EGUZKILORE
Número 23.
San Sebastián
Diciembre 2009
227 - 243

EL DELITO INFORMÁTICO

Leyre HERNÁNDEZ DÍAZ

Investigadora en formación
Beca pre-doctoral, Gobierno Vasco

Sumario:

I. EL DERECHO INFORMÁTICO

La delincuencia informática se encuadra dentro de lo que se conoce como "Derecho informático"[1]. Éste es el conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad[2], incluyendo como objeto de

1. Que nada tiene que ver con el concepto de "informática jurídica", referido al uso de las nuevas tecnologías de la información y comunicación como nuevas herramientas de trabajo para los juristas, siendo su objeto de estudio la aplicación de la tecnología de la información al Derecho. Sobre el origen y la evolución de este concepto, IASELLI, *Informatica giuridica*, pp. 7 ss.; sobre los distintos sectores que integrarían este ámbito jurídico, DI GIORGI/RAGONA, "L'informatica giuridica", pp. 9 ss.; y, en la doctrina española, PÉREZ LUÑO, en *Manual de informática y Derecho*, pp. 22 ss.

2. Así, ZICCARDI, G., "Il diritto dell'informatica", p. XIII.

estudio: 1º el régimen jurídico del software; 2º el derecho de las Redes de transmisión de datos; 3º los documentos electrónicos; 4º los contratos electrónicos; 5º el régimen jurídico de las bases de datos; 6º el derecho de la *privacy;* 7º los delitos informáticos; y 8º otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos[3].

En lugar de crear una nueva rama del Derecho dedicada exclusivamente al estudio de estos aspectos, podría haberse abordado la regulación o estudio de cuanto concierne al ámbito de digitalización del mundo empresarial, administrativo e incluso personal desde un análisis por cada una de las ramas del ordenamiento jurídico ya existentes, en las que habría que encajar estas nuevas realidades en función del aspecto concreto a analizar. Así, de los contratos electrónicos se ocuparía el Derecho civil o mercantil, de las conductas ilícitas vinculadas a las nuevas tecnologías el Derecho administrativo o penal, etc. Sin embargo, la complejidad de las relaciones informáticas, el crecimiento desmesurado de las mismas o el hecho de que en el estudio de estas nuevas relaciones se transite de una rama del ordenamiento jurídico a la otra constantemente (administrativa, civil, laboral o penal) ha favorecido que por motivos pragmáticos desde algunos sectores se haya reclamado la consideración de una nueva rama del ordenamiento jurídico que regularía las relaciones, cualesquiera, vinculadas con la informática[4] que tendría como característica, precisamente, el hecho de que en la disciplina confluyan normas administrativas, civiles, laborales, penales, etc.[5].

II. LA EVOLUCIÓN DE LA IMPLANTACIÓN DE LAS TICS (Tecnologías de la información y comunicación) y su vinculación con la aparición de nuevas conductas ilícitas o delictivas

La primera dificultad a la hora de afrontar el análisis de los delitos informáticos es su conceptualización. No resulta fácil considerar qué debe entenderse por delito informático y qué conductas pueden considerarse incluidas en el mismo; de hecho, ni siquiera la doctrina encuentra un concepto unitario de delito informático y las discrepancias en torno al mismo han llegado incluso a propiciar que algunos autores admitan la imposibilidad de dar una definición del mismo y renuncien a ello[6]. La doctrina ha debatido durante años si nos encontramos ante una categoría que pueda denominarse "delito informático" o si, por el contrario, se deben utilizar expresiones para definir la misma realidad que carezcan de un matiz jurídico-positivo y que hagan alusión, más bien, a categorías criminológicas: así las expresiones delincuencia informática, criminalidad informática o delitos informáticos, ésta no en cuanto concepto sino en cuanto

3. Clasificación del objeto de estudio del Derecho informático realizada por MARTINO, "Informatica e Diritto: farfugliato, imbricato rapporto" pp. 14 y 15.

4. Profundizan en la conveniencia de considerar que estas nuevas realidades integren una nueva rama del Derecho, MARTINO, "Informatica e Diritto: farfugliato, imbricato rapporto", pp. 9 ss.; o PÉREZ LUÑO, *Manual de informática y derecho*, pp. 18 ss., entre otros.

5. Véase ZICCARDI, "Il diritto dell'informatica", p. XIII.

6. Así se manifiesta, por ejemplo FERREYROS SOTO, "Aspectos metodológicos del delito informático", pp. 407 ss., que, prescindiendo de una conceptuación, se limita a enumerar las peculiaridades que presenta el conjunto de comportamientos a que puede venir referida la expresión.

realidad de características concretas[7]. Parte de este problema proviene de la vertiginosa velocidad con la que evolucionan las nuevas tecnologías y el consiguiente constante cambio y desarrollo, también extremadamente rápido, de las conductas delictivas vinculadas a las mismas.

Parece adecuado, por ello, antes de exponer los distintos conceptos de delito o delitos informático o informáticos que se han propuesto, hacer un repaso, en términos bastante generales, del modo en que se han ido implantando las nuevas tecnologías y del modo en que, en consecuencia, ha ido apareciendo el nuevo elenco de conductas lesivas de derechos vinculadas con la informática y la telemática.

Consideramos útil para este fin el modo sistemático en que fue definida esta evolución de las conductas delictivas (o merecedoras de serlo) vinculadas con las TICs en el "Informe sobre la situación del crimen organizado en Europa" realizado por el Consejo de Europa[8].

En primer lugar, la ingente acumulación de datos de carácter personal de la ciudadanía por parte de los gobiernos, aun cuando no estaba masificado el uso de los ordenadores, hace que comiencen las preocupaciones en torno al carácter reservado, la acumulación y el uso que podría hacerse de estos datos. Nace así el concepto de *privacy* y de derecho a la misma, que va más allá del tradicional de intimidad y que regula la acumulación en las bases de datos, de carácter informático o no, de información sobre los individuos y el uso que se hace de ella, así como la capacidad de decisión de cada ciudadano respecto a qué datos referentes a su persona deben ser compartidos o públicos. Ya en los años sesenta comienzan las primeras discusiones en torno a esta cuestión, sobre todo en materia civil y administrativa, planteándose el debate, en los años siguientes, también en términos penales[9].

Durante la década de los setenta, la difusión de los ordenadores en el mundo empresarial supuso que la mayoría de las manifestaciones de la delincuencia informática tuviesen relación con la delincuencia económica, siendo las más comunes el fraude informático, la manipulación de datos, sabotajes informáticos, espionajes empresariales, etc. Hasta el punto de que en este periodo eran estas nuevas modalidades de delincuencia económica las que integraban el concepto de delito informático; o, al menos, éstas eran las principales manifestaciones del mismo[10].

En los años ochenta, la generalización de los ordenadores personales entre la población trajo consigo, al mismo tiempo, el surgimiento de la piratería del *software*

---

7. Tempranamente se mostraron a favor de esta opción GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, pp. 51 ss.; y ROMEO CASABONA, *Poder informático y seguridad jurídica*, pp. 40 ss.

8. *Organised crime in Europe: the threat of cybercrime. Situation report 2004*, pp. 84 ss.

9. Véase el fundamental trabajo, en nuestra disciplina, de MORALES PRATS, *La tutela penal de la intimidad: privacy e informática*.

10. Uno de los pioneros en la vinculación de la delincuencia informática con la lesión de intereses patrimoniales o económicos fue SIEBER, *Computerkriminalität und Strafrecht*, p. 188. Sin embargo, ya en 1986, a la vista de la evolución del tipo de conducta vinculada al uso de las nuevas tecnologías, el mismo autor, en *The International Handbook on Computer Crime*, pp. 26 ss., incluyó también conductas lesvias de otro tipo de intereses. Véase, entre nosotros, en 1988, ROMEO CASABONA, *Poder informático y seguridad jurídica*, p. 22.

de los mismos, dando comienzo así a las primeras infracciones contra la propiedad intelectual que se generalizarían a finales de los años noventa, extendiéndose además de a dicho *software*, a productos como música o películas.

La expansión de Internet en la década de los noventa llevó aparejado el surgimiento de un nuevo método para difundir contenidos ilegales o dañosos, tales como pornografía infantil o discursos racistas o xenófobos. Serán justamente las conductas vinculadas a la difusión de contenidos ilícitos las que más pueden aprovecharse de la enorme implantación que tiene la Red a nivel mundial, así como de sus características técnicas que dificultan su descubrimiento, persecución y prueba.

En este período también se consolida la dependencia que los gobiernos y organismos internacionales tienen de los sistemas informáticos, tanto para su buen funcionamiento como para el almacenamiento de datos importantes y/o secretos y ello pondrá en el punto de mira para la comisión de delitos que atenten contra la seguridad del Estado, como la comisión de ataques terroristas a través de la Red, a los sistemas informáticos de estos Entes.

Hoy, con la expansión del uso de los sistemas informáticos y de la telemática en todos los ámbitos, tanto públicos como privados, prácticamente cualquier delito (homicidio, tráfico de drogas, delito de terrorismo, etc.) puede ver favorecida su comisión a través de la utilización de las nuevas tecnologías de la información y de la comunicación.

III. PRIMERAS DEFINICIONES DE LOS DELITOS INFORMÁTICOS

Las definiciones que a lo largo de los últimos cuarenta años se han aportado del concepto de delito informático van necesariamente unidas a la evolución que ha sufrido la implantación de las TICs en la sociedad y a las propias conductas delictivas, o merecedoras de serlo, vinculadas con las nuevas tecnologías de la información y de la comunicación.

Como antes se decía, las primeras conductas dañosas de cierta entidad que aparecieron unidas a la proliferación de los ordenadores se centraban, principalmente, en el ámbito empresarial y consistían en conductas lesivas del patrimonio. Por este motivo, aunque generalmente sin olvidar los posibles problemas que la acumulación de datos de carácter personal podía conllevar, que serían tratados de modo independiente al del tratamiento de la delincuencia informática en general, las primeras definiciones de lo que debía entenderse por delito informático se limitaban al ámbito patrimonial[11]. Incluso cuando ya se vislumbraba una proliferación de tipologías muy variadas de ilícitos vinculados con las nuevas tecnologías y la problemática que podía surgir de esta proliferación de ilícitos era al menos mencionada en los estudios realizados sobre el tema, el delito o delitos informáticos se analizaban, prácticamente de modo unánime, dentro de estudios doctrinales dedicados a la delincuencia patrimonial[12].

---

11. Importantes autores, como TIEDEMANN, "La criminalidad económica como objeto de investigación", pp. 173 ss., se han centrado exclusivamente en la vertiente patrimonial de estos delitos, considerándolos una parte de la delincuencia económica.

12. Véase, entre nosotros, ROMEO CASABONA, *Poder informático o seguridad jurídica*, pp. 47 ss., que analiza el concepto de delincuencia informática dentro del capítulo que en su libro dedica al fraude informático; o GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, pp. 51 ss.

Una de las primeras definiciones fue la aportada por PARKER, que definió los *abusos informáticos* como "cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio"[13]. Este autor no se limitó a describir las conductas relevantes para el ámbito penal sino que reconoce que se trata de un amplio abanico de conductas en las que se incluyen además de conductas de naturaleza penal, otras de relevancia civil y meros incidentes sin trascendencia jurídica. A pesar de la vertiente patrimonial de su estudio, el autor también se preocupó por los ataques a la intimidad que, con la creación de las primeras bases de datos, podían derivarse de la digitalización de datos de naturaleza privada.

En 1978, habiendo ya saltado a la prensa algunos de los primeros casos de delincuencia informática patrimonial, BEQUAI realizó un análisis de estos delitos considerando que en la definición del delito informático el acento debe ponerse en que los ordenadores pueden ser usados por el autor del delito no sólo como instrumentos para cometer el mismo sino también como objeto del delito. Este autor incluyó entre los *computer crimes* los delitos de sabotaje informático, robo de información digitalizada y programas, espionaje industrial, hurto de tiempo de uso del ordenador, robos de mercancías por manipulación de datos o fraudes financieros. Asimismo, se aproximó a los problemas concretos que plantea esta delincuencia, entre los que destacaba la facilidad con que pueden ser manipulados los ordenadores y su información, la dificultad de establecer medidas de seguridad de carácter técnico sin que, al mismo tiempo, se bloqueen la fluidez de las transacciones realizadas a través de los ordenadores[14], poniendo también de manifiesto, por último, los problemas de persecución que planteaban los delitos informáticos dadas las dificultades para la admisión de pruebas de carácter tecnológico que presentaban los ordenamientos jurídicos en aquel momento[15].

En contra de incluir entre los delitos informáticos, sin embargo, los ilícitos de carácter patrimonial en los que el sistema informático era el objeto del delito, en la doctrina española CAMACHO LOSA consideró que, no habiendo una definición de delito informático plenamente satisfactoria, debía considerarse delito informático "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas"[16]. Pero, dejó fuera del delito informático aquellas conductas que tienen como objeto del delito los dispositivos informáticos por la relación meramente accidental que, en su opinión, tienen éstas con la informática.

Otro de los autores españoles que se acercó tempranamente a la delincuencia informática de carácter patrimonial, aunque sin olvidar los problemas de *privacy* que puede provocar la acumulación de datos de carácter personal en ficheros, fue

---

13. PARKER, *Crime by computer*, pp. 12 ss. y 237 ss.

14. En esto insistiría también especialmente SIEBER, *La délinquance informatique*, pp. 166 ss.

15. BEQUAI, *Computer Crime*, pp. 3 ss.; y, del mismo, *White-Collar Crime: a 20th-Century Crisis*, pp. 105 ss.

16. CAMACHO LOSA, *El delito informático*, pp. 25 ss.

GONZÁLEZ RUS, que destacó la imposibilidad de agrupar todos los delitos vinculados con las nuevas tecnologías en un único concepto de delito. Por ello, sin intención de dar un catálogo exhaustivo, clasifica los "ilícitos informáticos" como un conjunto de delitos de carácter heterogéneo que puede dividirse en dos grandes grupos: por un lado, el de las amenazas para la intimidad personal y la esfera privada derivadas de la ingente acumulación de datos; y, por otro, el de los delitos patrimoniales, favorecidos en su comisión por las posibilidades que ofrecen las nuevas tecnologías. Y, centrándose en el grupo dedicado a los ilícitos patrimoniales relacionados con medios o procedimientos informáticos, el autor realiza una nueva subdivisión. Por una parte, considera los delitos contra el sistema informático, referido éste tanto a sus elementos físicos como lógicos, incluyendo aquí los delitos de hurto, hurto de uso, robo, apropiación indebida, estafa y daños. De otra parte, los delitos cometidos "por medio" del sistema informático, distinguiendo a su vez, dentro de éstos, aquéllos en los que el uso del modo informático no es absolutamente necesario, pudiéndose cometer el delito por un medio no informático si el autor así lo hubiese decidido, y los que únicamente pueden ser cometidos por medios informáticos. De este modo, no sólo incluye en los delitos informáticos aquéllos que se cometen a través de sistemas informáticos, sino también aquéllos que se cometen contra los sistemas informáticos[17].

Cabe destacar que tanto CAMACHO LOSA como GONZÁLEZ RUS, que escribieron sobre estas cuestiones en 1987 y 1986, respectivamente, ya mencionaban entre el catálogo de los delitos informáticos los denominados como piratería del *software*, que empezaban a despuntar en esa década.

La proliferación de conductas delictivas o ilícitas vinculadas a la informática fue complicando la definición de los delitos informáticos, no pudiendo ya limitarse ésta a conductas vinculadas estrictamente con el patrimonio o con la intimidad. Por ello, en 1983 un comité de expertos convocado por la OCDE definió, de una manera vaga e imprecisa, los *computer-related crimes* como "cualquier comportamiento, no ético o no autorizado relacionado con el procesado automático de datos y/o transmisiones de datos". Se trata de una primera aproximación a un posible concepto, adoptada en un principio por varios autores con el argumento de que una definición de esa amplitud permitiría el tratamiento de las mismas hipótesis de trabajo para distintas disciplinas y podría así usarse una misma definición en análisis penales, económicos, sociológicos, etc[18]. La definición puede servir como una primera aproximación conceptual que puede resultar útil para delimitar qué conductas ilícitas o indeseables tienen alguna vinculación con la informática; sobre todo, porque en los primeros años en que comenzaron estos nuevos ataques los Códigos penales se encontraban ante realidades no siempre abarcadas por ellos. De hecho, aún hoy son muchas las conductas, como el

17. GONZÁLEZ RUS, "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", pp. 107 ss.; véase su postura, en la actualidad, negando abiertamente la posibilidad de proponer un único concepto de delito informático, en GONZÁLEZ RUS, "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", pp. 14 ss.

18. Véase, entre otros, SIEBER, *The International Handbook on Computer Crime*, pp. 26 ss., y "Documentación para una aproximación al delito informático", p. 66, tras participar en la Comisión encargada de redactar la recomendación de la OCDE, y aun cuando en sus primeros trabajos se limitara a establecer una definición de delitos informáticos de carácter patrimonial (SIEBER, *Computerkriminalität und Strafrecht*, p. 188).

denominado *hacking* blanco, cuya caracterización como delictiva es discutible y discutida en los distintos ordenamientos penales, lo que dificulta más aún la propia conceptualización del delito informático. La pretensión del concepto de la OCDE de abarcar conductas tanto penales como extrapenales ha restado virtualidad operativa al mismo y favorecido su progresivo abandono en sede penal.

En todo caso, autores como SIEBER, a pesar de adoptar este concepto amplio de delito informático, terminan clasificando los ilícitos informáticos en dos grupos: los delitos patrimoniales vinculados con la informática y aquellos con relación a la acumulación de datos de carácter personal en los sistemas informáticos, mencionando, sin indagar demasiado en ellos, la problemática que podía surgir con la posible comisión de delitos contra intereses supraindividuales, o de cualquier otro tipo, a través de los ordenadores[19].

A pesar de que varios autores, apoyándose en la necesidad de un concepto amplio de delito informático, adoptaron un concepto similiar al antes descrito[20], una parte de la doctrina no tardó en poner de relieve, por un lado, la excesiva amplitud del concepto y, por otro, la escasez de valor que dicha definición aporta en términos estrictamente técnico-penales, ya que se pueden incluir en el mismo tanto conductas típicas como conductas que no encajan en la definición de delito que establezca cada Código penal[21].

A finales de la década de los ochenta ROMEO CASABONA, tratando de superar las definiciones arriba expuestas, puso de relieve que no se podía considerar la existencia de un significado general predicable al delito o abuso informático. No puede hablarse de un delito informático, dirá, sino de una pluralidad de ellos, en los que la única nota común es su vinculación de alguna manera con los ordenadores. No se trata de delitos que tengan un único bien jurídico común, añadía, ni la forma de comisión del hecho presenta siempre características semejantes, porque en ocasiones estamos ante delitos en los que el instrumento mediante el que se realizan las conductas es de naturaleza informática, mientras que en otras ocasiones el elemento de naturaleza informática lo aporta el propio objeto del delito. Por eso, considera más acertado hablar de delincuencia informática o de delincuencia vinculada al ordenador o a las tecnologías de la información[22].

Quizás la aportación más importante de este autor, en este contexto, sea justamente la idea de que la delincuencia informática o los delitos relacionados con la misma indican un aspecto de la criminalidad caracterizado por las especificidades aportadas por las funciones propias del ordenador de procesamiento y transmisión

19. SIEBER, *The International Handbook on Computer Crime*, pp. 3 ss.

20. Después de sus primeras definiciones centradas en el aspecto patrimonial, autores tan importantes como TIEDEMANN, *Poder económico y delito*, pp. 122 ss. acabarían definiendo la criminalidad informática atendiendo todo tipo de actos antijurídicos según la ley penal vigente o socialmente perjudiciales y por eso penalizables en el futuro realizados con el empleo de un equipo de procesamiento de datos.

21. Véase en este sentido, GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, pp. 56 ss.

22. Así, ROMEO CASABONA, *Poder informático y seguridad jurídica*, pp. 42 ss.

automatizados de datos y la confección y/o utilización de programas para tales fines[23]. Cualquier conducta que no tenga relación con esas funciones aunque se trate de una conducta delictiva, o deba considerarse su sanción, no deberá a juicio de ROMEO formar parte de la delincuencia informática, careciendo de importancia a su juicio si en la comisión del hecho el ordenador es el objeto sobre el que recae la conducta o el medio para cometerla, e incluso considerando irrelevante para la definición de la delincuencia informática, aunque no para el estudio de la misma, que la conducta pueda ser considerada delictiva o sea merecedora de serlo[24].

Poco después, también extensamente, GUTIÉRREZ FRANCÉS[25] se ocupó de los problemas de definición que planteaba el delito informático. Y, si bien el ámbito que introdujo a la autora en el análisis del concepto de delincuencia informática fue el del fraude informático, en su enfoque conceptual no se centró únicamente en la delincuencia informática patrimonial, poniendo de relieve, como ya otros muchos autores, que los sistemas informáticos y todos sus componentes no sólo pueden ser el medio a través del que se cometen los delitos en cuestión, sino que ellos mismos pueden ser objeto de un delito. La autora puso de relieve, mediante varios ejemplos, que prácticamente cualquier delito puede ser cometido utilizando sistemas informáticos y, por ello, descarta de antemano que en la definición de delito informático quepa incluirse todos los delitos en los que de alguna manera pueda aparecer involucrado un ordenador, pues cualquier delito podría entonces calificarse como informático.

Por otra parte, y en la línea ya avanzada por ROMEO CASABONA, la autora considera inadecuado el término "delito" porque tiene un significado muy específico en Derecho penal que no se ajusta a algunas conductas clasificadas en ocasiones como delitos informáticos pero que no tienen su encuadre en ninguna conducta tipificada penalmente. Por eso acabará explicando que no puede hablarse de un único delito informático, sino de una pluralidad de ellos, en los que la única nota común es la vinculación de alguna manera con los ordenadores, en concreto con las funciones propias del ordenador de procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para ello, sin que, sin embargo, sea el bien jurídico el mismo en todos los delitos informáticos ni presenten sus formas de comisión siempre las mismas características. En este sentido señala expresamente que es mejor recurrir a formulas menos rígidas, como la de "delincuencia informática", que reflejen el carácter criminológico de las conductas, para incluir así tanto a las conductas tipificadas como las merecedoras de serlo de *lege ferenda*.

---

23. Véase en este sentido, en Italia, entre otros, ZICCARDI, "Il diritto dell'informatica", p. 332, que tratando también de poner el énfasis en la parte técnica de los ordenadores o sistemas informáticos, aunque con un carácter diferente, define el delito informático como cada acto ilegal para cuya realización resulta esencial el conocimiento de la tecnología informática.

24. ROMEO CASABONA, *Poder informático y seguridad jurídica*, p. 43.

25. GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, pp. 49 ss.

IV. DELINCUENCIA INFORMÁTICA, CRIMINALIDAD INFORMÁTICA O DELITOS INFORMÁTICOS COMO ALTERNATIVAS AL DELITO INFORMÁTICO

En las primeras definiciones de "delito informático" que se han ido aportado por la doctrina no ha resultado fácil concretar un único concepto de delito informático; por ello, en la actualidad niega un sector de la doctrina la existencia de este concepto y, con ello, de esta tipología delictiva, prefiriendo utilizar para abarcar todo este conjunto de comportamientos que tienen que ver con la informática, de uno u otro modo, expresiones como "Delincuencia informática", "Criminalidad informática" o, simplemente, en plural, "Delitos informáticos".

Con argumentos similares a los aportados a principios de los noventa por varios autores, son ya ahora muchos los autores que se decantan por expresiones que eludan el término "delito", por la problemática antes apuntada en relación con las limitaciones que la utilización de un término que hace referencia a una realidad jurídica positiva conlleva: si sólo es delito lo que la ley penal establece como tal y en ella no existe referencia alguna al delito informático, no podría afirmarse, cuando menos en el ordenamiento español, como en otros muchos, que exista tal delito[26]. Se añade, además, que tampoco existe un Título en el Código Penal sobre los delitos informáticos, encontrándose las distintas conductas vinculadas de una u otra manera con los sistemas informáticos, ya sea por el medio de comisión, ya por el objeto del delito ya incluso por ambos aspectos, dispersas en diferentes Títulos del Código, en una ubicación en que lo que prima es el bien jurídico afectado[27].

Por ello la doctrina quizás hoy mayoritaria prefiere acudir a aquellas expresiones de "delincuencia informática" o "criminalidad informática" para incluir en ellas todos los comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera, y todos aquéllos en que dicho sistema sea él mismo el propio objeto sobre el que recae la acción delictiva[28]. Algunos autores añadirán la exigencia de que además las conductas incluibles en tales expresiones reúnan los requisitos que delimitan el concepto de delito[29]. Y otros, incluso, aun aceptando la heterogeneidad de estas conductas, dejan fuera del grupo aquéllas en las que los sistemas informáticos, o la información en ellos contenida, es el objeto sobre el que recae la conducta delictiva[30].

---

26. Véase, en la doctrina española, entre otros, MORANT VIDAL, *Protección penal de la intimidad frente a las nuevas tecnologías*, p. 42; o ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática,* pp. 13 ss.

27. Así, GONZÁLEZ DE CHAVES CALAMITA, "El llamado delito informático", pp. 45 ss.; MATA Y MARTÍN *Delincuencia informática y Derecho Penal*, pp. 21 ss.; y ROMEO CASABONA, "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal" pp. 6 ss.

28. Por todos, ÁLVAREZ VIZCAYA, "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la Red", p. 257.

29. Véase BAÓN RAMÍREZ, "Visión general de la informática en el nuevo Código Penal", p. 88; MONTERDE FERRER, "Especial consideración de los atentados por medios informáticos contra la intimidad y privacidad", p. 196; o PÉREZ LUÑO, *Manual de informática y Derecho*, p. 75.

30. Así, por ejemplo, CHOCLÁN MONTALVO, "Infracciones patrimoniales en los procesos de transferencia de datos", p. 69, definiendo la "criminalidad informática" como el conjunto de "actos, antijurídicos según la ley penal vigente, realizados con el empleo de un equipo automático de procesamiento de datos".

V. CIBERDELITOS

Con la expansión mundial de Internet desde algunos sectores se ha confirmado que ésta facilita la comisión de delitos, aunque su consolidación no haya implicado la aparición de nuevas conductas antisociales o ilícitas. Las clásicas figuras delictivas, ya presentes antes de su irrupción en nuestra realidad diaria, simplemente se han encontrado con un nuevo canal o medio que facilita enormemente su comisión, aunque también su persecución y enjuiciamiento[31].

Ello no obstante, la generalización del uso de Redes de transmisión de datos, en realidad sobre todo de Internet, ha favorecido la utilización de nuevos conceptos en los análisis de lo que puede considerarse es el Derecho Penal informático, al menos en sentido si no conceptual, sí descriptivo. Así, un sector de la doctrina empieza a prescindir incluso del término delito informático (o delincuencia informática, si se niega la existencia de aquél) para sustituirlo por otros como ciberdelito, ciberdelitos, cibercriminalidad, etc.

El término "cibercrimen" se ha señalado que describe "el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual"[32]. Estaríamos ante una nueva generación de delitos, que en lugar de tener una vinculación con los sistemas informáticos, o, mejor, además de tenerla, se caracterizan por la vinculación que tienen con el uso de redes de transmisión de datos, siendo su relación con los sistemas informáticos secundaria respecto a la que tienen con las redes de transmisión de datos. Es, por eso, esta vinculación con las Redes de transmisión de datos lo que les otorgaría su carácter específico[33].

En todo caso, no puede negarse que todo lo que es cibernético o telemático es también, al mismo tiempo, informático, mientras que no ocurre lo mismo en sentido inverso, siendo por tanto mucho más omnicomprensiva esta última categoría.

VI. POSIBLES BIENES JURÍDICOS EN EL DELITO INFORMÁTICO

A pesar de las discrepancias doctrinales ya comentadas en torno a la existencia o no de un concepto de "delito informático", cada vez son más las voces doctrinales que en el ámbito de la delincuencia informática sostienen la necesidad de creación de una nueva categoría jurídico penal que abarque las conductas vinculadas con el hecho informático, entendiendo que no estamos sólo –o no en absoluto– ante la lesión de bienes

---

31. Véase, por todos, FERNÁNDEZ TERUELO, "La sanción penal de la pornografía infantil a través de Internet", p. 250.

32. Expresamente, ROMEO CASABONA, "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", p. 11. Algún autor, como TOSATO, "Panorama di giurisprudenza sui reati informatici", p. 446, ha utilizado, en lugar de la expresión "ciberdelito", el término "delito cuasinformático" para referirse a la misma realidad delictiva.

33. Así, el propio ROMEO CASABONA, "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", p. 10.

jurídicos tradicionales, sino ante la lesión de un nuevo interés que merece ser objeto de atención también por el Derecho Penal.

Esta idea, extendida cada vez más entre los nuevos autores no conlleva, sin embargo, una unidad de criterio a la hora de entender cómo debe explicarse este interés y cómo debe definirse el bien jurídico penal a que pretende hacerse referencia. Las distintas posturas al respecto, no siempre tan divergentes, son básicamente las siguientes.

1. La Seguridad Informática

La primera de las interpretaciones hace hincapié en la seguridad informática como bien jurídico colectivo a tutelar, objeto de ataque con las conductas vinculadas a la cuestión informática. Se trata de un bien, se dirá, cuya protección evita la lesión de una serie de bienes jurídicos de carácter individual puestos en peligro con tales conductas atentatorias contra la seguridad de las redes y sistemas informáticos, pero no siempre efectivamente dañados[34]. La extensión en el uso de redes y sistemas informáticos, se dirá en otros términos, imprescindibles hoy para el desarrollo económico y social, para el correcto funcionamiento del ámbito tanto público como privado, hace que la protección de su seguridad sirva como medio para proteger otros bienes de carácter individual (patrimonio, intimidad, libertad sexual, honor, etc.) e, incluso, otros bienes de carácter supraindividal (orden público, paz pública, seguridad del Estado)[35]. Pero es esta expansión y dependencia social de las TICs las que hacen que un ataque a ellas deba ser considerado en sí mismo como un ataque a un nuevo bien jurídico colectivo. Cuando se daña un sistema informático concreto, se señala, no sólo se daña un bien jurídico individual, sino que se generan riesgos para toda la comunidad de usuarios[36].

Se trata, por tanto, de un bien jurídico de naturaleza colectiva, indisponible, como tal, por el individuo concreto, que no encuentra suficiente protección mediante la salvaguarda en exclusiva de bienes jurídicos de naturaleza individual, pues muchas veces, al margen de otras consideraciones, no existirá la voluntad lesiva de dañarlos de manera efectiva, lo que no empece que pueda entenderse idóneo un adelantamiento de las barreras de protección a la de meras situaciones de peligro para lo cual esta perspectiva pude ser eficaz[37].

---

34. Véase CARRASCO ANDRINO, "El acceso ilícito a un sistema informático", pp. 342 ss., basándose en la legislación europea e internacional en materia de delincuencia informática.

35. Así, DEL MORAL TORES, en "El coste del delito informático", p. 89.

36. En este sentido, CARRASCO ANDRINO, "El acceso ilícito a un sistema informático", p. 344, destacando, además de este carácter instrumental de la seguridad informática como medio de tutelar otros intereses, la insuficiencia de los ordenamientos actuales para abordar la protección de nuevos riesgos que no cubre en sí la de tales intereses individuales; véase también MORILLAS FERNÁNDEZ, en *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet*, pp. 109 ss.

37. Extensamente, PICOTTI, "Sistematica dei reati informatici, tecniche di formulacione legislativa e beni girudici tuttelati", pp. 70 ss.

2. Integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos

En un sentido bastante similar, otros autores hablan de la necesidad de proteger la integridad, confidencialidad y disponibilidad de los sistemas informáticos y de los datos contenidos en ellos.

Se toma en consideración la informatización de todos los datos, tanto pública como privada, y la necesidad de poder confiar en su autenticidad y en su disponibilidad plena como garantía para un desarrollo económico y social acorde a los tiempos actuales. Esto es lo que garantizaría la tutela de la incolumidad de los datos, de su libre disposición y de su mantenimiento en los términos en que los ha configurado su titular, bien jurídico también de carácter supraindividual que adelanta la intervención penal en cuanto al mismo tiempo es instrumental respecto de otros bienes jurídicos que pueden verse dañados o en peligro con el menoscabo de la accesibilidad, integridad o confidencialidad de determinados datos[38].

3. Intimidad informática

La consideración del bien jurídico intimidad informática –*habeas data* o autodeterminación informática– se ha contemplado de un modo especial en la doctrina italiana –téngase en cuenta que en este ordenamiento se contempla el delito de acceso abusivo a un sistema informático, sin ulterior lesividad, ya desde el año 1993–, que entiende que lo que ha de protegerse frente a esta clase de conductas vinculado al hecho informático es, principalmente, el bien jurídico individual "intimidad e inviolabilidad informáticas", como una nueva vertiente, si se quiere, de lo que es el domicilio físico de cada persona. Ello sin perjuicio de que además se reconozca que la protección haya de ir encaminada a garantizar, también, la seguridad y la integridad de los sistemas informáticos, es decir, la seguridad informática[39].

La intimidad informática –por algunos denominada libertad informática– se plantea como bien jurídico autónomo y diferenciado, de naturaleza estrictamente informática, merecedor y necesitado de protección penal específica. Su contenido central vendría dado por el derecho del individuo a decidir qué información personal se puede difundir sobre él y su familia y cuál pueda ser el destino de esta difusión. Pero, en realidad, estamos ante un derecho complementario del que tradicionalmente trata de garantizar la tutela de la intimidad en su sentido más amplio, simplemente vinculado al desarrollo concreto de la informática.

En todo caso, y esto es lo importante frente a otro tipo de posturas, no se trata sólo de reconocer el derecho de excluir a los demás de un determinado ámbito que el titular considera reservado y que ha de protegerse frente a intromisiones indeseadas, sino de un poder positivo de control sobre la información personal que los demás pueden tener de cada uno y sobre el uso que puedan hacer de la misma. Por eso se

---

38. RODRÍGUEZ MORULLO/ALONSO GALLO/LASCURAÍN SÁNCHEZ, "Derecho Penal e Internet", pp. 259 ss.

39. Véase FLOR, "Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concurso nel reato da parte dell'extraneus", pp. 1518 ss.

entiende necesario este nuevo concepto, entendiendo que lo que pretende abarcar no está suficientemente garantizado ni por los tradicionales medios de tutela de la propiedad o la posesión de las cosas materiales, ni por la protección prestada al secreto, a la intimidad personal y domiciliaria o a otro tipo de bienes inmateriales[40].

4. Otras propuestas

En un sentido parecido se apunta como nuevo bien jurídico de carácter supraindividual característico de los delitos informáticos la confianza en el funcionamiento de los sistemas informatizados. Como ya se ha mencionado en relación a las propuestas que aluden a la idea de la seguridad informática, los delitos vinculados con la informática no sólo dañan en su comisión bienes jurídicos individuales y concretos; su comisión también pone en peligro la confianza de la sociedad en el buen funcionamiento de los sistemas informáticos y de las redes de transmisión de datos. La gravedad de este quebrantamiento de confianza radica, precisamente, en la dependencia de la sociedad actual respecto de las TICs para el desarrollo personal, económico y social de los individuos[41].

QUINTERO OLIVARES afirma, por su parte, que la tecnología de Internet es en sí misma un nuevo bien jurídico a proteger por el ordenamiento; un nuevo bien jurídico de primera magnitud, dirá[42].

ROVIRA aludirá a la información sobre la información como nuevo bien jurídico supraindividual, primordial y básico en su opinión –aunque matizando que no será el único que lesionen las conductas vinculadas con la informática–, que trata de garantizar el acceso y conocimiento de la información que uno posee y que permite calificar todas las conductas que atenten contra ella como delitos informáticos[43].

Y ROMEO CASABONA, en propuesta de *lege ferenda* respecto a algunas conductas vinculadas con las nuevas tecnologías que aun no tienen cabida en nuestro Código Penal, acude a la expresión "comunicación pacífica a través de las redes telemáticas, con independencia de las garantías y protección que puedan ofrecerse a otros bienes jurídicos como la intimidad y los datos de carácter personal" para intentar definir un nuevo objeto de tutela, en el afán, dirá, de ofrecer una protección jurídica más intensa, entre otras, a las comunicaciones personales en cuanto tales, así como a las actividades de producción y consumo de información en las redes[44].

Se ha destacado asimismo que mediante el delito informático se dañan bienes tanto personales como patrimoniales y que, sin reconocer con ello que estemos ante conductas que atenten contra un específico bien jurídico, nos encontramos por ello

---

40. Ampliamente, PICOTTI, "Sistematica dei reati informatici, tecniche di formulacione legislativa e beni girudici tuttelati", *Il diritto penale della informatica nell'epoca de internet*, pp. 78 ss.

41. *Véase* CORCOY BIDASOLO, "Problemática de la persecución penal de los denominados delitos informáticos", pp. 9 s.

42. QUINTERO OLIVARES, "Internet y propiedad intelectual", p. 375.

43. ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, pp. 70 ss.

44. ROMEO CASABONA, "Los datos de carácter personal como bienes jurídicos penalmente protegidos", pp. 189 ss.

ante una categoría penal autónoma en la que el objeto de protección coincide no obstante con el de los tipos tradicionales que están siendo adaptados a las nuevas tecnologías[45].

VII. DISTINCIÓN ENTRE DELITOS COMETIDOS A TRAVÉS DE LA INFORMÁTICA Y DELITOS COMETIDOS CONTRA LA INFORMÁTICA

Sigue siendo frecuente, con todo, la distinción de muchos autores entre delitos relacionados con la informática en cuanto ésta constituye medio idóneo para la realización de los mismos y delitos en los que la informática es objeto del delito o la infracción, como ya se ha expuesto en las líneas anteriores, incluyendo en el concepto de delito informático tanto unos como otros[46] o, por el contrario, sólo unos u otros[47].

Esta distinción, la más frecuente, no impide reconocer, sin embargo, un tercer grupo de delitos que hace referencia a los otros dos, en cuanto en ocasiones nos encontramos con delitos cometidos contra y a través de los sistemas informáticos e incluso un cuarto en el que podrían incluirse los delitos contra la propiedad intelectual de nuevos bienes de naturaleza informáticos (propiedad intelectual e industrial de programas, nombres de dominio, topografías de productos semiconductores, etc.)[48].

Es cierto que estas distinciones pueden servir para hacer una exposición más clara de los delitos que en su comisión, sea por el medio, sea por el objeto o sea por ambos, tienen una vinculación con los sistemas informáticos. Pero también lo es que las mismas no terminan de abordar el problema de la concreción de un delito informático con un bien jurídico concreto a proteger frente al mismo y que, en este sentido, no acaba de tener sino una validez de exposición del conjunto de conductas a tener en cuenta sin que acabe de abordar, sin embargo, cuáles de ellas puede entenderse atentan contra algo que sea realmente nuevo, no en su realidad, pero sí al menos en cuanto a su necesidad de tutela penal[49].

VIII. CONCLUSIÓN

Dada la extensión del uso de los ordenadores y de las redes de transmisión de datos en la mayoría de ámbitos de nuestra sociedad, todos o prácticamente todos los delitos pueden cometerse a través de un sistema informático; en este sentido, las conductas ilícitas vinculadas con los sistemas informáticos son muchas y heterogéneas.

---

45. Así, por ejemplo, GARCÍA GARCÍA-CERVIGÓN, "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", pp. 291 s.

46. Expresamente, JOVER PADRÓ, "El Código Penal de la informática", p. 350.

47. Véase CHOCLÁN MONTALVO, "Infracciones patrimoniales en los procesos de transferencia de datos" p. 69.

48. Clasificación utilizada a fin de poder ofrecer una sistemática visión lo más completa posible de todos los delitos vinculados a las TICs por DE LA MATA BARRANCO, "Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general", pp. 49 ss.

49. Véase RODRÍGUEZ MOURULLO/LASCURAÍN SÁNCHEZ/ALONSO GALLO, "Derecho Penal e Internet", *Régimen jurídico de Internet*, pp. 259 ss.

Puede aceptarse también la existencia de una categoría criminológica que englobe las conductas penalmente relevantes vinculadas a la informática, que, sin mayores precisiones, cabe denominar "delincuencia informática", pero sin que la expresión indique otra cosa que la referencia a un modo criminal de actuación, propio de los nuevos tiempos, en las que los autores del delito se sirven de modos de comisión diferentes de los tradicionales, lo que conlleva que puedan tratar de predicarse diferentes características tanto de ellos, como de posibles víctimas, aspectos procesales a considerar, etc.

En todo caso, ello no impide que, al mismo tiempo, pueda intentar considerarse la posibilidad de profundizar en la definición de un nuevo bien jurídico, vinculado con la digitalización de la información, susceptible, merecedor y necesitado de tutela penal, dada la trascendencia que en nuestra sociedad actual están adquiriendo los ordenadores, en sus diferentes manifestaciones, para el desarrollo individual, económico y social de sus ciudadanos.

La idea de un bien jurídico sustantivo vinculado al hecho informático no va a suponer que cualquier conducta delictiva relacionada con las nuevas tecnologías deba necesariamente suponerse lesiona este bien jurídico y, por tanto, ser ubicada entre los delitos informáticos. Muchas de las conductas que sin duda pueden incluirse entre lo que es la delincuencia informática, como categoría criminológica, dañan únicamente bienes jurídicos tradicionales, bien es cierto que a través de nuevos medios más sofisticados, pero nada más.

Otras conductas, en cambio, sí implican algo más: ese menoscabo que tratan de explicar quienes aluden a los nuevos intereses que menoscaba quien atenta contra sistemas o datos informáticos, que deberá concretarse, en mi opinión, teniendo en cuenta sobre todo la necesidad de garantizar la integridad, confidencialidad y accesibilidad de los mismos, que de alguna manera es lo que todos los autores, con diferencias de matiz, tratan de tener en cuenta desde sus diferentes posturas. Sin perjuicio de aceptar que, además, las conductas a considerar puedan dañar otros intereses tradicionalmente objeto de atención en sede penal, lo que no siempre, sin embargo, tendrá que ocurrir (así, por ejemplo, de aceptarse la necesidad de su punición, en el caso del *hacking* blanco o de ataques *DOS)*.

Parece existir, en síntesis, una categoría criminológica que puede denominarse criminalidad informática, delincuencia informática o delitos informáticos, que incluye todas las conductas sancionadas por el Código Penal que tengan vinculación con la informática bien en su medio comisivo, bien en el objeto sobre el que recae la conducta, bien en ambos u otros ilícitos que en su momento puedan entrar a formar parte de él. Pero también es posible, y parece que aconsejable, insistir en el estudio sobre la conveniencia de proteger también un nuevo bien jurídico vinculado a lo informático, que todavía no aparece claramente definido en la legislación penal pero a favor del cual parece apostar cada vez más la doctrina que se ha detenido en estas cuestiones.

IX. BIBLIOGRAFÍA

ÁLVAREZ VIZCAYA, M.: "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red", en *Cuadernos de derecho judicial*, 10, 2001, 255-280.

BAÓN RAMÍREZ, R.: "Visión general de la informática en el nuevo Código Penal", en *Cuadernos de derecho judicial*, 11, 1996, 77-100.

BEQUAI, A.: *Computer Crime*, Massachussetts, 1978.

BEQUAI, A.: *White-Collar Crime: a 20th-Century Crisis*, Massachusetts, 1978.

CAMACHO LOSA: *El delito informático*, Madrid, 1987.

CARRASCO ANDRINO, M.M.: "El acceso ilícito a un sistema informático", en *La adecuación del derecho penal español al ordenamiento de la Unión Europea. La política criminal europea*, Valencia, 2009, 341-365.

CHOCLÁN MONTALVO, J. A.: "Infracciones patrimoniales en los procesos de transferencia de datos", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 69-95.

CONSEJO DE EUROPA: *Organised crime in Europe: the threat of cybercrime. Situation report 2004*, Francia, 2005.

CORCOY BIDASOLO, M.: "Problemas de la persecución penal de los denominado delitos informáticos", en *Eguzkilore*, 21, 2007, 7-33.

DE LA MATA BARRANCO, N.J.: "Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general", en *Delito e informática: algunos aspectos*, Bilbao, 2007, 41-82.

DEL MORAL TORES, A.: "El coste del delito informático" en *Cuadernos de la Guardia Civil: Revista de seguridad pública*, 23, 2001, 85-92.

DI GIORGI, R. M./RAGONA, M.: "L'informatica giuridica" en *L'informatica del diritto*, Milano, 2004, 3-17.

FERNÁNDEZ TERUELO, J. G.: "La sanción penal de la distribución de pornografía infantil a través de Internet" en *Boletín de la Facultad de Derecho de la UNED*, 20, 2002, 249-276.

FERREYROS SOTO, C.: "Aspectos metodológicos del delito informático" en *Informática y derecho: Revista iberoamericana de derecho informático*, 9-11, 1996, 407-412.

FLOR, R.: "Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'extraneus", en *Cassazione Penale*, 2009, 4, 1509-1525.

GARCÍA GARCÍA-CERVIGÓN, J.: "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", en *Icade: Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales*, 74, 2008, 289-308.

GONZÁLEZ DE CHAVES CALAMITA, M. E.: "El llamado delito informático", en *Anales de la Facultad de Derecho*, 21, 2004, 45-65.

GONZÁLEZ RUS, J.J.: "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en *Revista de la Facultad de Derecho de la Universidad Complutense*, 12, 1986, 107-164.

GONZÁLEZ RUS, J.J.: "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", en *Cuadernos penales José María Lidón*, 4, 2007, 13-41.

GUTIÉRREZ FRANCÉS, M.L.: *Fraude informático y estafa*, Madrid, 1991.

IASELLI, M.: *Informatica giuridica*, Napoli, 2002.

JOVER PADRÓ, J.: "El Código Penal de la informática", en *X años de encuentros sobre informática y derecho, 1996-1997*, Pamplona, 1997, 349-370.

MARTINO, A.A.: en "Informatica e Diritto: farfugliato, imbricato rapporto", en *Informatica giuridica. Nuove tematiche di diritto dell'informatica ed Internet*, Napoli, 2001, 7-33.

MATA Y MARTÍN, R. M.: *Delincuencia informática y Derecho penal*, Madrid, 2001.

MONTERDE FERRER, F.: "Especial consideración de los atentados por medios informáticos contra la intimidad y privacidad", en *Cuadernos de derecho judicial*, 3, 2006, 191-266.

MORALES PRATS, F.: *La tutela penal de la intimidad: privacy e informática*, Barcelona, 1984.

MORANT VIDAL, J.: *Protección penal de la intimidad frente a las nuevas tecnologías*, Valencia, 2003.

MORILLAS FERNÁNDEZ, D.L.: *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet*, Madrid, 2005.

ORTS BERENGUER, E./ROIG TORRES, M.: *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia, 2001.

PARKER, D.B.: *Crime by computer*, New York, 1976.

PÉREZ LUÑO, A.E.: *Manual de informática y Derecho*, Barcelona, 1996.

QUINTERO OLIVARES, G.: "Internet y propiedad intelectual", en *Cuadernos de derecho judicial*, 10, 2001, 367-398.

RODRÍGUEZ MOURULLO, G./LASCURAÍN SÁNCHEZ, J.A./ALONSO GALLO, J.: "Derecho Penal e Internet", en *Régimen jurídico de internet*, Madrid, 2001, 257-310.

ROMEO CASABONA, C. M.: *Poder informático y seguridad jurídica*, Madrid, 1988.

ROMEO CASABONA, C. M.: "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 1-42.

ROMEO CASABONA: "Los datos de carácter personal como bienes jurídicos penalmente protegidos", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 167-190.

ROVIRA DEL CANTO, E.: *Delincuencia informática y fraudes informáticos*, Granada, 2002.

SIEBER, U.: *Computerkriminalität und Strafrecht*, Köln, 1980.

SIEBER, U.: *The International Handbook on Computer Crime*, Chichester, 1986.

SIEBER, U.: *La délinquance informatique*, Bruxelles, 1990.

TIEDEMANN, K.: *Poder económico y delito*, Barcelona, 1985.

TIEDEMANN, K.: "La criminalidad económica como objeto de investigación", en *Cuadernos de Política Criminal*, 19, 1983, 171-184.

TOSATO, L.: "Panorama di giurisprudenza sui reati informatici", en *L'Indice penale*, 2001, 1, 445-462.

ZICCARDI, G.: "Il diritto dell'informatica", en *Manuale di diritto dell'informatica e delle nuove tecnologie*, Bologna, 2000, XIII-XVI.

ZICCARDI, G.: "Il diritto dell'informatica", en *Manuale di diritto dell'informatica e delle nuove tecnologie*, Bologna, 2000, 323-355.