EL LLAMADO «DELITO INFORMÁTICO»*

María Eugenia González de Chaves Calamita**
Universidad de La Laguna

RESUMEN

Aunque no existe en el mundo del Derecho español e internacional un concepto claro de lo que es el delito informático, varios autores han abordado con desigualdad de criterios los abusos en «la red» y sus repercusiones civiles y penales. Este estudio concluye que no sólo son necesarias medidas de carácter civil y penal para proteger los bienes jurídicos de los afectados por dichos abusos, sino también otras extrajudiciales, debido sobre todo al carácter transfronterizo de los delitos.

PALABRAS CLAVE: internet, delito informático.

ABSTRACT

Although there is not a clear concept of informatic crime offence in the Spanish and international law, some authors have tackled with unequal viewpoints the abuse within the «net» and their civil and criminal repercussions. This research concludes that not only civil and criminal steps need to be taken in order to protect the juridical goods of affected people but also extrajudicial steps, due to the cross-border's condition of the offence.

KEY WORD: internet, informatic crime offence.

1. INTRODUCCIÓN

A pesar de que no existe un concepto de delito informático que las disposiciones legales hayan acogido, y ni tan siquiera una referencia en el texto de la ley de esa expresión, no son pocas las referencias que en la doctrina, en la jurisprudencia, y en el lenguaje usual se hacen a la categoría «delito informático». En efecto ello podría hacernos pensar en su incorrección en la medida en que como tal carece de tipificación en la legislación penal[1].

De este modo, no existe delito si no hay una ley que lo cree. El Código Penal (art. 10) dispone que «Son delitos o faltas las acciones y omisiones dolosas o imprudentes penadas por la ley». Y entonces lo lógico sería afirmar que, como tal, no existe el delito informático en tanto que no está tipificado en el Código Penal, ni se encuentra en ningún otro sitio del ordenamiento que lo pudiera encuadrar como legislación penal especial. Aunque no hay que despreciar que la categorización de

un grupo de delitos que admitan esa identificación sería útil para poder realizar un estudio serio de los mismos[2].

A ello obedece el reiterado intento de procurar una definición general de delito informático.

De este modo, Davara Rodríguez[3], que cree necesario acudir a la referida denominación de delito informático para poder realizar su estudio, lo define como: «la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático o vulnerando los derechos del titular de un elemento informático ya sea el hardware o el software».

Por otra parte, Rovira del Canto[4] afirma que hoy no sólo puede hablarse de la existencia de meros *abusos informáticos*, derivados del uso y utilización de los sistemas informáticos y de telecomunicaciones, sino también de *comportamientos ilícitos informáticos*, esta vez derivados de la propia sociedad global del riesgo informático y de la información. Y que, en cuanto adquieren la suficiente entidad y gravedad como para constituir ataques serios a intereses jurídicamente protegidos y protegibles, tradicionales y nuevos (que deben ser contrarrestados con medidas que superen los meros ámbitos de la autorregulación, del Derecho Administrativo y del Derecho Civil, requiriendo la intervención del Derecho Penal), se constituyen en lo que podemos denominar delitos informáticos.

En este sentido, Rovira del Canto[5] nos muestra las principales características de lo que él llama «delito del riesgo informático y de la información» y su estudio lo lleva a las siguientes conclusiones:

1. La permanencia del hecho basada en la repetición de la actuación lleva a considerar al delito informático como delito continuado.
2. El automatismo y el distanciamiento temporal entre la acción y los efectos derivados de ésta llevan a la configuración del delito informático como delito de consumación instantánea y efectos permanentes.
3. La extensa y elevada lesividad del conjunto de acciones ilícitas trae consigo que la cuantía del perjuicio debe afectar a la configuración de subtipos agrava-

---

* Este trabajo obtuvo el Premio de Estudios Jurídicos «Felipe González Vicén» en enero de 2004.

** Becaria de colaboración del área de Derecho Penal de la Facultad de Derecho de la Universidad de La Laguna. Curso 2003-2004.

[1] V. así Davara Rodríguez, M.A. *Manual de Derecho informático*, p. 335.

[2] Sin embargo, si nos fijamos en países de nuestro entorno socio-cultural veremos cómo hace tiempo que el delito informático está tipificado y, en consecuencia, se incluye ahora en diversos códigos y normas de cada ordenamiento. Esto ha ocurrido, por ejemplo, en Alemania, Gran Bretaña, Suecia, Canadá, varios estados de EEUU, Australia y Francia.

[3] Davara Rodríguez, M.A. *Derecho informático*, pp. 318-319.

[4] Rovira del Canto, E. *Delicuencia informática y fraudes informáticos*, p. 68.

[5] Rovira del Canto, E. *Ob. cit.*, pp. 116-117.

dos o cualificados, y su análisis debe derivarse al ámbito de las responsabilidades civiles.

4. Las dificultades de averiguación y comprobación delictual no pueden solventarse directamente con medidas penales, sino primordialmente con medidas extrajurídicas y, en todo caso, procesales; suponen a la vez un mayor favorecimiento del delincuente. Aun así, parte de ellas pueden solventarse con su previsión legal penal específica y la creación de tipos delictivos amplios, utilizando conceptos jurídicos indeterminados y leyes penales en blanco y elaborados con criterios uniformes a nivel supranacional.
5. La frecuencia y la creciente diversidad de los comportamientos ilícitos informáticos suponen una mayor peligrosidad del conjunto de esta categoría delictual, y traen consigo la necesidad, para una adecuada respuesta penal, de la configuración de modalidades delictuales.
6. La posibilidad de distanciamiento temporal, en conjunción con las tres primeras características criminológicas indicadas, da lugar a una frecuente imposibilidad material de determinar con exactitud el concreto momento de la consumación delictual efectiva.
7. El distanciamiento espacial, la mayor movilidad y el carácter transfonterizo dan lugar a la necesidad de tipificaciones globales unificadas a nivel internacional.
8. El actual sujeto activo puede serlo cualquiera: delincuentes habituales, jóvenes, estudiantes u otros sin conocimientos cualificados, organizaciones criminales, incluso agencias gubernamentales. Con respecto al sujeto pasivo, se ha producido una inicial extensión de la conceptuación del potencial sujeto pasivo, y ahora comprende, no sólo a los titulares y demás beneficiarios legítimos de un sistema informático, como los usuarios y terceros de buena fe, sino incluso a cualquier *persona física o jurídica* que en cualquier momento, ocasión o circunstancia tenga o se encuentre vinculada directa o indirectamente con un sistema informático, la información en él contenida, o los datos que la representan.
9. El móvil último del autor de un delito informático es normalmente un ánimo de lucro genérico, aunque puede concurrir con otros de forma simultánea o posterior.

2. «LOS DELITOS INFORMÁTICOS» EN EL ORDENAMIENTO JURÍDICO

En el Código Penal de 1995, no existe una rúbrica que se titule «De los delitos informáticos», aunque podemos encontrar en él alusiones, en algunos tipos penales, a los delitos que se cometen a través de la informática. De este modo, tal y como afirma Orts Berenguer[6], en nuestro Derecho la informática constituye un me-

[6] Orts Berenguer, E. y Roig Torres, M. *Delitos informáticos y Delitos comunes cometidos a través de la informática*, pp. 13 y 14.

dio comisivo a través del cual pueden lesionarse distintos bienes jurídicos, tales como el patrimonio, la propiedad industrial e intelectual, la intimidad y otros intereses también tutelados. No obstante, en algunas infracciones el objeto material lo integran los propios sistemas o soportes informáticos, como ocurre con alguna modalidad específica del delito de daños o con los relativos a la propiedad intelectual en los que ésta recae sobre un programa de ordenador. Probablemente, por esta heterogeneidad de bienes, las infracciones relacionadas con la informática no están reguladas en un único epígrafe sino que se hallan dispersas a lo largo del articulado del Código. De este modo será la interpretación de cada uno de los tipos la que nos permitirá concluir si estamos o no ante una conducta punible, incardinable en la citada categoría de «delitos informáticos», para cuyo estudio se encuentran la dificultad consustancial a la dispersión normativa y otras de carácter pragmático derivadas, sobre todo, de la complejidad tecnológica que encierra en estos casos el instrumento del delito.

Además, señala Orts Berenguer que los avances de la técnica hacen muy difícil no sólo el descubrimiento de estas infracciones y la identificación de su autor, sino también la previsión acorde con el principio de seguridad jurídica de todas las posibles modalidades comisivas, en continua expansión debido a la celeridad con la que se suceden las innovaciones en este campo. Por tanto, las exigencias de taxatividad llevan al legislador a perfilar las posibles conductas delictivas con un mínimo de precisión. También se debe tener en cuenta que en las normas así elaboradas suelen utilizarse conceptos normativos, para cuya concreción resulta necesario acudir a la legislación civil y administrativa.

Otro problema fundamental que podemos encontrar en este sentido, tal y como señala Pica[7], es el que hace referencia al bien jurídico protegido. Este autor afirma que la tentativa de delinear un bien jurídico unitario, que abrace la entera materia informática, está inevitablemente destinada al fracaso porque estos hechos no representan un nuevo objeto de tutela, sino un nuevo modo de agresión y de comisión de actividades ilícitas que atienden a bienes jurídicos ya reconocidos y tutelados.

Si bien, tal y como señala Orts Berenguer[8], se aprecia en el conjunto de delitos informáticos una unidad criminológica y hasta político-criminal, no parece acertado, sin embargo, reconducirlos a un proceso unitario, homogéneo, desde el punto de vista dogmático. La amplísima gama de comportamientos punibles relacionados con los ordenadores y el papel muy diverso que pueden representar en estos hechos los elementos de los sistemas informáticos, hacen ciertamente complejo establecer un nexo común que haga presente un nuevo interés jurídico-penalmente relevante que quepa entender introducido en la legislación penal. Todavía más: los bienes jurídicos propuestos unitariamente para el conjunto de los delitos en los que aparecen los diversos elementos de los sistemas informáticos carecen de

---

[7] Pica, G. *Diritto penale delle technologie informatiche*, p. 34 y ss.

[8] Orts Berenguer, E. *Delitos informáticos y Delitos comunes cometidos a través de la informática*, p. 33 y ss.

una mínima precisión que posibilite cumplir con las funciones encomendadas al bien jurídico en el seno de la teoría jurídica del delito.

En definitiva, y según este autor, todo lo anterior muestra cómo esta reciente fenomenología delictiva no tiene la consecuencia de aportar ningún nuevo bien jurídico penalmente relevante. Tampoco está presente ningún otro aspecto o criterio que permita una incriminación conjunta de estos hechos. Entonces, si bien no es posible hablar de «delito informático», *sensu stricto*, sí parece adecuado denominar «delincuencia informática» o «criminalidad informática» a este conjunto de hechos con relevancia penal aunque desde distintos ángulos.

Por lo tanto, las únicas respuestas que proporciona nuestro ordenamiento jurídico, para los delitos que se cometen a través de la informática, son las reguladas en el Código Penal: la estafa informática (art. 248.2 CP); el supuesto específico de daños informáticos (art. 264.2); hechos relativos a la propiedad intelectual sobre obras en soporte informático (art. 270); descubrimiento, modificación o revelación de secretos personales y familiares (art. 197); uso indebido de terminales de telecomunicación (art. 256); fabricación o tenencia de programas o aparatos destinados a la falsificación (art. 400) e interceptación de las telecomunicaciones y su divulgación por autoridad o funcionario público (art. 536).

Por ello, parece absolutamente imprescindible estudiar cuáles serían las conductas punibles en relación a la informática, pero antes se especificará qué se entiende por delito informático.

3. PRECISIÓN DEL CONCEPTO DE DELITO INFORMÁTICO

Con la expresión «delitos informáticos» suele aludirse a las conductas que atentan de forma grave contra determinados bienes del individuo (pero también de personas jurídicas) que presentan una configuración específica y exclusiva de la actividad informática y telemática y han sido sometidos a una «tipología» técnico-criminológica: acceso, alteración, ocultación o destrucción no autorizados de los datos almacenados en un sistema informático; reproducción completa o parcial de datos contenidos en un sistema informático; creación de un fichero clandestino... En estos casos, el ordenador, sus elementos o los sistemas de telecomunicación al servicio de éstos son el objeto del delito.

En este sentido, el profesor Romeo Casabona[9] establece que hay que identificar los bienes jurídicos más significativos y vulnerables en relación con los medios informáticos, así como las formas de agresión que pueden experimentar. De este modo, señala dicho autor que los hechos que se realizan a través de los medios informáticos, siendo éstos el simple medio de expresión o de comisión inespecífico (por ejemplo, la difusión de pornografía, especialmente infantil y la provocación a

[9] Romeo Casabona, C.M. *Enciclopedia Penal Básica*, p. 518.

la discriminación por motivos racistas, a través de las redes telemáticas como Internet) no plantean ningún problema diferencial de tipicidad, si el hecho ya es previamente punible.

Por tanto, no podemos partir de la configuración del delito informático únicamente sobre el bien o interés jurídico tradicional afectado, olvidando los nuevos intereses surgidos de los retos de la sociedad actual y, por su importancia, entidad y afectación social global, merecedores también de protección.

Además, el concepto de delito informático debe venir presidido por su consideración de *pluriofensivo,* teniendo siempre concurrente la protección de los nuevos intereses derivados de la sociedad global del riesgo informático. Esos intereses deben conjugarse, además, con la protección de bienes jurídicos tradicionales, bien individuales bien colectivos. Con ello, quedan al margen de tal conceptuación aquellos supuestos delictivos en los que, viéndose afectados elementos informáticos, no presenten ninguna de las características propias del delito informático en lo que se refiere a las funciones automáticas de almacenamiento, tratamiento, transferencia y transmisión de la información.

El concepto de delito informático, por tanto, no debe venir referido a la realización de una conducta ilícita a través de elementos o medios informáticos, o meramente que éstos sean objeto de tal comportamiento delictivo, sino que debe constituirse en torno a la afectación de la información como bien jurídico protegido, primordial y básico, que no exclusivo. Por tanto, se deberá tener presente si resultan afectados otros bienes jurídicos, normalmente tradicionales[10].

4. CONDUCTAS PUNIBLES

En el Código Penal los delitos están ordenados en relación con el bien jurídico al que protegen. Es difícil encontrar un bien jurídico que englobe a la totalidad de los llamados «delitos informáticos», porque éstos se encuentran dispersos a lo largo de todo el Código Penal.

De este modo, en función del bien jurídico protegido, encontramos los siguientes delitos:

A. Delitos contra el patrimonio

1. *Estafas cometidas por medios informáticos*

El segundo apartado del art. 248 CP fue introducido por el legislador de 1995 con el fin de colmar la laguna punitiva existente en aquellos casos en que la

[10] Rovira del Canto, E. *Ob. cit.*, p. 71.

privación ilegítima de activos patrimoniales se realizaba a través de artificios informáticos haciendo difícil su incardinación en los tipos tradicionales al faltar el engaño y el error esenciales en el delito de estafa y resultar forzada también la equiparación de esas manipulaciones técnicas con el apoderamiento propio del hurto[11].

Art. 248 CP: «Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. 2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero». Además, a esto tenemos que añadir que éste ha sido el único artículo que se ha modificado con la reciente reforma del CP y se le ha añadido un apartado: «3. La misma pena se aplicará a los que fabriquen, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo».

Este nuevo precepto recoge la estafa cometida a través de cualquier manipulación informática o artificio semejante, y declara la tipicidad de todas aquellas conductas que mediante estos artilugios, con ánimo de lucro y en perjuicio de tercero, logren la transferencia no consentida de activos patrimoniales. Según Orts Berenguer[12], el engaño y el error son reemplazados por el uso de cualquier ardid informático, si bien no se mencionan las concretas maniobras fraudulentas, por lo que el legislador recurre a una cláusula genérica en la que queda comprendida toda manipulación informática.

El ánimo de lucro requerido en el tipo encarna un elemento subjetivo de lo injusto que puede definirse en general como «intención de enriquecimiento a costa del empobrecimiento de la víctima».

Por último, la consumación de la estafa informática se produce en el momento en que el sujeto consigue la transferencia consentida. Consecuentemente, se precisa la efectiva producción del desplazamiento patrimonial con el perjuicio y enriquecimiento consiguientes, lo que no impide apreciar la infracción en grado de tentativa si, una vez realizada o comenzada la manipulación, no llega a producirse el resultado señalado.

2. *Defraudaciones del fluido eléctrico y análogas*

Antes de la tipificación expresa de este delito, se dudaba en encuadrar su apoderamiento entre los supuestos de hurto o estafa. La jurisprudencia se inclinó a través de una dudosa interpretación analógica, por incluir estos hechos en el delito de hurto. Actualmente dichos delitos se recogen en la Sección 3 del Capítulo IV (art.

[11] Orts Berenguer, E. *Ob. cit.*, p. 62.
[12] Orts Berenguer, E. *Ob. cit.*, p. 63 y ss.

255), pero se ha añadido la defraudación a través de uso ilícito de equipo terminal (art. 256) mientras que la facturación fraudulenta en perjuicio de los consumidores mediante alteración de aparatos automáticos se tipifica entre los delitos relativos al mercado y a los consumidores en el art. 283[13].

2.1. Defraudaciones en las telecomunicaciones

Art. 255 CP «Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1. Valiéndose de mecanismos instalados para realizar la defraudación.
2. Alterando maliciosamente las indicaciones o aparatos contadores.
3. Empleando cualesquiera otros medios».

Art. 256 CP «El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento del titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses».

Art. 623. 4 CP «Serán castigados con arresto de dos a seis fines de semana o multa de uno a dos meses: Los que cometan estafa, apropiación indebida, o defraudación de la electricidad, gas, agua, u otro elemento, energía o fluido, o en equipos terminales de telecomunicación, en cuantía no superior a cincuenta mil pesetas».

La conducta punible gira, pues, en torno a la defraudación, entendida como la autorización indebida, sea porque se efectúa una conexión o toma que permite utilizar una energía o unas telecomunicaciones sin tener derecho a ello, porque no se ha suscrito el correspondiente contrato y verificada la correspondiente alta en el servicio de que se trate, etc.; sea porque aun habiendo un contrato, un alta o una autorización, se realiza alguna de las manipulaciones tasadas en el art. 255. Estas manipulaciones implican obtener un servicio, un suministro de energía o aprovechamiento de telecomunicaciones de una cuantía superior a la que se abona, ocasionando en ambos casos un perjuicio superior a las cincuenta mil pesetas.

Nos encontramos así, según Orts Berenguer[14], ante un delito de resultado, cuya consumación requiere la causación de un perjuicio económico superior a cincuenta mil pesetas (de ser inferior dará lugar a la aplicación de la falta del art. 623.4).

Por último, en materia de participación, quien realiza la alteración de los indicadores o contadores o coloca o aplica los mecanismos y no se beneficia directamente, será cooperador necesario del que sí se beneficia que será el autor.

[13] Muñoz Conde, F. *Derecho Penal.* P.E., p. 431 y ss.
[14] Orts Berenguer, E. *Ob. cit.*, p. 71 y ss.

2.2. Uso de equipos terminales de telecomunicaciones

En este precepto, la conducta típica estriba en hacer uso del equipo terminal de telecomunicación. En esta expresión quedan abarcados teléfonos, fax, correo electrónico, etc. En consecuencia, el uso de cualquiera de estos artilugios puede dar lugar a la aparición del delito. Y el consentimiento faltará, tanto si se usan sin autorización, como si se hace un uso excesivo de los mismos, que rebase los límites fijados por el titular o la persona autorizada a cuyo cargo se encuentra.

Además, en el artículo 256 CP no se castiga el mero uso de un equipo terminal de telecomunicaciones, sino el uso acompañado de un perjuicio cuantificable en más de cincuenta mil pesetas.

De este modo, sujeto activo es cualquiera que no sea titular o cotitular del equipo, mientras que el sujeto pasivo es el titular del equipo, sea propietario o no del mismo.

En el caso de que el perjuicio no llegara a materializarse, podría hablarse de tentativa, y si se materializa, pero en cuantía inferior a cincuenta mil pesetas, de la falta del art. 624.

Este delito requiere dolo. Además este dolo puede ser eventual, si el autor del uso no está seguro de si se producirá el perjuicio o no, y, no obstante, prosigue su propósito, asumiendo que se genere.

3. *Los llamados daños informáticos*

En el vigente Código Penal el legislador ha tomado conciencia de la especial trascendencia que puede presentar la manipulación de la información contenida en soportes informáticos, tipificando lo que se conoce como «sabotaje informático», «vandalismo informático» o «cyberpunk», esto es, la destrucción o inutilización del soporte lógico de un ordenador con el fin inmediato de imposibilitar la información procesada o almacenada[15].

De este modo, tenemos que tener en cuenta los siguientes preceptos:

Art.263: «El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas».

Art. 264: «La misma pena se impondrá (la del art. 264.1) al que por cualquier medio destruya, altere, o inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos».

[15] Orts Berenguer, E. *Ob. cit.*, p. 77 y ss.

La conducta típica consiste en destruir, alterar, inutilizar, o en dañar de cualquier otro modo, los datos, programas o documentos electrónicos, acogiéndose así a la jurisprudencia que venía considerando como delito de daños no sólo la destrucción total del bien sino también su deterioro o menoscabo. Además, según Orts Berenguer[16], debe entenderse como cometido el delito tanto si se destruyen físicamente los soportes en que se encuentran los datos, programas o documentos, como si éstos se manipulan o se borran a través del propio sistema informático.

Por el contrario, no dan lugar a la aplicación de esta figura aquellos virus que no destruyen, alteran o inutilizan los datos, programas o documentos electrónicos a que se refiere el tipo, y causan al usuario tan sólo la incomodidad de no poder utilizar momentáneamente el equipo o alguno de los servicios que ofrece la red.

4. *Delitos relativos a la propiedad intelectual*

En el art. 270 CP se contiene la regulación básica de los delitos contra la propiedad intelectual: en él se definen las conductas prohibidas y los objetos sobre los que éstas recaen[17].

Art. 270: «Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica o su transformación, interpretación, o ejecución artística fijada en cualquier otro tipo de soporte o comunicada por cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización. Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador».

La conducta típica puede consistir, tanto en la fabricación o puesta en circulación, como en la mera tenencia de cualquier medio específicamente destinado a neutralizar la protección de los programas de ordenador. A diferencia de lo que ocurre en las obras artísticas o científicas y con las demás obras literarias, en las que se requiere que exista reproducción, plagio, etc., en los programas de ordenador basta para realizar el tipo con tener cualquier artilugio destinado a anular los sistemas de protección. Esta cláusula, por su generalidad, podría considerarse contraria

[16] Orts Berenguer, E. *Ob. cit.*, p. 77 y ss.
[17] Orts Berenguer, E. *Ob. cit.*, p. 86 y ss.

al principio de seguridad jurídica, si no fuera porque se exige que dichos medios estén específicamente destinados a inutilizar esos dispositivos, es decir, ha de tratarse de mecanismos directamente dirigidos a vulnerar esas barreras.

5. *Delitos relativos al mercado y a los consumidores*

En este precepto el legislador recoge una serie de conductas paralelas, en general, a las contenidas en el art. 197, si bien guiadas por un propósito distinto: mientras en éste el apoderamiento de los documentos, datos, etc., se hace con la finalidad de vulnerar la intimidad ajena, en el tipo que nos ocupa el sujeto activo pretende descubrir, conocer, determinados datos relevantes de la empresa, tipificándose lo que se conoce como «espionaje industrial». Y, al igual que ocurre en el delito citado, el legislador ha tenido en cuenta aquí los nuevos sistemas técnicos de almacenamiento de datos[18].

Art. 278.1: «El que para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del art. 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, relevaren o cedieren a terceros los secretos descubiertos. 3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos».

B. Delito de amenazas

Las amenazas inciden sobre la libertad de obrar, sobre la voluntad del sujeto pasivo; de este modo, quien amenaza a otro persigue que éste adopte una resolución, la querida por aquél. Las penadas en el art. 169 pueden presentarse bajo diferentes formas, condicionales o no condicionales, y todas ellas pueden ser llevadas a cabo aprovechando las transmisiones electrónicas, aunque el específico subtipo agravado del párrafo segundo del art. 169 se halla vinculado a las amenazas condicionales y no a las restantes[19].

Art. 169.1: «El que amenazare a otro con causarle a él, a su familia o otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad mo-

[18] Orts Berenguer, E. *Ob. cit.*, p. 102 y ss.
[19] Orts Berenguer, E. *Ob. cit.*, p. 117 y ss.

ral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado:

1. Con la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años. Las penas señaladas en el artículo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono, o por cualquier medio de comunicación o de reproducción o en nombre de entidades o grupos reales o supuestos.
2. Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional.

Según el profesor Muñoz Conde[20], en las amenazas simples el bien jurídico protegido es, más que la libertad en formación del acto voluntario, el sentimiento de seguridad o de tranquilidad.

El subtipo agravado del párrafo segundo del art. 169.1 presupone una amenaza condicional de un mal constitutivo de alguno de los delitos enunciados en el encabezamiento del art. 169. Una de las variantes de aquél admite la verificación por medios informáticos, pues lo son de comunicación y de transmisión, porque nada más fácil que hacer saber a alguien, por su intermediario, que se le causará un mal constitutivo de delito si no se aviene a satisfacer determinadas exigencias. Esta tarea puede desarrollarse a través de varias formas: vía correo electrónico, por la intromisión en un programa ajeno o en una página *web*, dejando en ellos el recado, con la posibilidad de no dejar huellas que permitan la identificación del emisor y de dificultar notablemente el rastreo para su detección.

La fundamentación de este subtipo agravado se ha cifrado en que los medios descritos poseen una mayor capacidad de quebrar la libertad de obrar del sujeto pasivo, ya sea por su carácter anónimo, por su apariencia de realidad o por su especial potencialidad intimidatoria.

C. Delitos contra la libertad e indemnidad sexual

Hace unos años, vigente ya el Código Penal de 1995, los medios de comunicación dieron cuenta de que unos jóvenes habían ofertado a través de Internet material pornográfico protagonizado por menores de edad. Entonces, se estimó que tales hechos no eran perseguibles, por cuanto en el art. 189 en su anterior versión se castigaba sólo la utilización de menores para producir aquella clase de

[20] Muñoz Conde, F: *Derecho penal.* P.E., p. 159.

material y no el hecho de traficar con éste. La atipicidad de esta conducta indicada causó cierto revuelo y contribuyó junto con otros casos más recientes a que el legislador, en la ley orgánica 11/1999 modificara el referido art. 189[21].

Art. 189 CP: «1. Será castigado con la pena de prisión de uno a tres años:

a) El que utilizare a menores de edad o a incapaces con fines en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico o financiare cualquiera de estas actividades.
b) El que produjere, vendiera, distribuyere, exhibiere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. A quien poseyera dicho material para la realización de cualquiera de estas conductas se le impondrá la pena en su mitad inferior».

El legislador ha pretendido proteger penalmente varios bienes jurídicos de los que son titulares los menores de edad y los incapaces: los adecuados procesos de formación y socialización de unos y otros y su intimidad.

Los hechos típicos consisten en vender, distribuir, exhibir material pornográfico elaborado con menores o incapaces. Estos menores e incapaces podrían ser utilizados con fines o en espectáculos exhibicionistas o pornográficos retransmitidos «en directo» por la red, sin que propiamente se llegue a confeccionar material pornográfico.

Todas las modalidades que se prevén en el art. 189.1. b) son dolosas: el sujeto ha de conocer la naturaleza del material y ha de querer realizarlo, difundirlo o poseerlo con dichos fines, siendo indiferente que lo haga con ánimo lúbrico o de lucro.

Además, hay que decir que la consumación del delito se produce tan pronto como una persona consigue introducir en la red material pornográfico elaborado con menores o incapaces, de forma que quede al alcance de cualquier usuario. Si antes de que ello ocurra, bien porque el sujeto es sorprendido y se le impide culminar su propósito, bien porque una vez lo ha conseguido se logra retirar el material sin que un solo usuario haya tenido posibilidad de examinarlo, estaremos ante tentativas inacabada y acabada, respectivamente[22].

D. Delitos contra el honor

La relación entre las transmisiones electrónicas y los delitos contra el honor se produce por la posibilidad de utilizar aquéllas para calumniar o injuriar a al-

[21] Orts Berenguer, E. *Ob. cit.*, p. 126 y ss.
[22] Orts Berenguer, E. *Ob. cit.*, p. 129 y ss.

guien, sea de manera directa y personal, por medio de un e-mail, dirigido al sujeto pasivo, sea genéricamente, lanzando el ataque contra el honor de éste vía Internet, de forma que las imputaciones hechas puedan ser conocidas por cualquier usuario de la red, mediante la lectura de un mensaje, de una noticia, comentario o editorial en un periódico o en una revista editada en la red, etc.[23].

Art. 205: «Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio por la verdad».

Art. 208: «Es injuria la acción o la expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación. Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves.

Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o consciente desprecio hacia la verdad».

Art. 211: «La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante».

Los delitos de calumnias y de injurias pueden ser cometidos con suma facilidad con medios informáticos y telemáticos, y alcanzar, merced a las potencialidades de éstos, una enorme propagación. Todo ello autoriza a apreciar que se han hecho públicos, pues resulta obvio que estos medios presentan una eficacia superior a la de la imprenta y la radiodifusión en cuanto a la propagación de aquéllas[24].

Estos delitos presentan dificultades probatorias consustanciales a la utilización de los susodichos medios.

E. Delitos contra la intimidad

Los peligros potenciales que entraña la tecnología informática se ponen de manifiesto especialmente en los delitos que afectan a la intimidad, no sólo por la facilidad con que puede vulnerarse este derecho a través de las nuevas técnicas, sino también porque la mecanización de datos permite obtener información relevante sobre las personas registradas en los sistemas informáticos mediante la combinación de elementos que individualmente pueden resultar intrascendentes[25].

Art. 197: «El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión o grabación

[23] Orts Berenguer, E. *Ob. cit.*, p. 140 ss.
[24] Orts Berenguer, E. *Ob. cit.*, p. 146 y ss.
[25] Orts Berenguer, E. *Ob. cit.*, p. 15 y ss.

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

Las conductas punibles han de estar dirigidas a descubrir los secretos o a vulnerar la intimidad de otros. Lo primero que llama la atención en estas descripciones es el carácter reiterado de estas infracciones realizadas a través de un ordenador. Todo ello sin contar con que algunas de esas acciones podrían encuadrarse también en el apartado siguiente si no fuera porque se mencionan en este número.

Para que concurra este delito es necesario que el autor realice una acción física dirigida a obtener los datos secretos. De lo contrario se llegaría a soluciones tan inverosímiles como la posibilidad de aplicar una pena de prisión de hasta cuatro años a quien se limitase a leer mensajes, cartas, etc., que el interesado hubiese dejado al alcance de terceros. Pero si el sujeto, aprovechando la negligencia ajena, realiza algún acto dirigido al apoderamiento de información reservada, habría que considerar típica la conducta, aunque no se llegase a descubrir ningún aspecto reservado.

Además, también son subsumibles en esta modalidad típica los actos de apoderamiento que se lleven a cabo a través de otros mecanismos informáticos como es el caso de los denominados *sniffers*, es decir, programas rastreadores que capturan la información contenida en la red, y que posibilitan el acceso al correo electrónico de sus usuarios. El carácter clandestino de estos mecanismos dificulta en muchos casos su detección y la identificación de su autor[26].

Art. 197.2: «Las mismas penas se impondrán al que sin estar autorizado, se apodere, utilice o modifique en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de fichero o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».

La acción punible puede consistir en apoderarse, utilizar o modificar datos reservados de carácter personal, o en acceder a ellos. Por lo tanto, el dolo presupone ya el conocimiento y voluntad de actuar sobre esa clase de datos que afectan a la intimidad, de manera que el elemento analizado ha de concebirse como un requisito distinto y añadido a ese dolo; tanto si se realiza para causar un perjuicio real o con la especial intención de vulnerar la intimidad[27].

El simple acceso no consentido a un sistema informático ajeno, *hacking*, con fines formativos, de aprendizaje, etc., o por el simple reto de vulnerar el *password*, es atípico salvo que con esa entrada se ocasionen daños en el soporte físico o en los elementos lógicos, sancionables como delito o falta de daños.

---

[26] Orts Berenguer, E. *Ob. cit.*, p. 27 y ss.
[27] Orts Berenguer, E. *Ob. cit.*, p. 30 y ss.

Sin embargo, para otros autores como Ruiz Marco[28], la tipicidad contenida en el art. 197.2.II CP podría cubrir las conductas de *hacking*. En este subtipo se observa que no se incorpora ningún elemento subjetivo, ni el ánimo de vulnerar la intimidad, ni el ánimo de perjudicar etc. Las conductas de *hacking* o de mero intrusismo informático definidas como «conjunto de comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicación electrónica de datos y a la utilización de los mismos sin autorización o más allá de lo autorizado»[29] podrían encajar en un primer momento en este segundo inciso del art. 197 CP, ya que como se ha dispuesto, el tipo no exige el elemento de lo injusto.

5. POSIBLES CALIFICACIONES JURÍDICAS

Después de haber estudiado todas las posibles conductas punibles relacionadas con los medios informáticos, sólo nos queda analizar si lo dispuesto en el CP es suficiente para regular el «delito informático».

Como ya hemos visto a lo largo de este trabajo, es imposible crear en el Código Penal un apartado cuya rúbrica fuera «De los delitos informáticos» debido a las singularidades de este delito, ya que no existe un único bien jurídico protegido, sino varios.

El problema principal al que nos enfrentamos es el del gran número de delitos relacionados con la informática que surgen continuamente como consecuencia de la rápida evolución de las telecomunicaciones, y que no encuentran encaje en el CP de forma autónoma.

De hecho, es inacabable la lista de delitos que pueden ser cometidos con un modesto ordenador personal, y se puede afirmar que en algún momento de la ejecución de toda infracción puede haberse hecho uso de la informática[30]. Mediante un programa de ordenador se puede hacer detonar una carga explosiva, cometer un asesinato o varios; se pueden cometer lesiones, provocar abortos, atentados, se puede prestar un auxilio ejecutivo al suicidio...

El CP regula, como ya hemos visto, algunos de estos delitos. Pero muchos de ellos quedan fuera y es aquí dónde surgen los problemas. ¿Qué hacemos con estos ilícitos?, ¿cómo los regulamos?, ¿y los que aparezcan en un futuro? Actualmente conductas como el *spam* (el envío de publicidad no deseada, normalmente a través de correo electrónico), el escaneo de puertos o la apología del terrorismo a través de Internet no están contempladas entre los delitos tipificados en el CP español.

---

[28] Ruiz Marco, F. *Los delitos contra la intimidad*, p. 79.

[29] Morón Lerma, E. *Internet y Derecho Penal:* Hacking *y otras Conductas ilícitas en la Red.* p. 51.

[30] Orts Berenguer, E. *Ob. cit.*, p. 158 y ss.

Como ya se ha afirmado anteriormente, es muy difícil saber a día de hoy las conductas penalmente relevantes que se cometerán en el futuro, porque el avance de las telecomunicaciones se produce a pasos agigantados. Es por ello por lo que considero que al no poder ser penados como delitos autónomos en sí mismos, podríamos castigarlos por el tipo básico del delito en cuestión (el cual se ha cometido a través de medios informáticos) y posteriormente añadirle la circunstancia genérica del art. 22.2 CP, donde se establece que: «Son circunstancias agravantes: Ejecutar el hecho... aprovechando las circunstancias de lugar, tiempo o auxilio de otras personas que debiliten la defensa del ofendido o faciliten la impunidad del delincuente».

El delincuente aprovechará, sin duda, estas circunstancias de lugar y de tiempo para cometer el delito. Además, a éstas podrán unirse otras como la rapidez para cometer el delito, para borrar pruebas y para encubrirse.

Por todo ello, la adición de la circunstancia genérica sería la solución más apropiada, ya que con ella se puede englobar a todos los delitos que se cometan en un futuro que, estando regulados en el CP, se realicen con medios informáticos.

Por ejemplo, imaginemos que se produce una falsificación de las cuentas de una sociedad a través de medios informáticos. Lo que encontramos en el CP es el tipo básico para la falsificación de las cuentas de una sociedad que dispone en su art. 290 CP que: «Los administradores, de hecho o de derecho, de una sociedad constituida o en formación que falsearen las cuentas anuales u otros documentos que deban reflejar la situación jurídica o económica de la entidad, de forma idónea para causar un perjuicio económico a la misma, a algunos de sus socios o a un tercero, serán castigados con la pena de prisión de uno a tres años y multa de seis a doce meses».

De este modo, empleando la informática, los administradores de una sociedad pueden falsear las cuentas y documentos de ésta, ya que cada vez está más extendida la práctica de utilizar medios informáticos para llevar la contabilidad de una empresa.

Si vamos al CP veremos que sólo encontramos el tipo básico de este delito, pero no dice nada acerca de la posibilidad de su comisión por medios informáticos. Es por ello, por lo que si nos encontramos ante un delito contable que se cometa a través de estos medios, aplicaríamos el tipo básico y le añadiríamos la circunstancia agravante del art. 22.2 CP, de este modo evitaríamos lagunas de punibilidad.

Como conclusión, creo necesario reiterar, como solución al problema planteado, que los delitos que se cometan a través de medios informáticos, y que estén tipificados en el CP como delitos autónomos (estafa, daños), se castigarán como tales; mientras que los que se cometan a través de esos mismos medios y no estén regulados en el CP, se castigarán por el tipo básico del delito en cuestión y se les añadirá la circunstancia genérica del art. 22.2.

También sería necesaria una cooperación para regular este tipo de delitos a nivel internacional, debido a su carácter peculiar. Así, podríamos encontrarnos ante acciones punibles en las que el sujeto activo puede estar, por ejemplo, en Estados Unidos y el sujeto pasivo en España y, en estos casos, se plantearían serios problemas de jurisdicción. No debemos olvidar que para Internet no existe, hasta ahora,

una jurisdicción aplicable, y que esta carencia es uno de los problemas más graves que puede encontrar un tribunal a la hora de condenar este tipo de ilícitos.

6. INTERNET Y EL DELITO INFORMÁTICO

La mayoría de los delitos informáticos guardan relación con Internet y son varios los autores que ponen énfasis en la necesidad de crear una jurisdicción que regule los delitos cometidos a través de la red. Es el caso de Cafferata[31], para quien la red de redes se nos presenta como un conglomerado global de computadoras interconectadas que adquieren y distribuyen información entre sí desde distintos lugares físicos, y que por ello ignora los límites geopolíticos.

Así afirma que, a pesar de que Internet ha supuesto la gran revolución de las telecomunicaciones, ya que se puede acceder a todo tipo de información a través del ordenador y permite intercambiar ideas [...] no todo ha sido positivo, ya que, éste, desgraciadamente, también es un medio para cometer delitos. De este modo, se pueden cometer ilícitos a través de la red de forma sencilla gracias, fundamentalmente, a la rapidez del sistema, a la facilidad para borrar las pruebas y a la dificultad a la hora de identificar al sujeto activo de tales ilícitos.

¿Debe estar la red sujeta a algún tipo de regulación jurídica? Autores como Brenna[32], que difunden sus teorías a través de Internet, consideran que sí, y para ello este autor propone las siguientes alternativas: unificar las reglas legales; creación de una ley sustantiva de Internet o reconocer a Internet una jurisdicción propia y asignar disputas a un Tribunal Internacional de Arbitraje de Internet o a una Corte Especial exclusiva para estas disputas.

Existe un proyecto de «magistrado virtual», auspiciado por el National Center for Aumated Information Research, American Arbitration Asociation y Villanova Center for information law and policy. Esta iniciativa, según Cafferata[33], consiste en aplicar una especie de sistema de arbitraje internacional para los conflictos suscitados por transacciones en la red. De este modo el magistrado podrá emitir sentencias en conflictos en línea, a través del correo electrónico. Esto permitiría, a quien presenta reclamaciones sobre la aplicación de las normas, que sus casos fueran oídos por una parte neutral.

Según lo analizado hasta ahora, existirían dos maneras conocidas de alcanzar un derecho unificado sustantivo para Internet: que las Cortes y Tribunales desarrollasen con sus pronunciamientos un derecho común de Internet o que se realiza-

---

[31] Cafferata, F. *Acciones legales en Internet y resolución de conflictos on line*, p. 4. <http://www.it-cenit.org.ar/Seminarios/DerEconDIG2000/material/accleg/accleg.htm>.

[32] Brenna. Acciones legales en internet y resolución de conflictos, p. 6. <http://www.it-cenit.org.ar/Seminarios/DerEconDIG2000/material/accleg/accleg.htm>.

[33] Cafferata, F. *Acciones legales en Internet y resolución de conflictos on line*, p. 10. <http://www.it-cenit.org.ar/Seminarios/DerEconDIG2000/material/accleg/accleg.htm>.

sen acuerdos o tratados internacionales a tal fin. Este Derecho unificado sustantivo de Internet, generado a partir de la decisión de las Cortes, tendría la característica de ser un derecho de sujeto específico y no de lugar específico.

Burnstein[34], quien también utiliza la red para exponer sus teorías, propone tomar, para la creación de una legislación común en la materia, como modelo la *lex mercatoria*. Esta ley de comercio tuvo origen en una colección de prácticas y costumbres desarrolladas por los viajantes de comercio de la Europa medieval y se convirtió en «obligatoria» en todos los países comerciales del mundo civilizado por aquellos tiempos.

De este modo, así como los comerciantes desarrollaron y practicaron ese conjunto de usos y costumbres hasta convertirlos en ley, podría pensarse que los usuarios de Internet desarrollarán usos y costumbres del mundo *on line*, y que esta práctica generase, por su acatamiento, un derecho común de este espacio, que algunos denominan ciberespacio. Así, cuando un Tribunal fuere llamado a intervenir para resolver una disputa de Internet buscaría, en este derecho consuetudinario del ciberespacio, la colección de costumbres, usos y prácticas, que ya estuvieran aceptadas, por los usuarios, gobiernos, industrias y demás sujetos reconocidos en la red.

En España, cabe destacar la existencia de la ARBITEC (Asociación Española de Arbitraje Tecnológico), constituida en mayo de 1989. Ésta, en febrero de 1997, se convirtió en la primera institución española que admite solicitudes de arbitraje a través de Internet, utilizando la red en todas las fases del procedimiento arbitral.

7. CONCLUSIÓN

«El problema de los delitos informáticos no es técnico sino humano»[35].

Es evidente que no son las máquinas las que delinquen sino los hombres. También está fuera de toda duda la inexistencia de una solución técnica de aplicación universal que pueda permitir que, con la compra de un determinado aparato o con la aplicación de una tecnología concreta, nos encontremos totalmente a salvo de la delincuencia informática.

La primera premisa que tenemos que asumir es que el enfoque correcto del problema «seguridad informática versus delitos informáticos», es que se trata de un asunto de hombres contra hombres dentro, eso sí, de un entorno altamente tecnificado. Pero, en cualquier caso, el primer factor del éxito está en la anticipación, en ir por delante, en que la seguridad preceda a la delincuencia, aunque en ningún caso debemos olvidar que las medidas de seguridad que un hombre ha establecido, otro hombre puede violarlas. Por ello, el segundo factor a tener en

[34] Burnstein. *Acciones legales en internet y resolución de conflictos on line*, p. 25.
[35] Camacho, L. *El Delito informático*, pp. 125-126.

cuenta debe ser el concepto de *seguridad permanente*: la continuidad en la aplicación de las medidas establecidas y la permanente adecuación de la seguridad a las nuevas circunstancias mediante la aplicación de nuevas medidas que refuercen o sustituyan a las antiguas.

Además, estas medidas de seguridad deben llevarse a la práctica rápidamente, ya que los delitos en Internet se han multiplicado en los últimos años. Como ejemplo podríamos señalar el informe de la Policía Autónoma Catalana[36], en el que se afirma que la exhibición de *pornografía infantil* en la red, las estafas y los ataques de seguridad a las empresas, tanto del ámbito privado como del público, se han disparado en los últimos años. En este informe destaca, también, la aparición cada vez más frecuente de *crackers*, usuarios destructivos cuyo objetivo es el de crear virus e introducirse en otro sistema para dañarlo. Por último, se hace referencia al hecho de que cada día más personas utilizan este medio, tanto para comunicarse como para realizar compras, etc., y esto provoca que el número de delitos o de *estafas* también sea mayor. Todo esto hace cada vez más necesaria una legislación aplicable a los delitos que se cometen a través de los medios informáticos.

Por otra parte, Alfons Cano, jefe de la unidad de delitos tecnológicos de los Mossos d'Esquadra, comenta la variación que ha sufrido su unidad desde el año 1995, cuando fue creada. Mientras algunas formas delictivas han crecido, como se comentaba anteriormente, otras han disminuido, como es el caso de las *amenazas* a través del correo electrónico, gracias a los filtros de «correo no deseado».

A tenor de lo anteriormente afirmado, considero que el problema fundamental se produce al conjugarse dos factores esenciales: en primer lugar, el problema de que Internet facilita la comisión de delitos, principalmente por la rapidez con la que se cometen los hechos, porque difícilmente se dejan huellas [...] y, en segundo lugar, porque la imaginación del delincuente informático no tiene límite. De este modo, según manifiesta Luis Camacho[37], las «técnicas de la guerrilla urbana», que por desgracia son eficaces y también dificilísimas de prevenir y controlar por las Fuerzas de Seguridad del Estado, pueden ser sustituidas por la «guerrilla informática» que, de forma más simple, más eficaz y menos sangrienta, puede desestabilizar la convivencia ciudadana provocando el pánico en la sociedad.

Mediante estas técnicas, se puede sembrar el caos circulatorio en las grandes ciudades a través de la manipulación de los sistemas informáticos de control del tráfico, descompensando el funcionamiento de los semáforos para que se abran y se cierren todos a la vez, poniéndolos simultáneamente en intermitente en todas las direcciones.

También se podrían cortar los suministros de energía eléctrica por períodos prolongados en las grandes urbes, lo cual puede hacerse extensible a los servicios de agua, gas, teléfono, etc.

---

[36] <http://www.delitosinformáticos.com>.

[37] CAMACHO, L. *El Delito Informático*, p. 141.

Además, se podrían inutilizar los controles informatizados de seguridad en grandes instalaciones industriales, con lo que se provocarían accidentes laborales, alterando los controles de temperatura, presión, etc., en procesos químicos, refinerías y similares.

En definitiva, podemos afirmar que la informática abre nuevos perspectivas al delincuente, fomenta su imaginación, favorece su impunidad e incrementa los efectos del delito convencional. A todo ello contribuye la facilidad para la comisión y encubrimiento de estas conductas y la dificultad para su conocimiento.

El objetivo de este trabajo ha sido demostrar la inexistencia de suficientes normas capaces de regular el delito informático en el ordenamiento jurídico, puesto que el desarrollo de las nuevas tecnologías produce ataques cada vez más graves a los bienes jurídicos, y de ahí mi insistencia en que sea el Derecho Penal el que regule dichas conductas.

Ante esta nueva realidad en la que nos vemos inmersos, el legislador debe ponerse en marcha para impedir que este tipo de conductas se sigan cometiendo y, en consecuencia, impedir la impunidad de los presuntos delincuentes. Como ya he señalado anteriormente, una posible solución sería la de agravar la pena con la circunstancia genérica del art. 22.2 CP.