'elle un moyen approprié pour la commission des délits très différents, dont la détermination de l'auteur et du lieu de commission de l'infraction -et, par conséquent, la compétence pour juger certains crimes- se révèle difficile. D'autre part, le fonctionnement singulier des systèmes informatiques et les problèmes de définition de la titularité conditionnent l'attribution de responsabilité des infractions commises à travers les systèmes informatiques ou contre ceux-ci. Ainsi, le

(Nota): Contribución a las Jornadas "Retos en la securización de los territorios digitales: Delitos informáticos", Leioa, 26-27 abril 2007 (subvencionadas por el Dpto. de Industria, Comercio y Turismo del Gobierno Vasco –"Cluster de Privacidad y Seguridad Digital", del Proyecto Etortek "AmiGUNE"–).

problème essentiel repose sur la détermination de la responsabilité pénale des auteurs, et préciser la responsabilité des intermédiaires de services.

Summary: Due to the characteristics of the computer services this way of communication constitutes a perfect way to commit very different offences, being very difficult to determine the responsible and the place where the crime was committed and, therefore, the competent jurisdictions. On the other hand, the special working environment of computer systems and the problems of titularity definition have also a big influence in order to the attribution of responsibility for the crimes committed through computer systems or against them. Thus, the essential problem lies in determining the penal responsibility of participants, and clarifying the responsibility of the services intermediaries.

Palabras clave: Criminología, Derecho penal, Responsabilidad penal, Delitos informáticos.

Gako hitzak: Kriminologia, Zigor Zuzenbidea, erantzukizun penala, informatika delituak.

Mots clef: Criminologie, Droit Pénal, Responsabilité pénale, Délits informatiques.

Key words: Criminology, Penal Law, Penal responsibility, Computer offences.

1. INTRODUCCIÓN

1.1. La informática constituye un instrumento indispensable en todos los ámbitos de actividad. Tanto la organización y administración de empresas y administraciones públicas, como la investigación científica, la producción industrial o el estudio y la investigación, e incluso el ocio, necesitan de la informática. Sin embargo, junto a las incuestionables ventajas que representa, su utilización también presenta aspectos negativos, una faceta negativa de la informática es la "criminalidad informática"[1]. Este concepto abarca la informática como objeto del ataque y como medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial, contra la intimidad, propiedad intelectual, pornografía, defraudaciones –estafas, alzamientos de bienes, apropiaciones indebidas, delito fiscal…– y daños –sabotaje informático–. La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, de la facilidad de acceso a ellos, de su, relativamente, fácil manipulación… Con el auge de Internet a todo ello hay que sumar el fácil acceso desde todos los puntos del planeta. La importancia que Internet ha tenido en esa faceta negativa a la que me he referido ha propiciado que surja una subespecie de criminalidad, la llamada *Cibercriminalidad*[2].

1.2. La informática está intrínsecamente unida a la idea de globalización y su utilización, en concreto, a través de Internet[3], dificulta extraordinariamente determinar el lugar de comisión del delito y, en consecuencia, la competencia para juzgar unos

---

1. El término "criminalidad" parece más adecuado que el de "piratería", utilizado, por ejemplo, por SEMINARA, "La pirateria su Internet ed il diritto penale", en *Annali Italiani del Diritto d'autore della cultura e dello spettacolo,* 1996, p. 183 ss., aun cuando en su trabajo este título está justificado al analizar, especialmente, las infracciones de derechos de autor a través de Internet.

2. Esta terminología es utilizada tanto la doctrina, FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet*, Ed. Constitutio Criminales Carolina (CCC), 2007; como por el legislador, p.ej. *La Convención sobre Cibercriminalidad,* del Consejo de Europa, de 23 de noviembre de 2001.

3. Los problemas que podían derivarse de la utilización Internet ya fueron anunciadas, calificando el sistema de transmisión de datos en Internet como "autopistas de la información" -Information Highway-, en este sentido GRIESE/SIEBER, "Internet als erste Ausbaustufe des Information Highway", en Hilty, *Information Highway, Beiträge zu rechtlichen und tatsächlichen Fragen*, 1966.

determinados hechos, así como la autoría[4]. Todo ello conlleva dificultades de incriminación de estas conductas lo que, atendiendo a los graves perjuicios que puede provocar, ha llevado a que, en la mayoría de países, se cree una legislación específica sobre delincuencia informática. En aras a minimizar los problemas procesales se han aprobado diversos Convenios internacionales para facilitar la investigación, persecución y castigo de los delitos cometidos utilizando la informática. En la Comunidad Europea, la *Convención Europea sobre Cibercriminalidad*, del Consejo de Europa, de 23 de noviembre de 2001, establece directrices dirigidas a los Estados miembros, tanto en el ámbito del Derecho penal material como procesal[5].

1.3. Al respecto, en el Código Penal de 1995 no se creó un Título específico referente a la criminalidad informática, o una legislación especial, como se había hecho en otros países, sino que se optó por una vía intermedia. Frente al modelo legislativo anterior, en el que no se contemplaba la informática ni como medio de comisión de delitos ni como objeto de protección, en el Código de 1995 se toma en consideración, de forma específica, la informática en relación con diversas modalidades delictivas. Referencias a la delincuencia informática como medio de comisión de delitos encontramos en los delitos contra la intimidad, de descubrimiento y revelación de secretos, en los delitos contra la indemnidad y libertad sexual, de corrupción de menores, en los delitos contra la propiedad, como la estafa, o en los delitos contra el mercado y los consumidores, el acceso a servicios de radio, televisión o servicios interactivos prestados por vía electrónica. Así mismo, la informática –*Hardware* y *Software*–, como objeto de protección se toma en consideración en los delitos contra la propiedad intelectual, protegiendo, en particular, los programas y en los delitos de daños –daños o "sabotaje" informático–. A ello hay que sumar otras conductas delictivas, realizadas a través de Internet, que pueden castigarse sin necesidad de crear tipos específicos, así, por ejemplo, delitos contra la libertad, como amenazas y coacciones, delitos contra el honor, falsedades, defraudación de telecomunicaciones, revelación de secretos de empresa –espionaje industrial–, delitos contra la propiedad industrial, publicidad engañosa, blanqueo de capitales…

2. DELITO INFORMÁTICO Y CIBERCRIMINALIDAD

2.1. En este contexto creo conveniente diferenciar entre lo que, tradicionalmente, se ha denominado "delito informático", en relación con la delincuencia patrimonial y socioeconómica[6] y el resto de delitos cometidos a través de la informática, relativos a la intimidad, la libertad, la indemnidad sexual… En este segundo ámbito es donde Internet es el instrumento que justifica desde una perspectiva político-criminal un tratamiento diferenciado, tanto por el Derecho penal material como por el procesal.

2.2. Naturaleza del delito informático. Para un sector doctrinal el delito informático es únicamente una forma de realización de distintos tipos delictivos. En consecuencia

4. Cfr. Fernández Teruelo, *Cibercrimen*…, op.cit, p. 14-26.

5. Cfr. Mata y Martín, *Estafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago*, Ed. Thomson/Aranzadi, 2007, p. 173-195, con referencia a la normativa que se ha dictado en el marco de la Comunidad Europea para luchar contra la delincuencia informática.

6. Vid. Mata y Martín, *Estafa Convencional, Estafa Informática*… op.cit., passim., obra que está, específicamente, orientada a este aspecto de la Cibercrimalidad.

el bien jurídico protegido en el delito informático será aquél protegido en el delito que presuntamente se ha realizado: patrimonio, Hacienda Pública… Otra concepción de la criminalidad informática le concede autonomía entendiendo que con el fraude informático se protege un bien jurídico con naturaleza propia: "*la confianza en el funcionamiento de los sistemas informatizados*", como interés de carácter supraindividual –colectivo–. Se parte de que el buen funcionamiento de los sistemas es condición indispensable para el normal desarrollo de las relaciones económicas y personales de nuestros días, porque de ello depende que no se colapsen las actividades del mundo bancario, bursátil, de seguros, transportes, gestión tributaria, Seguridad Social, sanitario… Esta segunda posibilidad es la admitida en muchas legislaciones locales estadounidenses que tipifican, de forma autónoma, conductas de acceso ilegal a un sistema informático, su uso sin autorización y la manipulación ilícita y modificación de datos informatizados, siguiendo una construcción análoga a la de las falsedades. Según esta regulación, si como consecuencia de una de estas manipulaciones se obtiene una subvención ilícita o se comete un delito fiscal estaríamos frente a un concurso ideal o real de delitos, en el mismo sentido que en la actualidad se suscita entre falsedades y delito fiscal o entre delito fiscal y contable. Con estas previsiones se trata de adelantar las barreras de protección en atención a la especial peligrosidad que suponen estos nuevos instrumentos de comisión de delitos. Nuestro Código Penal recoge algunas conductas típicas cuya única legitimación sería entender que el bien jurídico protegido son los propios sistemas informatizados, o la confianza en su buen funcionamiento. Esta naturaleza ostentan los preceptos introducidos por LO 15/2003, que tipifican: a) actos preparatorios de la estafa informática, art. 248.3 CP; b) la fabricación, importación, distribución o tenencia de medios destinados a suprimir o neutralizar sistemas de protección de los programas, art. 270.3 CP; y c) facilitar el acceso a sistemas, art. 286.1 y 3 CP, alterar o duplicar números identificativos o comercializarlos, art. 286.2 CP e, incluso, la utilización de los equipos o programas que permiten el acceso no autorizado, art. 286.4 CP.

2.3. Elementos del delito informático. A pesar de los diversos conceptos que se han propuesto sobre el delito informático y la discusión existente acerca de su naturaleza, lo cierto es que, en todos ellos, encontramos unos elementos comunes:

a) Conducta fraudulenta: uso indebido o fraudulento de elementos informáticos a través de la introducción o manipulación de datos falsos.

b) Instrumento: presencia de los componentes físicos y/o lógicos del sistema informático.

c) Finalidad: obtención de un beneficio ilícito, directo o indirecto, no necesariamente patrimonial.

d) Resultado: perjuicio, no necesariamente patrimonial, de tercero o de la colectividad.

Como veremos, la llamada estafa informática regulada en el art. 248.2 CP, podría calificarse como delito informático puesto que posibilita castigar como estafa la modificación ilícita de un resultado, a través de alterar un procesamiento informático con ánimo de lucro y en perjuicio de tercero[7].

7. Cfr. Romeo Casabona, *Poder informático y seguridad jurídica*, Ed. Fundesco 1987, ya definía la manipulación informática como: "incorrecta modificación del resultado de un procesamiento automatizado en cualquiera de sus fases de procesamiento o tratamiento informático con ánimo de lucro y en perjuicio de tercero".

2.4. Modalidades delictivas relacionadas con la incorporación de los documentos informáticos. En parte, la tipicidad de conductas relacionadas con la informática proviene de la incorporación de los datos informatizados al concepto penal de documento. El art. 26 CP equipara, al concepto clásico de documento como papel escrito, todo soporte material que exprese o incorpore datos. A efectos penales es documento cualquier soporte informático que exprese o incorpore datos o hechos con cualquier tipo de relevancia jurídica[8]. El art. 7 de la Convención del Consejo de Europa sobre Cibernética, incrimina la falsificación de documentos electrónicos, entendiendo por falsificación tanto la alteración de sus funciones como su destrucción. No obstante, y pese a que de la redacción del art. 26 CP se podría concluir que cualquier dato incorporado a una soporte informático sería un documento no cabe entender por tales los que no sean atribuibles a una persona[9].

a) Falsedades documentales. Lo relevante del art. 28 CP, es que elimina el problema que, con anterioridad a esta regulación, se había suscitado para calificar como documento los datos informatizados y, en consecuencia, para calificar como falsedades documentales, la falsificación de esta clase de documentos. Por consiguiente, cuando los arts. 390 ss. CP, se refieren a documentos se ha de interpretar que tienen también está consideración los datos informáticos siempre que sean idóneos para alterar la realidad jurídica, en cuanto cumplan las funciones de perpetuación, garantía y prueba, atribuidas a los documentos. La autenticidad de un documento electrónico requiere que los datos informáticos que se utilicen como medio para identificar al autor de la declaración provengan de persona autorizada y no del abuso del secreto de las bases que lo garantizan. Entiendo, sin embargo, que el abuso de estas claves podría calificarse también como falsificación del documento, siempre que pueda identificarse la autenticidad[10]. Con la actual regulación siguen suscitándose dudas acerca de la autenticidad porque el certificado que emiten los prestadores de servicio sobre la autenticidad del documento y la firma electrónica se genera automáticamente. La posibilidad de que la alteración de documentos electrónicos sea típica es político-criminalmente indispensable, si tenemos en cuenta que, cada vez en mayor medida, los documentos tanto públicos, como mercantiles e incluso oficiales se reflejan en datos informatizados y se introducen en el tráfico jurídico a través de un sistema informático. Todo ello es de aplicación a las falsedades documentales especiales previstas, por ejemplo, en los delitos societarios, art. 290 CP, falseamiento de cuentas anuales o documentos que reflejen la situación jurídica o económica de la sociedad o en el llamado "delito contable", art. 310 CP.

b) Falsificación de moneda. La incorporación de la informática a la falsificación de moneda surge a partir del art. 387 CP, redactado conforme LO 15/2003, en el que se equipara a la moneda de curso legal, el llamado "*dinero de plástico*" –tarjetas de crédito, de débito…–. Consecuentemente, la manipulación de la banda magnética de uno de esos instrumentos de pago constituye un proceso de elaboración

---

8. Entre otras, SSTS 1456/2002, 13 de septiembre; 626/2002, 11 de abril; 389/1999, 12 de marzo; 913/1998, 30 de junio; 579/1998, 22 de abril; 1573/1997, 19 de enero de 1998.

9. Cfr. QUERALT JIMÉNEZ, *Derecho penal español. Parte Especial*, 5ª ed. Ed. Atelier 2008, p. 621 ss., se muestra crítico ante la redacción del art. 28 CP en base a que sólo da importancia al soporte en el que se incorporan datos sin exigir que esos datos sean inteligibles y atribuibles a una persona.

10. Cfr. Ley 59/2003, 19 de diciembre, de firma electrónica y RDL 14/1999, sobre firma electrónica, que incorpora la ordenamiento jurídico español la Directiva CEE 99/93, 13-12, sobre las condiciones relativas a las firmas electrónicas y a los servicios de certificación.

o fabricación de moneda, incardinable en el art. 386 CP[11]. La inclusión de un precepto específico que contemple la falsificación de tarjetas, responde a la Decisión Marco del Consejo de Ministros de la UE, de 28 de mayo de 2001, sobre "*la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo*". Esta normativa abarca las alteraciones de tarjetas de crédito pero no el dinero electrónico, es decir, las transferencias fraudulentas de dinero. Estas conductas pueden ser calificadas como estafa, apropiación indebida o alzamiento de bienes pero no como falsificación de moneda, puesta que ésta requiere, en todo caso, un soporte material.

c) Delincuencia socio-económica. En todos aquellos delitos socio-económicos en los que la conducta típica, de engaño, apropiación, defraudación…, se lleva a efecto a través de la manipulación fraudulenta de documentos informatizados, como veremos, se han minimizado si no eliminado los problemas para calificar esos comportamientos como típicos.

2.5. Otros delitos relacionados directa o indirectamente con la delincuencia informática

a) Pornografía infantil

Las reformas del Código Penal en esta materia han supuesto la incriminación de nuevas conductas, la incorporación de elementos típicos agravantes y el endurecimiento de las penas, en gran medida por el auge de la pornografía infantil y la facilidad de distribución y acceso que proporciona Internet. Situación que ha sido denunciada por las más diversas instancias internacionales[12]. En un primer momento, por LO 11/1999, de 30 de abril, se introdujo el delito de corrupción de menores, que había sido derogado por el CP de 1995, modificando el art. 189.1 CP. En este apartado se introduce como conducta típica la producción, venta, distribución y exhibición por cualquier medio de material pornográfico en el que se hubieran utilizado menores. Para evitar lagunas de punibilidad, que podría propiciar Internet, se establece una excepción absoluta del principio de territorialidad, de forma que la tipicidad alcanza a los supuestos en los que el material tiene su origen en el extranjero o del que se desconozca su procedencia. Más criticable es la equiparación, en este mismo inciso, de la conducta de producir, vender…, con la de facilitar esas mismas conductas[13]. Por LO 15/2003, se incrementan las penas en estos delitos, se introducen nuevos tipos agravados y, en el art. 189.2 CP, se prevé el castigo de la tenencia para uso propio de material pornográfico en el que se hubieran utilizado menores. Así mismo se prevé el castigo de la llamada pornografía infantil "virtual", en la que sin utilizar a menores se emplea o utiliza su voz o imagen modificada (art. 189.7 CP). Los argumentos a favor de la incriminación de conductas en las que es difícil justificar la lesión, no ya de la libertad sexual, sino también de la indemnidad

---

11. Cfr. Acuerdo no jurisdiccional del Pleno de la Sala 2ª del TS, de 28 de junio de 2002.

12. Cfr. Fernández Teruelo, *Cibercrimen*…, op.cit, p. 54 ss., ampliamente sobre las Convenciones y normativa internacional en las que se insta a los Estados a establecer las medidas necesarias para proteger a los menores.

13. Cfr. Fernández Teruelo, *Cibercrimen*…, op.cit, p. 72 ss, analiza los diversas formas en que se distribuye la pornografía en Internet que, en algunos supuestos, podría dificultar su castigo, pero que cabría siempre en la fórmula de "facilitar" la producción, distribución, venta, exhibición…

sexual de menores o incapaces, ponen el acento en la facilidad que se tiene de acceso a esta pornografía y, en consecuencia, el riesgo de que estas personas se introduzcan de lleno en la pornografía infantil real[14]. Problemática que se acentúa dado que la protección alcanza hasta los 18 años, cuado en los abusos sexuales la falta de consentimiento válido se sitúa en los 13 años. Solución discutible desde una perspectiva político-criminal, que, tanto desde un punto de vista de derecho penal material como procesal, se incrementa por la dificultad de determinar la edad. En este sentido, habrá que valorar, primero, la concurrencia de dolo, que requiere el conocimiento de la minoría de edad, y, en caso de dudas, aplicar el principio *in dubio pro reo*.

b) Descubrimiento y revelación de secretos personales y profesionales

1º Descubrimiento y revelación de secretos personales. En la doctrina se ha discutido si la protección de los datos informatizados es un bien jurídico autónomo respecto de la intimidad o no. En esta dirección un sector de la doctrina afirma que en los tipos relacionados con datos informatizados se protege el "derecho a la autodeterminación informativa"[15] o "derecho a la protección de datos personales"[16]. Creo, sin embargo, que esta diferenciación carece de fundamento serio y que con la protección de los datos informatizados lo que realmente se protege es el derecho a la intimidad[17]. No puede olvidarse que la informática es un instrumento idóneo para cambiar o incorporar nuevas modalidades de conductas que atentan contra la intimidad e, incluso, facilitar los ataques. Ello puede justificar una regulación específica, incluso en el ámbito penal, pero no la autonomía del bien jurídico protegido. Por lo demás esta pretendida autonomía sólo serviría para dificultar la protección o formalizarla.

En el art. 197.2 y 3 CP se contempla expresamente tanto el apoderamiento de datos personales que se encuentren en soportes informáticos como el acceso "por cualquier medio" a los mismos[18] y su divulgación, revelación o cesión. La regulación penal atiende a las especiales características que reviste el almacenamiento de datos en soportes informáticos, tomando en consideración la LO 15/1999, de Protección de Datos de Carácter Personal, modificada por LO 62/2003. En este precepto se

---

14. Cfr. Boldova Pasamar, "Art. 189", en *Comentarios al Código Penal. Parte Especial*, vol. II (Díez Ripollés/Romeo Csabona Coords.), Ed. Tirant lo Blanch 2004, considera que esta conducta supone un peligro abstracto para la libertad e indemnidad sexual de los menores; en otro sentido, Díez Ripollés, "Trata de seres humanos y explotación sexual de menores. Exigencias de la Unión y legislación española", *Revista Penal* nº 2, 1998, p. 19, incluso antes de la última reforma, consideraba que en algunas de las conductas típicas se castigan prácticas que se apartan de las "sexualmente mayoritarias".

15. Lucas Murillo de la Cueva, *El derecho a la autodeterminación*, Ed. Tecnos, Madrid 1990, p. 27 ss.

16. Oliver Lalana, "El derecho fundamental "virtual" a la protección de datos. Tecnología transparente y normas privadas", *La Ley* 22 julio 2002, p. 1 ss.; en la jurisprudencia constitucional, en el mismo sentido, STC 254/1993 FJ 6º.

17. En el mismo sentido, Ruiz Miguel, "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea", en *Temas de Direito da Informática e da Internet*, Ed. Coimbra, Janeiro 2004, p. 47.

18. Comete este delito el *hacker* que accede a datos sensibles, en este sentido, Queralt Jiménez, *Derecho penal español,* op.cit., p. 260 ss., citando la sentencia del Juzgado de lo Penal de Barcelona, de 15 de febrero de 2006, caso Wanadoo.

tipifica, así mismo, la alteración o utilización de datos informatizados en perjuicio del titular de los datos o de tercero. En el art. 197.4 CP se prevé un tipo agravado para los supuestos en los que el autor sea el encargado de los ficheros o soportes informáticos. En el mismo sentido, en el art. 198 CP, se regula otro tipo agravado para los casos en que el autor sea funcionario público, siempre que para la realización de la conducta se prevalga de su cargo.

En esta línea, el Proyecto de Reforma del Código Penal, que entró en el Congreso de los Diputados, el 15 de enero de 2007, y ha quedado en suspenso, establecía que "*La tutela penal de la intimidad y de los secretos ha sido tradicionalmente fragmentaria, y condicionada a la realización de conductas de apoderamiento de papeles, cartas o mensajes, o de instalación de aparatos de captación de imagen o sonido, pero a la vez que la importancia fundamental de ese bien jurídico exige cada vez mayor atención y medidas legales, como son esencialmente las recogidas en la legislación sobre protección de datos, crecen los riesgos que lo rodean, a causa de las intrincadas vías tecnológicas que permiten violar la privacidad o reserva de datos contenidos en sistemas informáticos. Esa preocupante laguna, que pueden aprovechar los llamados hackers ha aconsejado, cumpliendo con obligaciones específicas sobre la materia plasmadas en la Decisión Marco 2005/222/JAI de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información, incorporar al artículo 197 del Código penal un nuevo apartado que castiga a quien por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático. La realidad de que los actos de invasión en la privacidad en todas sus manifestaciones no son siempre llevadas a cabo por individuos aislados ha determinado la incorporación de una cualificación punitiva para todas las acciones descritas en el artículo 197 en el caso de que se cometan en el marco de organizaciones criminales*".

Esta reforma respondía a la Decisión Marco 2005/222/JAI, de 24 de febrero, y proponía la modificación del apartado 3º del art. 197 CP, tipificando expresamente el acceso ilícito a datos o programas informáticos, siempre que se vulneren medidas de seguridad. Es decir, se configura como un "robo con fuerza", ¿debemos entender que el "hurto" sería atípico, o, por el contrario, se castigaría conforme al 197.2 CP que, por cierto, lleva aparejada una pena mayor?

2º Descubrimiento y revelación de secretos laborales y profesionales. En el artículo 199 CP, que tipifica el descubrimiento y revelación de secretos laborales y profesionales, no se contempla de forma específica el hecho de que los secretos se encuentren en soportes informáticos, pero, en principio, debe entenderse que la previsión respecto de los secretos personales tiene eficacia, en los aspectos que ello sea posible, también en este ámbito, ya que ambos preceptos se encuentran en el mismo Capítulo. Infra veremos la problemática que puede suscitar la autoría en estos casos.

c) Delitos contra el patrimonio

1º Delitos contra el patrimonio de apoderamiento: robo con fuerza en las cosas. La utilización de tarjetas magnéticas o de cualquier otra modalidad de apertura electrónica para acceder al lugar donde se encuentran los bienes muebles ajenos y apro-

piarse de ellos había planteado problemas sobre si la utilización ilícita de estos sistemas de apertura podía entenderse abarcado por el concepto normativo de "fuerza" previsto en el Código Penal. En la actualidad, la calificación de las conductas en las que se accede a los bienes ajenos utilizando sistemas informáticos puede ser calificada como robo con fuerza y no como hurto. La introducción del párrafo 5º del art. 238 unido al nuevo concepto de llave falsa, previsto en el artículo 239.3º CP, soluciona este debate. Con el art. 238.5º se considera fuerza la inutilización de cualquier sistema de alarma o guarda, lo que implica calificar como fuerza en las cosas la inutilización, por ejemplo, de sistemas informáticos que comuniquen la vivienda con la policía o empresas de seguridad. Así mismo, expresamente, el art. 239.3º CP, a efectos penales, equipara a llave falsa, la utilización de tarjetas magnéticas o perforadas y los mandos o instrumentos de apertura a distancia. No obstante, la casuística utilizada al referirse a las "tarjetas" y limitarlas a las perforadas y magnéticas suscita de nuevo lagunas de punibilidad. Ello es así porque hay tarjetas de apertura que no son de esa naturaleza sino que utilizan otros sistemas informáticos[19].

2º Delitos contra el patrimonio de defraudación: "delito informático" (estafa a través de manipulaciones informáticas). Problema similar al anterior suscitaba la discutida "*utilización abusiva de tarjetas de crédito en cajeros automáticos*", que se había calificado indistintamente como robo con fuerza en las cosas, como apropiación indebida e, incluso, como estafa, aun cuando, como había puesto de relieve la doctrina mayoritaria[20], fundamentar esta última calificación era muy difícil puesto que en estos supuestos afirmar la concurrencia de engaño que induce a error, error que a su vez provoca la disposición patrimonial era más que discutible[21]. En el artículo 248.2 CP se equipara a la estafa la manipulación informática dirigida a conseguir la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero[22]. En consecuencia, este tipo permite calificar como estafa no sólo la "*utilización abusiva de tarjetas de crédito en cajeros automáticos*" sino, también, otros muchos supuestos de estafas, así como apropiaciones indebidas, delitos societarios, alzamientos de bienes… La amplitud del precepto posibilita interpretarlo como tipificación del llamado **delito informático**, al que nos referíamos con anterioridad, ya que los elementos previstos en el artículo 248.2 CP son los mismos que un amplio sector entiende como constitu-

---

19. En este sentido, QUERALT JIMÉNEZ, *Derecho penal español,* op.cit., p. 423 ss.

20. Por todos, vid. MATA Y MARTÍN, "Criminalidad informática: una introducción al Cibercrimen", en *Temas de Direito da Informática e da Internet*, Ed. Coimbra, Janeiro 2004, p. 32 ss, ampliamente sobre los problemas que se suscitaban para calificar estas conductas como estafa.

21. En otro sentido, DE LA MATA BARRANCO, "Utilización abusiva de cajeros automáticos: apropiación de dinero mediante tarjeta sustraída a su titular", *Poder Judicial* nº especial IX 1988, p. 172 ss.; GUTIÉRREZ FRANCÉS, "Fraude informático y estafa", *Actualidad Informática Aranzadi* (11) 1994, p.11, afirmaban que no existe una predeterminación legal del concepto de engaño y que, por consiguiente, no requiere necesariamente una relación directa entre dos personas.

22. La doctrina mayoritaria alemana y un amplio sector de la española estiman que este precepto mantiene el núcleo esencial de la estafa. Cfr. KINDHÄUSER, *Nomos Commentar zum Strafgesetzbuch*, Band 5, 2003, párr. 263ª; VOGEL, "Estafa en la UE", *Fraude y corrupción en el Derecho penal económico europeo* (Arroyo/Nieto Coords.), Universidad de Castilla la Mancha 2006, p. 45; GONZÁLEZ CUSSAC, *Derecho Penal. Parte Especial*, Ed. Tirant lo Blanch 1999, p. 453 ss; ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Ed. Tirant lo Blanch 2001, p. 69; GONZÁLEZ RUS, *Derecho penal español. Parte Especial* (Cobo del Rosal Coord.), Ed. Dykinson 2005, p. 522; MATA Y MARTÍN, *Estafa Convencional, Estafa Informática…* op.cit, p. 63 ss..

tivos del delito informático: actuación fraudulenta e ilícita, sobre medios informáticos, para obtener un beneficio provocando el perjuicio de tercero[23]. Por LO 15/2003, se introduce un nuevo apartado en el que se tipifican conductas preparatorias para la comisión de estas estafas informáticas, consistentes en producir, introducir, poseer o facilitar programas de ordenador destinados a la comisión de estafas informáticas. El precepto tiene un significado análogo al delito de tenencia de útiles para las falsificaciones, art. 400 CP, en el que también se han incorporado, expresamente, los programas de ordenador como sistema para llevar a efecto la falsificación. En todo caso, incluso aceptando que político-criminalmente sea adecuada su incriminación, atendiendo al principio de proporcionalidad es inaceptable que se castigue con la misma pena un acto preparatorio. Crítica a la que se suma la referente a la tenencia, que habrá que restringir en el sentido de que se pruebe su destino al tráfico, así como la equiparación de "facilitar" a las conductas de producir o introducir que deberá interpretarse como distribuir. Por otra parte, es evidente que los supuestos en los que el programa tenga otras utilidades, la conducta no es típica porque no puede considerarse "específico" para la comisión de estafas informáticas.

La importancia de la utilización de la informática para la comisión de delitos patrimoniales llevó a que, en el Proyecto de Reforma del Código Penal de 2007 (PRCP 2007)[24], en su Exposición de Motivos, se estableciese que: "*Entre las estafas descritas en el artículo 248 del Código penal, cuyo catálogo en su momento ya se había acrecentado con los fraudes informáticos, ha sido preciso incorporar la cada vez más extendida modalidad consistente en defraudar utilizando las tarjetas ajenas o los datos obrantes en ellas, realizando con ello operaciones de cualquier clase en perjuicio de su titular. Pero no acabarán ahí las modificaciones penales provocadas por los delitos vinculados a las tarjetas, como más adelante se expondrá."*[25]. Con esta reforma se pretendían dos finalidades, en ambos casos

---

23. Cfr. González Rus, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", *RECPC* 01-04, 1999, entiende que en este precepto caben todos los casos en los que "se efectúa una transferencia no consentida de activos patrimoniales en perjuicio de tercero"; en otro sentido, Queralt Jiménez, *Derecho penal español,* op.cit., p. 480 ss., considera que este precepto no puede considerarse estafa por lo que no puede castigarse la falta ni aplicase las agravantes del art. 250 CP, y se muestra crítico por entender que no respeta el principio de legalidad; Chocián Montalvo, "Estafa por computación y criminalidad económica vinculada a la informática", *Actualidad Penal* 1997, p. 1079, consideraba que la estafa clásica y la informática no eran asimilables; el mismo, *El delito de estafa*, Ed. Bosch 2000, p. 297, matiza su postura anterior y afirma que sí son aplicables las agravantes del art. 250 CP. Para otro sector de la doctrina, estas conductas tienen mayor similitud con los delitos de apoderamiento, en este sentido, Anarte Borrallo, "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información", *Derecho y Conocimiento*, en *Anuario Jurídico sobre la Sociedad de la Información*, vol. 1, Universidad de Huelva 2001, p. 231; Mestre Delgado, *Manual de Derecho penal (Parte especial)*, Ed. Colex 2001, p. 266 ss.

24. Proyecto de Reforma que entró en el Congreso de los Diputados el 15 de enero de 2007. Lo tomo en consideración pese a que por la coyuntura política no es posible que sea aprobado, porque los preceptos analizaos en este trabajo responden a Directiva Europeas. En consecuencia, es de esperar que, en algún momento, en su caso con modificaciones no muy relevantes, pasen a ser legislación vigente.

25. El PRCP 2007, modificaba el apartado 2. del art. 248, en el siguiente sentido:

2. También se consideran reos de estafa:

…

discutibles desde una perspectiva político-criminal. En primer lugar, se regulaba de forma más amplia algo que ya estaba previsto en el art. 248.2 CP. Ello es así porque la redacción típica del precepto permite castigar no sólo la utilización fraudulenta de tarjetas de créditos sino también la utilización de datos obtenidos de esas tarjetas para comprar en Internet…, conforme a su comprensión como "delito informático"[26]. Por otro lado, se trataba de adelantar de nuevo las barreras de protección castigando tanto la producción como la introducción o el facilitamiento de programas de ordenador destinados a la comisión de estafas informáticas. En el supuesto del llamado *phising* (consistente en obtener, a través de Internet, datos personales sobre números de cuentas bancarios de tarjetas de crédito…, de una persona para crear cuentas falsas, gastar su dinero…), entiendo que no cabría en este segundo apartado. Sin embargo, no es necesaria una tipificación expresa puesto que cuando se usan esos datos estaríamos frente una manipulación informática, típica conforme al art. 248.2 CP. Las dudas que plantea la doctrina parten de que se trataría de una conducta omisiva que difícilmente encaja en la estafa, sin embargo, no cabe duda de que, independientemente de cómo se hayan obtenido los datos, su utilización fraudulenta es activa[27].

3º Defraudaciones: hurto de uso del Software y del Hardware. La utilización del sistema informático sin costo consiste en el acceso ilegítimo a un sistema informático, para su utilización en beneficio propio, que suponga un perjuicio económico para el titular del sistema informático. En el Código Penal de 1995 se introduce el artículo 256 CP[28], que protege el uso ilegítimo de los sistemas y medios informáticos. No obstante, en este precepto se hace referencia expresa a las telecomunicaciones pero no a los sistemas informáticos, por lo que, en su caso, se debería

---

…

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren o facilitaren programas informáticos especialmente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en ellos, realicen operaciones de cualquier clase en perjuicio de su titular.

26. Cfr. STS 20 noviembre de 2001, establece que la manipulación informática puede consistir en la alteración de elementos físicos o en la introducción de datos falsos. En otro sentido, CHOCLÁN MONTALVO, "Infracciones patrimoniales en los procesos de transferencias de datos", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Ed. Comares 2006, p. 76 ss., plantea dudas, en atención al principio de legalidad, acerca de la tipicidad de la introducción en el sistema de nuevos datos ajenos para realizar compras.

27. Cfr. MATA Y MARTÍN, *Estafa convencional, estafa informática*…, op.cit., p. 86, pone de manifiesto que, aunque inicialmente puedan verse como casos omisivos, son realmente comportamientos comisivos.

28. Artículo 256, modificado por LO 15/2003, *El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a 400 euros, será castigado con la pena de multa de tres a 12 meses.*

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses..

entender que estos están comprendidos en el art. 255, dentro de "*u otro elemento… ajeno*". Por otra parte, la nueva regulación, en relación con la anterior al CP de 1995, amplía también las modalidades de conductas típicas, que de acuerdo con el artículo 536 CP 1973, eran muy limitadas. Según el artículo 255. 3º CP, serán conductas típicas todas aquellas que sean adecuadas para defraudar una energía, fluido o elemento ajeno cualesquiera que sea el "*medio clandestino*" utilizado para lograr dicha defraudación. Por tanto, cualquier acceso ilícito al sistema informático podría calificarse como "medio clandestino", siempre que sea necesario utilizar claves ajenas. Incluso con el sistema WIFI, excepto si es en abierto, precisa introducir una clave para poder acceder.

d) Delitos contra el patrimonio sin enriquecimiento: Sabotaje informático.

La protección del Software y de los datos informatizados se tipifica, de modo específico, en el artículo 264. 2 CP que castiga los daños producidos sobre cualquier elemento informático. En este precepto se amplía el concepto tradicional de daño, siguiendo la teoría funcional de la utilidad, a los supuestos de destrucción, alteración o inutilización de datos, programas o documentos. Con ello se pretende contemplar, por un lado, la especial característica de los daños informáticos –ocasionados por medios distintos a la mera destrucción física– y, por otro, la especial gravedad del perjuicio originado con esta modalidad de daños, sobre todo si se tiene en cuenta el relativamente bajo o nulo valor material del soporte físico que se destruye o incluso la inexistencia de destrucción, en sentido estricto[29]. La especial protección penal de los medios informáticos se entiende mejor si ponemos en relación este delito con la cláusula concursal prevista en el artículo 278. 3 CP, a la que hicimos referencia, en la que se considera concurso de delitos y no de leyes la concurrencia, junto al descubrimiento de secretos de empresa, de la destrucción, alteración o inutilización de estos datos informatizados. En relación con el problema que advertíamos en el apartado anterior, la regulación del sabotaje informático, ubicada entre los delitos de daños, dificulta entender como típica la destrucción de soportes informáticos por el propio creador del programa, ya que el artículo 264.2 CP, lógicamente, al tratarse de un delito contra la propiedad, se refiere a la causación de daños en programas "ajenos", por lo que en los supuestos de destrucción del programa por su autor será difícil la consideración de esta conducta como típica.

En relación con el llamado sabotaje informático en el PRCP, se introducían modificaciones, justificadas en base a que: "*Pasando ahora al delito de daños valga decir que la reforma no ha hecho otra cosa que unir los actuales arts. 263 y 264, para facilitar la comprensión del sentido de unas normas que no tenían que estar separadas al tratarse siempre de la misma conducta variando en función de medios y de finalidades. En cambio, resultaba inadecuada la presencia de la destrucción de documentos, datos o programas contenidos en redes, soportes o sistemas informáticos, que reciben su propia regulación en el siguiente artículo 264, que se destina en exclusiva a las diferentes modalidades de ataques a los sistemas informáticos entre las cuales los antedichos daños son sólo una posibilidad. Con esa especialización*

29. Cfr. Corcoy Bidasolo, "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", *La Ley* vol. 1, nº 2400, 1990, passim, ampliamente sobre la diversidad de conductas que caben en este concepto y la analogía de estas conductas con los daños comunes, si se interpretan conforme al concepto funcional de daño. Es decir, daño no como destrucción sino como inutilización.

de los daños se completa el cumplimiento de la ya mencionada DM 2005/222/JAI sobre ataques contra los sistemas de información."[30]. En la propuesta, sin embargo, aunque pretendidamente tratara de incorporar nuevas conductas típicas, al utilizar una técnica legislativa casuística, introduce nuevos verbos típicos que serían subsumibles en los ya previstos y la misma finalidad de exhaustividad puede dar lugar a lagunas de punibilidad no justificadas. En sentido positivo, es adecuada tanto la incorporación de tipos agravados como la limitación de la tipicidad a supuestos que revistan gravedad. Esto último es especialmente relevante sobre todo teniendo en cuenta que en esta modalidad de daños no existe un requisito de punibilidad que limite la tipicidad, como sucede con la cuantía superior a 400 euros, en los daños comunes.

e) Delitos contra la propiedad intelectual

1º Protección del Software[31]. La protección penal de los derechos de autor del creador de un programa informático se tipifica en el art. 270 CP, ya que el programa de ordenador, de acuerdo con la Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual (LPI), es objeto de protección según el art. 10. 1. i) de dicha ley[32]. En consecuencia, los programas de ordenador, en cuanto a su protección penal, se equiparan a las obras literarias, artísticas o científicas. La protección de los programas en la LPI, se ha de poner en relación con la L 16/1993, de 23 de diciembre, de incorporación al derecho español de la Directiva 91/250 CEE, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador, que pretende unificar la legislación europea en materia de protección de los programas de ordenador y establece los límites, titulares y requisitos de la protección de los programas. De acuerdo con esta normativa, art.

---

30. Art. 264. PRCP *1. El que sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos o programas informáticos ajenos, será castigado, en consideración a la gravedad del hecho, con la pena de prisión de seis meses a dos años.*

2. El que sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema de información ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, será castigado, atendiendo a la gravedad del hecho, con la pena de prisión de seis meses a tres años.

3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1º. Se hubiese cometido en el marco de una organización criminal.

2º. Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

4. Cuando los delitos comprendidos en este artículo se hubieren cometido en el marco o con ocasión de las actividades de una persona jurídica y procediere la declaración de su responsabilidad penal de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado en los supuestos previstos en los apartados 1 y 2, y del tanto al décuplo en el supuesto del apartado 3."

31. Ampliamente sobre al protección penal del software, MATA Y MARTÍN, "Perspectivas sobre la protección penal del software", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político.-criminales* (Romeo Casabona Coord.), Ed Comares 2006, p. 97 ss.

32. Cfr. MATA Y MARTÍN, "Protección penal de la propiedad intelectual y servicios de radiodifusión e interactivos: excesos y equívocos", en *Gobierno, Derecho y Tecnología: las actividades de los poderes públicos* (Fernando Galindo Coord.), Ed. Thomson-Civitas 2006, p. 299 ss, críticamente sobre la protección penal de los programas de ordenador en el Código Penal.

1º 1, los programas se asimilan a las obras literarias o artísticas, siguiendo la directriz establecida en el Convenio de Berna. Según el art. 1º 3, se protegen únicamente los programas originales, en el sentido de que sean una creación intelectual propia del autor, excluyendo de esta protección los programas que tengan como finalidad ocasionar efectos nocivos en un sistema informático, art. 1º 4. Esta excepción tiene una especial importancia dados los gravísimos perjuicios que se han ocasionado a través de la utilización de programas destructores –*crash programs*–. Los programas destructores, aun cuando sean originales, no pueden ser objeto de protección ni a través de la Ley de Propiedad Intelectual ni, por consiguiente, por los delitos contra la propiedad intelectual. Un problema particular, que no ha sido contemplado, ni en esta normativa ni en el Código Penal, es la utilización de estos programas destructivos por el propio creador de un programa que ha sido vendido a un tercero, al que le destruyen sus soportes informáticos. En el art. 270.3 CP. se castiga la creación, puesta en circulación y tenencia de un programa destinado a inutilizar los sistemas de protección de otro programa[33]. Partiendo de que, tratándose de actos preparatorios[34], protegidos además civilmente, es discutible que esté legitimada la intervención penal, no se entiende la razón por la cual este precepto limita la conducta típica a los supuestos en que el programa destructor esté dirigido a suprimir dispositivos de protección y no se castiga la creación, puesta en circulación o tenencia de programas que tengan como finalidad ocasionar efectos nocivos en estos mismos programas.

2º Protección de los derechos de autor. Internet, junto con los más diversos sistemas reproductores, al alcance de cualquiera, ha propiciado el acceso ilegítimo a obras originales protegidas a través de la LPI, al igual que los programas de ordenador a los que se hizo referencia[35]. Este acceso puede llevarse a efecto con fines comerciales o para uso propio o de un grupo. El término *piratería* se concibe como la comercialización y distribución de obras protegidas por la LPI a través de Internet. En la reforma de la LPI por Ley 23/2006, se trata, entre otras cuestiones, de trasladar el modelo tradicional de canon analógico al canon digital, restringir el concepto de copia privada al ámbito doméstico y regular la instalación de medidas tecnológicas anticopia. Pese a toda esta normativa sigue siendo muy sencillo acceder a todo tipo de obras (música, cine, fotos, libros…) en toda clase de soportes (DVD, CD…) por precios cuasi simbólicos o gratis. El hecho de que muchas de estas conductas sean irrelevantes, valoradas individualmente, y de que tengan como única finalidad el uso de la obra obtenida, dificulta la protección legal y muy especialmente la penal, desde el momento en que el art. 270 CP requiere ánimo de lucro. Cuestión diferente son las organizaciones que se

---

33. Cfr. Gómez Martín, "El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3º CP. A la vez, un estudio sobre los delitos de emprendimiento o preparación en el CP de 1995", RECPC 04-16 (2002).

34. Para algunos autores no todas las conductas previstas en el art. 270.3º CP, son actos preparatorios sino sólo la tenencia. En este sentido, Jorge Barreiro, *Comentarios al Código penal* (Rodríguez Mourullo Dir./Jorge Barreiro, Coord.), Madrid 1997, p. 775; Gómez Martín, RECPC 04-16 (2002).

35. La Directiva 2001/29/CE, de 22 de mayo, trata de adecuar los derechos de autor y conexos al entorno digital, asumiendo las obligaciones contraídas en el marco de los Tratados Digitales OMPI (WCT Y WPPT). En la misma dirección se suceden diversas leyes y reglamentos al socaire de la normativa europea, entre los que cabría reseñar la Ley 19/2006, de 5 de junio, para facilitar la aplicación de reglamentos comunitarios en esta materia y la reforma de la LPI, por Ley 23/2006, de 7 de julio.

dedican a la copia y posterior comercialización de obras obtenidas ilícitamente. Respecto de los particulares se ha suscitado un duro enfrentamiento entre las sociedades que gestionan los derechos de autor y las asociaciones de consumidores y usuarios. Sin entrar a fondo en esta cuestión, por exceder con mucho de la finalidad de este trabajo, lo cierto es que no se pueden poner "puertas al campo" y que, independientemente de a qué consenso se llegue, carece de sentido la intervención penal. Entre otras razones, porque la redacción actual de los delitos contra la propiedad intelectual determina que el bien jurídico protegido se circunscriba al ámbito patrimonial[36]. Como decía, la exigencia típica de ánimo de lucro determina que queden fuera del ámbito penal todas las actividades de esta naturaleza realizadas de forma altruista, puesto que el ánimo de lucro debe ser interpretado estrictamente como lucro comercial[37].

3º Protección de la topografía de un producto semiconductor[38]. En el art. 273.3. CP, se protegen, dentro de los delitos contra la propiedad industrial, estos elementos informáticos cuando, conociendo que están registrados, se fabriquen, importen, posean, utilicen, ofrezcan o introduzcan en el comercio, sin el consentimiento del titular. Una vez más en estos ámbitos relacionados con la informática o mejor con las nuevas tecnologías se tipifican actos preparatorios, diferentes a los previstos en el art. 17 de la Parte General del Código Penal. Ello cuando la tipicidad de los actos preparatorios debería ser excepcional, en atención al principio de lesividad, y, de nuevo, con igual pena que las conductas a las que preceden, con evidente conculcación del principio de proporcionalidad. Consecuentemente, la doctrina[39] y jurisprudencia interpretan restrictivamente el tipo excluyendo la tipicidad en todos aquellos supuestos en los que esos elementos informáticos se posean para realizar copias privadas o/y que no sean específicos para eliminar o neutralizar la protección.

f) Delitos contra el mercado

1º Delitos de descubrimiento y revelación de secretos de empresa: espionaje industrial. En el art. 278 CP se prevé, expresamente, el descubrimiento de secretos de empresa a través del apoderamiento de soportes informáticos. La diferencia con los delitos de descubrimiento y revelación de secretos personales, profesionales o laborales debe delimitarse a partir del bien jurídico protegido, según afecte a la intimidad o al sistema económico y/o el patrimonio, y según la naturaleza de los datos descubiertos o revelados. Así mismo, cuando esos datos estén protegidos por la ley de propiedad industrial, estaremos ante un concurso de leyes. El delito está regulado de tal forma que se castiga el mero apoderamiento de los secretos, con lo que no se plantea el

---

36. Cfr. Díaz y García Conlledo, "Los derechos de autor conexos. Su protección penal: cuestiones generales y naturaleza patrimonial, personal o mixta del bien jurídico protegido", *ADPCP* 1990, p. 803 ss

37. Cfr. Fernández Teruelo, *Cibercrimen*…, op.cit, p. 98 ss, ampliamente sobre el *altruismo* y el concepto de ánimo de lucro.

38. Por topografía de productos semiconductores se entiende la disposición y diseño de los elementos y capas del circuito cerrado de "chips" empleados en el sector de la electrónica, el automóvil o la telefonía.

39. Cfr. Fernández Teruelo, *Cibercrimen*…, op.cit, p. 102 ss, entiende que en todo caso será necesario el ánimo de lucro. Por su parte la Circular de la FGE 15/2003, pone de manifiesto la licitud de quien está en posesión de un medio apto para obviar la protección con el objeto de realizar una copia privada en los términos que autoriza la LPI, en su art. 25, tras la reforma operada por Ley 23/2006.

problema que, en general, en estos casos se suscitaba cuando el autor es un empleado o un ex-empleado de la empresa. El apoderamiento de datos secretos de la empresa será típico sea quien sea el autor y tenga o no obligación de secreto. Esta interpretación se deriva de la redacción típica y de que en el art. 279 CP se prevé un tipo agravado para el supuesto en que quien se apodere de los datos "tuviere legalmente obligación de guardar reserva". En el apartado tercero del art. 278 CP, se establece una cláusula concursal según la cual en el supuesto de concurrir el descubrimiento y revelación de secretos empresariales con la destrucción de soportes informáticos estaremos frente a un concurso de delitos y no de leyes, lo que supone otorgar una especial autonomía a la informática como objeto de protección penal.

2º. Acceso ilegítimo a sistemas de comunicación y servicios. Se discute la ubicación sistemática entre los delitos contra el mercado y consumidores, al afirmar que se protegen los intereses de las empresas concesionarias o prestadoras de servicios y, por consiguiente, el patrimonio privado[40]. No obstante, en este supuesto, como en la mayoría de delitos contra el mercado y los consumidores, se protege, junto a un interés patrimonial privado, el mercado y la libre competencia. El art. 255 CP tipifica la defraudación de telecomunicaciones, a través de ampliar expresamente a los sistemas de telecomunicaciones, los supuestos clásicos de defraudación de fluido eléctrico y análogos. La analogía se mantiene no obstante, puesto que se incluye, como objeto del delito, cualquier "otro elemento, energía o fluido ajeno". Este precepto al delimitar las conductas típicas no abarca supuestos como el *Phreaking* (uso de frecuencias de audio para utilizar teléfonos ajenos) o el *Wardriving* (utilización no consentida de conexiones inalámbricas como el WI-FI o el Bluetooth), Excepto si aplicamos la cláusula genérica del art. 255. 3º, relativa al "empleo de medios clandestinos", que en relación con las conductas enunciadas supone equiparar a "medios clandestinos" la ausencia de consentimiento del titular[41]. Conductas que, sin embargo, en principio, podrían ser calificadas conforme al art. 256 CP, que tipifica el uso de terminales de telecomunicaciones sin el consentimiento de su titular[42]. El problema esencial estriba, en ambos casos, en la exigencia de un perjuicio superior a 400 euros, ya que, con independencia de la dificultad de valorarlo, en la mayoría de supuestos el titular tiene tarifa plana, por lo que el uso por tercero no le perjudica. Ello explica que las sanciones en este ámbito sean de naturaleza administrativa y se centren en los supuestos de utilización de sistemas de telecomunicación ajena por parte de hoteles, bares y comunidades de propietarios.

---

40. Cfr. Martínez-Buján Pérez, *Derecho Penal. Parte Especial* (A.A.V.V.), Ed. Tirant lo Blanch 2004, p. 588 ss.

41. Fernández Teruelo, *Cibercrimen*…, op.cit, p. 152 ss, considera sin embargo que estas conductas pueden castigarse conforme al art. 255 3º CP.

42. Fernández Teruelo, *Cibercrimen*…, op.cit, p. 153, entiende que estas conductas no pueden castigarse conforme al art. 256 CP porque no es necesario el acceso físico a un terminal ajeno.

g) Delitos contra intereses supraindividuales.

1º Atentados contra la seguridad nacional: revelación de secretos relativos a la seguridad nacional.

2º Atentado contra la integridad de los procedimientos basados en la informática y en los procesamientos de datos: delitos de falsedades.

3º Atentados contra la legitimación democrática de las decisiones parlamentarias vinculadas a los ordenadores: delitos electorales.

3. AUTORÍA Y PARTICIPACIÓN EN LOS DELITOS RELACIONADOS CON LA INFORMÁTICA. ESPECIAL CONSIDERACIÓN DEL SUJETO PASIVO

3.1. El particular funcionamiento de los sistemas informáticos, en unos casos, y los problemas de definición de la titularidad en otros condicionan la atribución de responsabilidad en los delitos cometidos a través de sistemas informáticos o contra éstos. A ello se suma el problema de identificación de los autores en base al teórico anonimato que proporciona la red, aun cuando ello suponga un problema de prueba que la propia tecnología puede facilitar, como de hecho se está comprobando. Desde la perspectiva del Derecho penal material, en particular, en los delitos cometidos a través de Internet, el problema esencial es determinar quién o quiénes son responsables jurídico-penalmente de entre todos los intervinientes. Es necesario saber a quién son imputables los hechos ilícitos y quiénes son meros facilitadores o tenedores. En particular, se plantea la responsabilidad de los intermediarios de servicios que hacen posible el acceso y transmisión de la información a través de la red[43]. La cuestión se complica cuando, como sucede en los delitos de corrupción de menores, se castiga la mera tenencia de pornografía infantil, incluso virtual.

3.2. Se ha planteado la posibilidad de aplicar la llamada responsabilidad en cascada, art. 30 CP, como concepto tradicional de autoría para delitos cometidos en medios de comunicación. De *lege lata* es posible aplicar el precepto porque finalmente Internet es un medio de comunicación aun cuando se suscita la cuestión derivada de la redacción del precepto que limita la aplicación a "medios o soportes de difusión mecánicos". Para algunos autores ello impide la aplicación del precepto porque deja fuera todos los medios de comunicación no mecánicos, es decir, no sólo Internet sino también la radio o la televisión[44]. Otro sector doctrinal entiende, por el contrario, que la drástica limitación de la aplicación del precepto a modos de impresión técnicamente poco avanzados y casi desaparecidos supondría su inaplicación y que, sin embargo, con una interpretación teleológica y no literal es posible su aplicación[45]. Con independencia de las críticas que merece este precepto, Internet tiene un sistema de funcionamiento muy diferente a los tradicionales, especialmente, en lo que respecta a los ámbitos de responsabilidad.

---

43. Cfr. Mata y Martín, "Criminalidad informática: una introducción al Cibercrimen…", op.cit, p. 205.

44. En este sentido, López Barja de Quiroga, *Autoría y participación*, Ed. Akal/Iure 1996, p. 90

45. Cfr. Gómez Tomillo, *Libertad de información y teoría de la codelincuencia. La autoría y participación en los delitos cometidos a través de los medios de comunicación de masas*, Ed. Comares 2000, p. 126 s. En sentido similar, Quintero Olivares, *Manual de Derecho Penal*, Ed. Aranzadi 2000, p. 650 s., afirma que el concepto mecánico sólo excluye los supuestos de comunicación personal, oral o escrita.

Los ámbitos de responsabilidad en los que se basa el sistema de responsabilidad en cascada son diferentes, puesto que Internet se caracteriza por la ausencia de una organización jerárquica, sistema que está en el origen del art. 30 CP. No hay que olvidar, sin embargo, que el fundamento de este precepto es, entre otras razones, evitar lagunas de punibilidad cuando el autor directo de los hechos no reside en España, cuestión que puede suscitarse en muchos casos en base a la utilización de Internet[46].

3.3. La problemática surge en relación con la posibilidad de atribuir responsabilidad penal por contenidos ilícitos ajenos, es decir, que han sido creados por un tercero. En el ámbito civil y administrativo se han desarrollado sistemas de responsabilidad a nivel europeo a partir de la Dir. 2000/31 CEE, seguida por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI). En esta ley se establecen las condiciones de responsabilidad de las diversas modalidades de intermediación: 1º) operadores de redes y proveedores de acceso (art. 14); 2º) servicios de copia temporal de datos solicitados (art. 15); 3º) servicio de alojamiento o almacenamiento de datos (art. 16); 4º) servicios de enlace a contenidos o instrumentos de búsqueda (art. 17). Con independencia del casuismo de la ley es manifiesta su finalidad de imputación de responsabilidad por actividades y contenidos ajenos. Para la atribución de responsabilidad civil o administrativa el requisito esencial es que el intermediario conozca la ilicitud del contenido y/o la posibilidad de que esos elementos sean idóneos para lesionar derechos de terceros. En el caso de que el intermediario conozca la ilicitud, para eludir la responsabilidad debe impedir el acceso de terceros a esa información. En la misma línea se desarrollan los deberes de colaboración de los prestadores de servicios con las autoridades. En el art. 11 LSSI se establece la interrupción de la prestación o retirada de los contenidos por parte de los prestadores de servicios establecidos en España. En el art. 36 LSSI se establece que los prestadores de servicios deben proporcionar esa información a las autoridades competentes y permitir el acceso al personal investigador.

3.4. Esta ley establece un ámbito de responsabilidades administrativas que puede ser utilizado, desde las diversas teorías de la competencia vigentes en el ámbito penal, para imputar responsabilidad penal cuando esa información o lesión de derechos de terceros constituyera delito. Para ello hay que diferenciar, en primer lugar, entre contenidos delictivos propios y ajenos. Conforme a la LSSI, se entienden por propios no sólo

---

46. Cfr, STS 14 julio 1993, establece que: "*En el relato histórico de la sentencia constan los elementos que para aplicar la responsabilidad que a los directores de la publicación en que se inserte el texto delictivo señala, en defecto del que realmente haya sido autor de dicho texto, el art. 15 CP. 1º que el autor del texto aunque conocido, no está domiciliado en España, lo que aquí se da, pues tal autor residía en Portugal, siendo además de nacionalidad portuguesa, y 2º el acusado era el Director del periódico " DIRECCION002 ", coordinando en cuanto tal al Subdirector y Jefes de Área y teniendo la facultad de aceptar o rechazar la publicación de cualquier artículo o publicación. Siendo de destacar que se cumple también, contra el criterio mantenido por la Sala "a quo", el requisito de no ser exigible la responsabilidad del autor material ya que, siendo nacional del país en que reside, no puede ser reclamado para responder penalmente en España, que es la condición impuesta para la sucesión de la responsabilidad en cascada por el art. 15 referido, que lo que pretende es que esa clase de hechos en los que la autoría queda limitada por el juego de los arts. 13 y 15 CP, no por ello sean sustraídos a la jurisdicción penal española cuando el delito se cometa en el territorio o en las condiciones en que tal jurisdicción tiene su ámbito de actuación. Sin que el hecho de intentarse una acción penal contra aquél en el país de su residencia pueda considerarse suficiente para excluir la concurrencia de tal condición, toda vez que se desconoce las circunstancias y resultado de dicho intento.*"

los creados directamente por los prestadores de servicios o intermediarios sino también aquéllos respecto de los que haya originado la transmisión o efectuado la selección de los datos o de los destinatarios de los mismos. No obstante, no puede pasarse por alto que, desde una perspectiva penal, en estos casos se trata realmente de una cooperación en un hecho ajeno. Sin embargo, siempre que se conozca la ilicitud puede hablarse de participación porque el delito no se ha consumado, ya que es necesaria la intervención del prestador de servicios para que esos datos puedan lesionar un bien jurídico, ya sea la intimidad, la indemnidad o la propiedad. El problema surge respecto de la posibilidad de condenar a un partícipe desconociéndose quién es el autor, debido al principio de accesoriedad limitada de la participación. Ello explica la equiparación de las conductas de facilitamiento a las de ejecución directa en diversos delitos relacionados con las nuevas tecnologías[47]. No obstante, la Parte Especial del Código Penal no puede servir para derogar los principios generales establecidos en la Parte General, en este caso, en relación con la autoría. En consecuencia, en el proceso se deberá probar que ese autor desconocido ha realizado un hecho antijurídico.

3.5. Respecto de la responsabilidad por contenidos ajenos, es decir, por incumplimiento de los deberes de vigilancia que se establecen en la LSSI, las dificultades son mayores y debe plantearse si político-criminalmente es conveniente la intervención del Derecho penal en el control de los contenidos de la Red. En principio, deberíamos partir de la inexistencia de una obligación general de control por parte del proveedor en relación con los contenidos y actividades ajenas, al menos desde la perspectiva penal. No obstante, existe también la posibilidad de establecer obligaciones penales de control de esas actividades y contenidos ilícitos. No sería algo muy diferente de la regulación generada en relación con la receptación en los artículos 301 al 303 CP, donde, entre otras conductas, se castiga a quien transmita bienes a sabiendas de que tienen su origen en un delito o realicen cualquier otro acto para ayudar a la persona que haya participado en la infracción a eludir el castigo. Si político-criminalmente se ha considerado legítimo castigar a quien actúa con posterioridad a la comisión del hecho delictivo, en mayor medida puede entenderse legítimo obligar a actuar para impedir la consumación de un delito. No obstante, existiendo la previsión de sanciones administrativas por el incumplimiento de esta labor de vigilancia, en todo caso, la intervención penal debería reservarse para conductas dolosas de los prestadores de servicios[48].

3.6. La cuestión de quién es, o quién puede ser, sujeto pasivo se suscita especialmente en la protección de datos informatizados y del *Software*. En primer lugar, respecto de la protección de la intimidad en algunas normativas europeas –Austria, Dinamarca, Islandia, Luxemburgo y Noruega– se reconoce este derecho también respecto de las personas jurídicas. Un sector doctrinal considera que de esa forma también se protegen los derechos de las personas físicas que las integran[49]. La cuestión es compleja en atención a la tendencia a equiparar a todos los efectos la persona física

---

47. Vid. Supra, 2.

48. En otro sentido, Mata y Martín, "Criminalidad informática…, cit., p. 230, propone que también pudiera castigarse el incumplimiento imprudente del deber de vigilancia por parte del prestador de servicios.

49. Cfr. Lucas Murillo de la Cueva, *Informática y protección de datos personales,* CEC, Madrid 1993, p. 49 s.

a la jurídica. Ello, no obstante, y partiendo de que se protege la intimidad como derecho subjetivo, entiendo que sujeto pasivo puede serlo exclusivamente la persona física. Cuestión distinta es que se protejan determinados datos de la persona jurídica, en cuanto tengan un valor económico, tal y como sucede en el art. 278 CP.

3.7. En la estafa informática también se suscita el problema de quién es realmente el sujeto pasivo, puesto que en algunas estafas quién sea el perjudicado depende de situaciones contractuales de aseguramiento. La llamada estafa triangular en la que la persona engañada es diferente de la perjudicada ha existido siempre. Esta situación es, sin embargo, la común en la estafa informática puesto que al producirse la disposición patrimonial como consecuencia de una manipulación informática la determinación de quién es el perjudicado dependerá de las relaciones contractuales entre la terminal informática manipulada, los titulares de la empresa que gestiona el patrimonio y el titular de ese patrimonio. En la STS 1472/2004, de 21 de diciembre, se plantea un supuesto de estafa informática. El acusado Jesús, recurrió la sentencia de la Audiencia Provincial de Las Palmas, porque no había aplicado la excusa absolutoria de parentesco, cuando era el hijo de la titular de la cuenta corriente de la que se retiraron 30.000 euros, a través de la manipulación de una terminal propiedad del BBV, vinculado a esa cuenta corriente. Terminal que se encontraba en la empresa de la que eran propietarios los padres. En la sentencia del Tribunal Supremo se afirma que el art. 268 CP no es aplicable porque la acción no se dirigió contra el patrimonio de los padres del recurrente, sino que fue realizada empleando instrumentos informáticos que se encontraban en el ámbito de dominio de éstos y que permitían efectuar disposiciones sobre el patrimonio del mismo. En la sentencia se afirma que lo importante es saber quién fue el sujeto pasivo de la estafa informática, pues sólo el perjudicado puede ser sujeto pasivo, conforme al art. 268 CP[50].

3.8. La atribución de responsabilidad no es fácil, en algunos casos, como consecuencia de la concreta relación vendedor-propietario-cliente, derivada de la especial naturaleza de los contratos de servicios informáticos y de las empresas de Software. Esta situación contractual dificulta la calificación del sujeto que realiza materialmente la conducta como autor en sentido penal[51]. En relación con el Software el problema de fondo es determinar quién tiene la titularidad de los derechos sobre el Software, así como qué derechos adquiere quien lo compra. En España se ha optado por la

---

50. En este sentido, STS 1472/2004, establece que: "*Como es sabido en el delito de estafa tanto es el sujeto pasivo del delito el sujeto que obra por un error al que ha sido inducido mediante engaño y realizó la disposición patrimonial, como el que sufre el daño patrimonial, que puede ser un sujeto distinto del que realizó la disposición patrimonial. El tipo penal del art. 248.2 CP tiene la función de cubrir un ámbito al que no alcanzaba la definición de la estafa clásica. La nueva figura tiene la finalidad de proteger el patrimonio contra acciones que no responde al esquema típico del art. 248.1 CP, pues no se dirigen contra un sujeto que pueda ser inducido a error. En efecto, los aparatos electrónicos no tienen errores como los exigidos por el tipo tradicional de la estafa, es decir, en el sentido de una representación falsa de la realidad. El aparato se comporta según el programa que lo gobierna y, en principio, sin error. De manera que el sujeto pasivo sólo puede ser el titular del patrimonio perjudicado. En el presente caso, no cabe duda que el perjudicado ha sido el Banco y, por lo tanto, es el sujeto pasivo del delito*".

51. En particular, respecto de los delitos de daños -sabotaje informático-, por la determinación de a quién pertenece la titularidad de la propiedad sobre el programa o los datos destruidos y, por otro lado, respecto de aquellos supuestos en los que el vendedor o el propietario del programa utilizan el sabotaje como medida coactiva para realizar determinados derechos que sustentan sobre el programa.

protección de los derechos sobre el Software a través de la propiedad intelectual, equiparándolos a las obras literarias (art. 1 Ley 16/1993, 23 diciembre, de Propiedad Intelectual). En el art. 270. 1. CP se incluyen tanto los derechos morales del autor como los de explotación. Ello suscita la cuestión de que estos programas se llevan a efecto, generalmente, en el seno de empresas, por personas que trabajan en ellas como informáticos. ¿Quién ostenta el derecho, la empresa o el autor? En otros casos el problema surge por la necesidad de acudir a estructuras de autoría mediata para poder atribuir la responsabilidad a un sujeto; e incluso, en ocasiones, se plantea la duda sobre la propia existencia de un autor, en sentido estricto, así, por ejemplo, cuando la alteración de datos es consecuencia de una orden del propio ordenador.

3.9. El tratamiento de los supuestos en los que la destrucción se realiza por el titular del programa, en ejercicio de un presunto derecho sobre el propio programa destruido debe encontrar una respuesta acorde con criterios de política-criminal. Ello no únicamente respecto del ámbito de la informática, sino de carácter general sobre la conveniencia o no de la creación de un tipo específico de realización arbitraria del derecho propio, que no quede cubierto por el actual art. 337 CP. Aun cuando si, en el ámbito del delito de realización arbitraria del propio derecho, se utilizara el concepto de violencia que la jurisprudencia aplica en las coacciones no existiría ningún problema para condenar conforme a este precepto.

3.10. Respecto del sujeto pasivo, en relación con la pornografía, se suscitan problemas respecto de la forma de impedir el acceso a menores. En particular, en el supuesto del art. 186 CP, de facilitar material pornográfico a menores, máxime cuando se trata de prestadores de servicios. La solución se ha buscado a través de la exigencia de que esos contenidos no sean de libre acceso. En el fondo la misma solución adoptada respecto de las revistas y otros materiales pornográficos, aun cuando los medios previstos deban ser diferentes. Respecto de la corrupción de menores se plantea la cuestión del límite de edad, al que me refería supra, puesto que está fijado en los 18 años. ¿Está justificado que se limite en mayor medida la intervención en la producción de material pornográfico que en los abusos sexuales?

4. EL TIPO SUBJETIVO EN ESTOS DELITOS

4.1. En principio, los problemas que suscitan las diferentes modalidades delictivas cometidas a través de la informática, en relación con el tipo subjetivo son mínimas. Muchos de los problemas surgen de la confusión entre móvil y dolo, algo que no es característico de estos delitos sino que se trata de una confusión bastante generalizada en nuestra doctrina y jurisprudencia. Los problemas se originan en aquellas modalidades delictivas en las que *ex ante* se desconoce el efectivo alcance que tendrá la conducta. Aun cuando no se exija que el sujeto conozca y quiera el resultado lesivo, para que una conducta pueda calificarse como dolosa el autor debe conocer el efectivo y exacto peligro que ésta supone. Sólo los resultados que sean realización de este peligro conocido por el sujeto pueden ser imputados a la conducta. Nos encontramos, por tanto, frente a supuestos que deberíamos calificar como *dolus generalis*. En relación con la pornografía la cuestión se complica porque incluso cuando el material pornográfico sea de acceso previo pago, no puede excluirse que los menores accedan puesto que son los que mayor habilidad han desarrollado para acceder a páginas de pago, codificadas, protegidas…

4.2. En relación con el dolo del sujeto activo, en la corrupción de menores, sobre todo desde el momento en que se castiga no sólo la producción de material pornográfico con menores, sino también la difusión e incluso la tenencia, se planteará en muchos casos el problema del conocimiento de esa minoría de edad. El desconocimiento de la minoría de edad que, no olvidemos, está fijada legalmente en los 18 años, excluye el dolo y, en consecuencia la tipicidad.

4.3. En otros casos, la cuestión es relativamente más compleja porque puede tratarse de dolo sobrevenido, cuando se accede casualmente a información que afecta a la intimidad o a la indemnidad sexual. Entiendo que en esos casos no puede hablarse de dolo respecto del acceso, por lo que el descubrimiento del secreto o de la pornografía serán atípicos. Sin embargo, la posterior revelación, en el caso de los secretos, si sería típica como delito de revelación de secretos. En el caso de la pornografía infantil, al castigarse la tenencia para uso propio, en cuanto el sujeto advierta que se trata de material pornográfico con menores y no lo destruya concurrirá dolo.

4.4. También es problemático el tipo subjetivo en el supuesto de los intermediarios que no impiden el acceso de terceros a información de esa naturaleza o que pueda lesionar sus intereses económicos. Como veíamos, precisamente en este punto la dificultad de probar la existencia de dolo, junto a la peligrosidad de las conductas negligentes en el cumplimiento del deber de vigilancia, ha llevado a que se proponga el castigo de la comisión imprudente.

4.5. Relacionado con el conocimiento y con el error, aun cuando en el ámbito de la culpabilidad se pueden suscitar errores de prohibición. Ello es así porque determinadas actividades pueden ser lícitas en unos países y en otros no. ¿Se puede exigir a los intermediarios y prestadores de servicios conocer la legislación de los países a donde pueden transmitirse esos datos?[52].

5. ACTOS PREPARATORIOS, TENTATIVA Y CONSUMACIÓN

5.1. La especificidad de las conductas en las que se utilizan sistemas informáticos plantea graves dificultades en algunos de estos delitos. Así mismo, en este ámbito surge una política criminal extensiva en la que se castigan actos preparatorios, en unos casos, y de cooperación, posteriores al inicio de la ejecución, en otros, que dificultan la aplicación de los esquemas clásicos. Así, por ejemplo, la conducta de prestadores de servicios que transmiten datos o definen destinatarios se trata de un supuesto de participación posterior a la creación de los datos pero que se produce con anterioridad a la consumación y, en muchos casos, sin connivencia con el autor. Ello es así porque la consumación requerirá, en unos casos, el acceso a los datos –datos personales o pornografía– y, en otros, que el engaño produzca un error en el destinatario y éste realice la disposición patrimonial, y el envío a los destinatarios, e incluso la selección de éstos, depende de los prestadores de servicios.

---

52. Morales García, "Criterios de atribución de responsabilidad a los prestadores de servicios e intermediarios de la sociedad de la información", en *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet* (Morales Prats/Morales García coords.), Ed. Aranzadi 2002, p. 208 s.

5.2. En el sabotaje informático, el problema se plantea especialmente en aquéllos casos en los que media un lapso de tiempo entre una conducta, en sí misma sin eficacia lesiva, y otra, que provoca directamente los resultados lesivos, pero únicamente, en tanto en cuanto existía esa conducta previa. En los supuestos en los que, para que se inicie la destrucción de los datos o programas, ha de pasar únicamente un lapso de tiempo se suscitan ambos problemas: inicio de la ejecución y momento de la consumación.

5.3. Otra cuestión a considerar se suscita en aquellos casos en los que se introduce una página web o se mandan correos electrónicos destinados a engañar a los destinatarios de forma que realicen una disposición patrimonial que les va a producir un perjuicio económico. El problema estriba en que dada la naturaleza intersubjetiva del engaño en la estafa, no puede afirmarse que el engaño sea idóneo *ex ante* para provocar el error[53]. Por consiguiente, no puede calificarse como tentativa de estafa múltiple estas conductas puesto que sólo en algunos casos es posible ya *ex ante* la consumación.

5.4. Sobre la introducción de nuevos tipos que pueden calificarse de actos preparatorios, como sucede con el art. 270.3º CP, se plantea una cuestión de legitimidad, en la que aparte de la consideración estrictamente penal, debe tomarse en consideración que se trata de conductas protegidas civil y administrativamente. El problema no es tanto el que estemos frente a delitos de peligro abstracto[54] sino sobre la necesidad y merecimiento de pena de estas conductas. Algunos conciben estas conductas como tentativa respecto de la reproducción ilícita o plagio de un programa. Sin embargo, entiendo que en este caso, para poder hablar de tentativa se suscitan dos problemas: 1º) No necesariamente se dará la inmediatez temporal que requiere la tentativa; 2ª) Será regla, casi general, que los autores de estos actos preparatorios sean diferentes de aquellos que copien o plagien el programa. En todo, es necesaria una interpretación restrictiva del tipo ya que, conforme a la legislación extra-penal, las conductas no serán típicas cuando se trate de dispositivos utilizados para realizar copias de seguridad y privadas. Por consiguiente, el tipo concurre cuando la conducta consista en la fabricación, puesta en circulación o tenencia de medios que sólo sirvan para la neutralización o supresión de dispositivos técnicos de protección de sistemas informáticos[55].

6. IMPUTACIÓN DEL RESULTADO. PROBLEMÁTICA CONCURSAL. PARTICULAR ATENCIÓN A LA FIGURA DEL DELITO CONTINUADO

6.1. La imputación del resultado suscita problemas cuando *ex ante* el sujeto desconoce el riesgo exacto que está creando con su conducta y, a sensu contrario, cuando el sujeto cree conocer el riesgo pero éste excede con mucho a lo previsto. Si se parte de que sólo se pueden imputar los resultados que son realización del riesgo típico, en

---

53. Cfr. GALLEGO SOLER, *Responsabilidad penal y perjuicio patrimonial*, Ed. Tirant lo Blanch 2002, sobre la necesidad de engaño bastante, atendiendo a los deberes de autoprotección de la víctima.

54. GÓMEZ MARTÍN, RECPC 04-16 (2002), considera que este precepto es de peligro abstracto porque en este delito se protege la propiedad intelectual que es un bien jurídico individual. Siendo cierto este punto de partida, entiendo que al tratarse de un adelantamiento de las barreras de protección, puede afirmarse que se trata de un delito de peligro abstracto y además en el sentido clásico de delito de peligro concebido como "adelantamiento de la barrera de protección", no como protección de un bien jurídico supraindividual.

55. En este sentido, GÓMEZ MARTÍN, RECPC 04-16 (2002).

este caso doloso, creado por el autor, no serán imputables los resultados no previstos, desde los conocimientos del autor, ni aquellos que sean consecuencia de la complejidad de los sistemas informáticos o de la ejecución incorrecta de la distribución o producción por parte del autor. Así, por ejemplo, si una persona envía pornografía infantil a otro y se equivoca de destinatario se suscita un error *in persona* que, en principio, es irrelevante por lo que, consecuentemente, podría imputarse el resultado. Por el contrario, si la pornografía llega a más de una persona, por un envío incorrecto, estaríamos frente a un delito consumado pero no podría imputarse la existencia de un concurso de delitos o de un delito continuado, sino de un único delito. Ello es así porque, aun cuando la conducta del sujeto pudiera ser calificada de imprudente, sólo está previsto el castigo de la comisión dolosa, tanto en los delitos de descubrimiento y revelación de secretos como en la estafa o en la pornografía infantil. Dificultades de imputación de los resultados se suscitan también cuando son los prestadores de servicios quienes determinan a qué personas se envían esos datos e incluso qué datos se envían.

6.2. Otro problema propio de la criminalidad informática surge cuando, como consecuencia de un único comportamiento, los resultados lesivos se van reproduciendo por sí mismos. Esta cuestión se suscita tanto en el ámbito, por ejemplo, de las estafas realizadas a través de manipulaciones informáticas, como en los sabotajes informáticos o en la distribución de pornografía infantil. En las estafas una orden puede implicar perjuicio para múltiples personas, por ejemplo, si se ordena retirar 0,5 euros de todas las cuentas corrientes de un banco. En el sabotaje la introducción de un programa destructivo puede afectar a múltiples programas, en muchas ocasiones de forma indiscriminada e incalculable, incluso para el propio sujeto. En la pornografía la situación es similar puesto que una vez "colgado" el material en la red la posibilidad de acceso, ya sea previo pago o libre, se materializa a través de Internet, a nivel global.

6.3. La multiplicidad de resultados lesivos imputables a una única conducta plantea la cuestión concursal. Es necesario delimitar cuándo nos encontramos frente a un concurso ideal o real de delitos o, en su caso, frente a un delito continuado. Parece claro que en aquellos delitos que afectan al patrimonio, en sus distintas versiones, estafas, sabotaje informático…, lo adecuado sea aplicar la figura del delito continuado. Ello incluido los delitos contra la propiedad intelectual, incluso admitiendo que también se protegen derechos morales. Por el contrario, en los delitos contra la intimidad, en principio, no cabe la aplicación del delito continuado, puesto que no se trata de un bien jurídico personal que no se contempla en la excepción prevista en el art. 74.3 CP. No obstante, se podría plantear la analogía entre la excepción prevista para los delitos contra el honor respecto de los delitos contra la intimidad. En los delitos relativos a la pornografía infantil y la corrupción de menores cabe la figura del delito continuado, como excepción del art. 74.3 CP. Aplicación que, por otra parte, es jurisprudencia mayoritaria en el ámbito de los delitos contra la libertad sexual en los que las víctimas son menores[56], con independencia de lo criticable que pueda ser este criterio.

---

56. Ejemplo, de esta jurisprudencia, entre muchas otras, STS 988/2006, 10 octubre, califica los abusos sexuales sufridos por menores durante años como delito continuado, cuando, independientemente de que no se pueda determinar el número sí se ha probado que fueron muchas más de tres veces respecto de cada uno de los menores.

7. LUGAR DE COMISIÓN Y COMPETENCIA JURISDICCIONAL

7.1. El lugar de comisión de hechos ilícitos cometidos a través de la informática suscita problemas similares a los relativos al momento de comisión del delito y la delimitación entre los concursos de leyes y de delitos. Para la criminalidad informática, especialmente si se comete a través de Internet, la legislación penal concebida tradicionalmente como cuerpo legislativo vigente para un determinado territorio no es válida[57]. No obstante, es cierto que el problema no es exclusivo de la criminalidad informática sino que es una de las consecuencias de la criminalidad transnacional. Aunque finalmente ésta también es posible por la utilización de las nuevas tecnologías. Al respecto hay dos soluciones, que pueden ser concurrentes: a) armonización de las legislaciones y facilitamiento de los mecanismos de cooperación internacional[58]; b) establecer cláusulas de extraterritorialidad, tal y como ya existen en materia de terrorismo, genocidio, tráfico de personas… En el supuesto de la criminalidad informática, en el Código Penal se ha previsto la extraterritorialidad en la corrupción de menores, art. 189 1. b), donde se castiga: "la *producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hubiesen sido utilizados menores de edad o incapaces, o lo poseyere para estos fines,* ***aunque el material tuviere su origen en el extranjero*** *o fuere desconocido."*

7.2. No obstante, la solución puede buscarse también a través de determinar en qué lugar se entiende cometido el delito. En general, en los delitos informáticos, la conducta de creación de los datos o/y de su transmisión… se produce en un país y los resultados en otros muy diversos. Respecto del lugar donde se entiende cometido el delito existen tres construcciones jurídicas que posibilitan la solución de este problema. Son las teorías de la acción, del resultado y de la ubicuidad. Es precisamente esta última la que se ha impuesto, tanto en derecho comparado como en nuestra doctrina y jurisprudencia[59]. De acuerdo con la teoría de la ubicuidad el delito se entiende cometido tanto en el lugar donde se produce el resultado como donde se lleva a efecto la conducta. Ello no excluye la cuestión de la competencia porque, de acuerdo con la teoría de ubicuidad, todos los Estados en los que se ha realizado la conducta y/o producido los resultados tendrían competencia. La solución a esta cuestión de competencia debería solventarse a través del principio de personalidad. Es decir, de entre todos los Estados en principio competentes, sería competente aquel del que sea nacional el autor. En el ámbito de la delincuencia informática puede adquirir una especial relevancia este principio, conforme al cual el Estado de origen del sujeto también tiene competencia para juzgar los hechos cometidos en otro Estado, aunque en él no se haya realizado la conducta ni producido los resultados. Esta solución resulta conflictiva, sin embargo, en los supuestos de coautoría de personas nacionales de diversos Estados y cuando la conducta no es ilícita o tiene una natura-

---

57. En este sentido, SEMINARA, S., "La piratería su Internet e il diritto penale", *Revista Trimestrale di Diritto penale dell'econoia*, nº 1-2, 1997, p. 111.

58. En este sentido, Convenio de Cibercrimen, Budapest 23 noviembre 2001 (firmado por 30 países, no cuenta con el número suficiente de ratificaciones para entrar en vigor), tiene como finalidad armonizar las legislaciones y facilitar su persecución.

59. En concreto, en relación con Internet, adoptan esta postura, RODRÍGUEZ MOURULLO/ALONSO GALLO/ LASCURAIN SÁNCHEZ, "Derecho penal e Internet", *Régimen jurídico de Internet*, La Ley 2002, p. 265.

leza diferente en uno y otro. A ello se suman los problemas derivados de la existencia o no de Tratados de extradición, del contenido de esos Tratados y de la reticencia generalizada, por parte de todos los Estados, de entregar a sus nacionales para que sean juzgados en otro Estado.

7.3. Así mismo, en el ámbito de la delincuencia informática realizada a través de Internet, subsiste la cuestión de si también tiene competencia jurisdiccional el Estado donde se han producido conductas que debemos calificar de cooperación, como son las de los prestadores de servicios que transmiten datos o seleccionan datos y/o destinatarios. El problema surge desde el momento en que la teoría de la ubicuidad supone una extensión del principio de territorialidad de la ley penal que para algunos plantea problemas político-criminales e incluso jurídico-constitucionales[60]. En todo caso, es evidente que de la intervención de diversos Estados en relación con un mismo hecho delictivo pueden surgir conflictos jurisdiccionales de carácter internacional por lo que cada vez son más necesarios los Tratados de Cooperación jurisdiccional tanto en el ámbito de la Unión Europea[61] como a nivel mundial. No hay que olvidar que junto al principio de territorialidad, rigen los principios de universalidad, de protección de intereses del Estado y de personalidad.

7.4. Por lo demás, se seguirá planteando el problema de las diferencias de tratamiento legislativo de estas conductas. Especialmente en relación con los intermediarios y proveedores de Internet, sus funciones y servicios pueden tener repercusión en cualquier lugar del mundo. Su actuación e incluso el contenido de esos datos serán ilícitos en unos países y en otros no. O, en todo caso, es seguro que en unos tendrán un significado diferente que en otros, tanto en relación con el contenido de la conducta típica como sobre todo de la pena.

---

60. Anarte Borrallo, "Incidencias de las nuevas tecnologías en el sistema penal…", op.cit., p. 213 s.; Climent Barbera, "La Justicia penal en Internet. Territorialidad y competencias penales", en *Internet y Derecho Penal*, CDJ X, Madrid 2001, p. 262 s.

61. En este sentido, tiene una gran importancia, en cuanto avance en la cooperación internacional, la Ley 3/2003, 14 de marzo, de **Orden de Detención Europea**, que permite reclamar directamente por el juez español competente emitiendo una orden de detención europea dirigida al juez competente del país donde se encuentre el sujeto.