DELITOS CONTRA EL SISTEMA O POR MEDIOS INFORMÁTICOS

Por
Virginia Arango Durling
Catedrática de Derecho Penal
Universidad de Panamá

I. INTRODUCCIÓN

En el derecho comparado se sanciona la delincuencia informática, ya sea cuando se trate de actos que atentan contra los medios informáticos, o por el contrario cuando se realizan por los medios informáticos (González Rus, p.130).

En el primer supuesto, estamos ante hechos que atentan contra los *elementos físicos del sistema informático (hardware, monitores, dispositivo de almacenamiento de diskettes, cintas, discos, de comunicación etc.) y a elementos lógicos (ficheros, datos y no programas) del sistema informático*, es decir, que son hechos que afectan la información almacenada, son en esencia actos que se persigue tutelar el contenido de la información de un sistema y no el hardware (Jijena Leiva, p. 83), y que han sido considerados en esencia como delitos de naturaleza informática.

Por su parte, los delitos cometidos por medio del sistema informático, son *los instrumentos o el medio en que se vale el sujeto para la realización del delito, como* por ejemplo, estafas, falsificaciones, delitos contra la intimidad, entre otros.

Entre los delitos contra los medios informáticos, podemos mencionar, el Acceso no autorizado al sistema de procesamiento de datos o uso no autorizado de computadora, la fabricación, tenencia y circulación de dispositivos técnicos dirigidos a desproteger programas de ordenador, el

delito de Sabotaje Informático, el espionaje informático, Espionaje de datos y los Fraudes Informáticos.

Desde otra perspectiva, también se habla de delitos informáticos que suponen un ataque al orden económico y a la privacidad, mencionándose entre los primeros, los fraudes, la copia ilegal de software, el sabotaje informático, el robo de uso de sistema informático, mientras que en el segundo supuesto, se afecta la intimidad o privacidad del sujeto.

Lo que sí debe tenerse presente, que la denominación "delito informático", es susceptible de diversas conceptualizaciones, para algunos, se trata de delitos relacionados con ordenadores (Salt, p. 50), que comprenden la manipulación fraudulenta de los ordenadores, con fines de lucro, destrucción de banco de datos, copia de soportes lógicos, etc.. En otros casos, ha sido concebido como delitos electrónicos, es cualquier conducta criminal que haga uso de la tecnología, como *método,* es decir, instrumento mismo que la realiza la infracción, como *medio*, el sujeto se vale del objeto para cometer el delito, vgr. Lectura de información confidencial, o como *fin*, dirigido directamente a la entidad física o su material, vgr. Dañar la memoria, la quema de la computadora (Lima, Delitos, p. 175).

Antes de terminar, debe mencionarse que con anterioridad al Código Penal del 2007, era muy reducido el número de delitos por medios informáticos, sin embargo, con la nueva legislación se ha ampliado el ámbito de los delitos informáticos, como medio y contra los sistemas como veremos mas adelante.

II. NATURALEZA JURIDICA Y FUNDAMENTO DE LA INTERVENCION PENAL

En el derecho comparado las legislaciones han ido adecuando su normativa vigente a fin de contrarrestar la criminalidad informática en sus

diversas manifestaciones, pues es evidente que su afectación redunda en innumerables bienes jurídicos.

En sí puede partirse de que el *patrimonio* ha sido uno de los bienes jurídicos frecuentemente atacados, ante los supuestos de fraudes informáticos o en otros casos ante el sabotaje informático, por el enriquecimiento patrimonial que se ha obtenido por la manipulación de datos (Romeo Casabona, p.72), sin dejar de mencionar los ataques a la *intimidad*, por el acceso sin autorización a sistemas y la utilización ilegitima de los mismos (Jijena Leiva, p.30)

Además, la intervención penal se ha fundamentado para dar una respuesta a los constantes ataques a la *propiedad intelectual* por la reproducción, distribución u otras formas en contra de los programas de software (Busch, p.130), aunque para algunos se justifique su intervención pues los avances tecnológicos, presentan un ataque directo a la i*nformación* en si misma (Jijena Leiva, p.20).

Y es que tratándose de estos hechos, estamos ante titulares de una gran diversidad, la persona afectada en su intimidad personal en otro caso en su patrimonio, el Estado, en su seguridad informática, el autor, en los programas de software, entre otros.

De lo anterior se desprende que la tutela de estos delitos es compleja, ya que en ocasiones se trata de delitos por medios informáticos, por lo que la fórmula a la que se ha llegado es la de incorporarlos en las figuras existentes, en otro caso creando nuevos tipos penales que respondan a esta nueva forma de criminalidad, pues la naturaleza jurídica de estos no ha permitido individualizarlo en un solo bien jurídico.

No está demás decir, los problemas e inconvenientes en cuanto al objeto material que es diverso, y ya han quedado atrás las discusiones sobre la corporeidad de la cosa según anota González RUS (p.472), de manera que

estamos en ocasiones ante un objeto intangible o inmaterial, como son los datos, archivos (Rovira del Canto, p.225)

Todo lo antes expuesto, nos lleva a considerar que es indispensable su tutela penal, razón por la que acertadamente a partir del Código Penal del 2007 se hayan incorporado no solo los delitos por medios informáticos, sino también otras formas de criminalidad informática.

En tal sentido, se aprecia que se tutela la libertad e integridad sexual, el honor, la libertad y el patrimonio económico castigando una variedad de delitos por medios informáticos, al igual que sucede contra la seguridad colectiva, la fe publica y la personalidad jurídica del Estado, mientras que la tutela contra los medios informáticos, se efectúa a través de los "Delitos contra la seguridad jurídica de los medios informáticos".

III. DE LOS DELITOS CONTRA LOS MEDIOS INFORMÁTICOS EN EL DERECHO COMPARADO

A. Acceso no autorizado al sistema de procesamiento de datos o uso no autorizado de computadora

El acceso no autorizado al sistema y la lectura de ficheros o procesamiento de datos, se puede realizar con fines de obtener un provecho o de dañar a la víctima, ya sea para extorsionar, por sabotaje industrial o político, con fines de fraudes o atacar la intimidad) etc (Lima, p.32), y se trata de hechos de que por sí ya constituyen hechos punibles ya previstos en la ley, siendo la computadora solo un medio para su ejecución.

En sentido contrario, el acceso sencillamente es de paseo, por placer (joyriding, cometido por piratas juveniles (hacking), que quieren vencer el reto de un sistema de seguridad de una empresa, que si bien no tiene un fin ilícito, suele provocar innumerables pérdidas a las compañías por posibles bloqueos de sistema u otras deficiencias (Sieber, p.78).

Por otro lado, el acceso no autorizado a banco de datos puede revestir la forma de espionaje informático, y en otros casos ha consistido en delitos para sacar dinero de cajeros automáticos (Manfred Monhkenschlager, p.135), o en general realizar fraudes informáticos, cuando por ejemplo, una persona tiene acceso al cajero automático mediante la utilización de la tarjeta por un tercero, o cuando se tiene acceso mediante la utilización de una tarjeta falsa o alterada (Romeo Casabona, p.121 y ss.).

El acceso no autorizado ha merecido un interés en el derecho comparado, por los graves peligros que implican estos actos, de manera que se sancionen cuando recae sobre cuestiones de seguridad nacional, sobre instituciones financieras, agravando la pena cuando resultare supresión o modificación de las datos contenidos en el sistema, cuando se intercepta o acceda a un sistema de tratamiento de información de apoderarse, usar o conocer indebidamente la información.

Ahora bien el acceso indebido no autorizado o indebido a banco de datos, ficheros u otros, o en general los fraudes informáticos, pueden realizarse por diversos métodos que comprenden los siguientes:

- Introducción de datos falsos (data diddling)
- El caballo de Troya (Trojan horse)
- La Técnica de Salami (Rounding down)
- Superzapping
- Puertas falsas (Trap doors)
- Bombas lógicas (logic bombs)
- Ataques asíncronos (Asynchronous attacks)
- Recogida de información residual (scavenging)
- Divulgación no autorizada de datos reservados (data leakage)
- Piggybacking and impersonation
- Pinchado de líneas wiretapping

- Simulation and modeling
- Los Hackers. (Camacho, p.371)

De lo antes expuesto se desprende, que esta clase de hechos, requiere por lo menos de una serie de conocimientos en informática, en el manejo de ordenadores (Jijeiva Leiva, p.110), a los que se conoce en el mundo de la informática, como hackers, diferenciándolos de los crakers, que por el contrario causan daños informáticos (González Rus, p. 242).

Para terminar, el Código Penal del 2007, sanciona en el artículo 283, el acceso, el ingresar a una base de datos, red o sistema informático, es decir, que el sujeto lo hace de manera indebida o clandestina, castigándose con la pena de prisión de dos a cuatro años, que no es más que lo que se conoce como "intrusismo informático". Pero también, el código habla de *utilizar* una base de datos, etc. sin autorización, castigando así la mera intromisión, como por ejemplo, la lectura confidencial a los datos personales, violando en ambos casos las medidas de seguridad, pues debe quedar claro que en ambos supuestos no existe una finalidad de dañar, defraudar o manipular en el delincuente (Moron Lerma, p. 42).

B. Fabricación, tenencia o circulación de dispositivos técnicos dirigidos a desproteger o neutralizar programas de ordenador

El legislador español sanciona como tipo alternativo (art. 270) estas tres modalidades ejecutadas con fines comerciales y de duplicación de programas de ordenador (reproducción, instalación de copias), ejecutadas sin autorización de su titular, que lesionan la propiedad intelectual relacionada con ficheros de datos y programas de ordenador de CARMONA y otros, p.780).

La tenencia de copias ilegales o de copiones informáticos cuyo destino particular, es civilmente ilegítimo, ha indicado QUERALT, (p.422) que no es constitutivo de delito alguno contra la propiedad intelectual, mientras esto no se ponga en circulación, y agrega el autor que no se ve la razón que pudiera llevar a castigar la tenencia de una copia ilegal de un programa de ordenador y no la de un libro, y en consecuencia, esa tenencia debe entenderse con fines comerciales.

Con toda razón sostienen GONZÁLEZ RUS y otros (p.78l) "que la intervención penal ha ido demasiado lejos", y que el actual art. 270 (III), llevaría a castigar la "mera tenencia" sin ánimo de lucro ni perjuicio a tercero, por cualquier usuario que los emplee exclusivamente para uso privado, de manera que aunque expresamente no se requiere debe exigirse y estar implícito el animo de lucro tanto en la fabricación como en la circulación.

En efecto, se ha adelantado la intervención penal para ciertas conductas "fabricación y puesta en circulación" e incluso la de mero acto preparatorio de la tenencia respecto de cualquier medio técnico "copiones" informáticos. No cabe duda de que el Código penal ha ido en esta materia más de la que la propia protección civil de los programas de ordenador (Jorge Barreiro y otros, p. 775, Muñoz Conde/ García Aran.).

Finalmente, no debe tenerse comprendido en estas acciones, aquellos actos de desproteger programas que incluyen otras acciones distintas (comprensión/ descomprensión de ficheros, encriptación, desencriptación, comparar, formateos especiales, etc.)

C. Sabotaje informático

Se entiende por sabotaje desde el punto de vista clásico (Villalobos p.150) como el "acto deliberado e intencional encaminado a causar daños

en instalaciones, maquinarias, materias primas y mercancías", es decir, la destrucción total de un sistema o de sus programas por un incendio provocado, que en el caso de la informática, concretamente estamos hablando de la destrucción, limitación o alteración de la capacidad de los elementos informáticos realizados por virus, cáncer, programas borradores, etc, hecho que aparece comprendido en el nuevo código Penal del 2007 (art.224).

También se ha señalado que el sabotaje informático comprende todas aquellas conductas dirigidas a atacar los sistemas informáticos, ya sea que se dirijan a causar daños en el hardware o en el software (Salt, p. 52) mediante incendios, explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en el equipo, etc., es decir un comportamiento encaminado a la destrucción física que es similar a cualquier acto análogo a la destrucción de otra clase de objetos.

Estamos pues, desde el punto de vista de la técnica informática es una modalidad de conducta que causa destrozos lógicos, o sea todas aquellas conductas que producen como resultado la destrucción, ocultación o alteración de datos en un sistema informático (Salt, p. 53), que pueden comprender borrar documentos de archivo, desenchufar el ordenador de la electricidad mientras se esta trabajando o en confeccionar programas conocidos como virus informático, con crash programs, borrado mediante imanes, etc.(Sieber, p.76).

En general, pues el sabotaje informático provoca de manera popular daños al sistema lógico, con uso de crash programs, programas destructores, cáncer de rutinas, bomba de tiempo, que consumen en poco tiempo el programa, los programas virus, el borrado de datos mediante imanes, etc.(Sieber, p.76)..

En el caso de nuestro país, el sabotaje informático, de manera técnica, no tenemos conceptualizado este delito, pues constituye una forma agravada del delito de daño, considerándose como un hecho atentatorio contra el patrimonio económico, en la que a nuestro modo de ver, no se trata en si de un daño a la cosa mueble en si, sino de un daño a los datos, archivos, o programas, en general, a la información contenida en la misma.

En efecto, el legislador se refiere al daño ocasionado por medios informáticos, expresión amplia, que puede provocarse por el uso de programas destructores (virus informático), entre otros, y en la cual el sujeto lo efectúa con el ánimo de inutilizar , dañar o modificar los datos.

Lamentablemente, este hecho debió haberse configurado de manera autónoma, haciendo alusión a los actos constitutivos del sabotaje informático, como son: borrar, suprimir, inutilizar, modificar, como así se refiere el derecho comparado., ya que como afirma Salt estamos ante un delito de daño. a falta de disposición especial al respecto, pues en opinión de este autor, en el caso de los datos lógicos de un sistema considerado como de naturaleza intangible, no alcanza su protección penal, y sea necesario para ello como ha sucedido en otros países destinarle una protección especial mediante los actos de destrucción alteración ocultación o cancelación de datos.

En este sentido, se refiere la doctrina a las agresiones a los sistemas o elementos informáticos, el denominado Sabotaje informático y las agresiones al soporte material (Romeo Casabona, p.175), que tienen por objeto causar un perjuicio patrimonial en el usuario del ordenador empresas, entidades bancarias u otras, sin dejar de mencionar aquellas que tienen fines políticos contra la seguridad y defensa de los Estados, por ejemplo sobre el armamento y organización operativa de las fuerzas armadas, ficheros de la policía. etc.

Así ha entendido ROMEO CASABONA, (p.177), que la incriminación de estas conductas a través del delito de daño plantea problemas cuando radica en el soporte lógico no físico, incorporal del sistema informático, aunque se llegue a la conclusión de la punibilidad a través del delito de daños, sin embargo, considera que es necesario una intervención del legislador para una mejor cobertura penal de estas conductas y además para fijar penas más adecuadas al desvalor de estos actos.

En conclusión, los actos ejecutados con fines de ocasionar efectos nocivos a un sistema informático, son constitutivos de un delito de daños (Queralt, p.423), según así lo ha entendido la doctrina, y pueden recaer sobre la figura del delito de incendio cuando la destrucción recaiga sobre los elementos lógicas del sistema y su aspecto físico.

IV. LOS DELITOS CONTRA LA SEGURIDAD JURIDICA DE LOS MEDIOS INFORMATICO.

A. Determinaciones previas

El Código Penal de 1982, contenía de manera limitada delitos informáticos, entre los que podemos mencionar los delitos cometidos por tarjetas de crédito, la pornografía infantil, y los delitos financieros.

De conformidad con la nueva legislación penal del 2007, se contempla en el Capítulo I “Delitos contra la seguridad Informática” del titulo VIII, los “Delitos contra la Seguridad jurídica de los medios electrónicos”, y siguiendo su tenor literal debe interpretarse que el bien jurídico tutelado es la “seguridad informática”, que se manifiesta en el interés del Estado por castigar a través de una pluralidad de figuras delictivas la injerencia de terceros a medios electrónicos(medios informáticos que tienen informaciones en base de datos, red o sistema informático, que están

reservados a sus titulares, por razón de la función o actividad que realizan, las cuales deben ser mantenidas de manera confidencial, y con un acceso restringido.

B. De las diversas figuras delictivas

1. Acceso e utilización indebida

El nuevo Código Penal, castiga la intromisión en una base de datos, red o sistema informático en el artículo 285, de la siguiente manera:

"Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión"

Se sanciona el *acceso ilegal* y la *utilización indebida* de base de datos, red o sistema informático, efectuada tanto por un intruso, como por la persona encargada de la base de datos o sistema informático hecho que puede ser efectuado de manera clandestina, abusiva o ilícita, violando las medidas de seguridad como por ejemplo, las claves de entrada dispuestas para impedirlo (Arboleda Vallejo/Ruiz Salazar, p. 189).

Estamos ante un acceso ilícito a los sistemas informáticos (piratería informática) cuyo fenómeno se conoce como "hacking", en la que se realicen una serie de comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicación electrónica de datos, sino también a la utilización de los mismos sin autorización o mas allá de lo autorizado (Moron Lerma, p. 42)

Se trata de un comportamiento realizado por placer (hackers), sin ánimo de espiar, solo de pasear, por lo que el legislador, en este caso ha adelantada la protección penal, por los peligros que implica la intromisión a la base de datos, sistema informático, que resguardan datos, castigando así la mera lectura de la información confidencial contenida en una base de datos de oficinas publicas o bajo su tutela, en instituciones publicas o privadas, o mixtas que prestan un servicio publico y en bancos, aseguradores y demás instituciones, financieras o bursátiles, sin que se requiera para ello ningún

propósito en particular, claro que si se realiza con fines lucrativos se agrava la pena (art. 287). Finalmente, debe quedar claro que no queda comprendido en esta norma los daños a los datos que se provoquen, pues estos encajan en el delito de daños agravado por sabotaje informático.

2. *Apoderamiento, copia, utilización, o modificación de datos en transito o contenidos en una base de datos o sistema, y la Interferencia, obstaculización o el impedir su transmisión.*

El artículo 286 dice lo siguiente:

> "Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión".

Se sanciona el *apoderamiento indebido* de los datos en tránsito contenidos en una base de datos o sistema informático, que básicamente es una especie de hurto, que en sentido tecnológico implica el tomar los datos ajenos contenidos en una base de datos, por ejemplo.

Pero también, la norma castiga el acto de *copiar*, que debe efectuarse a través de los procedimientos tecnológicos, es decir, se duplica o reproduce sin la alteración o destrucción de la base de datos, que en este último caso, ha sido identificado como espionaje de datos informáticos.

No queda comprendido aquí la copia ilegal de software, que es un atentado contra la propiedad intelectual.

De igual forma, es posible que el sujeto *utilice los datos contenidos en el sistema informático o en una base de datos,* sin que para ello se exija una finalidad especial, pero si se hace con fines lucrativos se aumenta la pena (art. 287).

Por lo que respecta a la *modificación*, no es mas que la transformación o el cambio de la información en la base de datos y constituye un ataque contra

los medios informáticos pues la información almacenada queda afectada constituyendo un delito contra la violación de la integridad de los datos y de los sistemas.

En cuanto al artículo 286, se castiga también la *Interceptación* ilegal en la base de transmisión y otros comportamientos con términos distintos interferir, interceptar, obstaculizar o impedir que son expresiones sinónimas, que tienen en común, la de impedir su transmisión, es decir, el funcionamiento del sistema de información y que implican por consiguiente su interrupción, a través, por ejemplo, de la cancelación, alteración de datos informáticos, o su conversión en inaccesibles, que necesariamente debe realizarse por medios técnicos, por ejemplo un e-mail bombing o un ataque a un sitio web.

Por otro lado, debe tenerse presente que le son aplicables las agravantes previstas en el artículo 287, de un tercio a una sexta pare de la pena si se cometen contra datos contenidos en bases de datos o sistema informático de:

Oficinas públicas, o bajo su tutela, instituciones públicas, privadas o mixtas que prestan un servicio público, bancos, aseguradoras y demás instituciones financieras y bursátiles, o cuando fueren cometidos con fines lucrativos.

Por último, el artículo 287 determina que las penas previstas en este capítulo se aplicaran independientemente de lo previsto en el título XIV, cuando se trate de información confidencial de acceso restringido referente a la seguridad del Estado,

BIBLIOGRAFÍA

ABOSO Gustavo Eduardo/ ZAPATA, Maria Florencia, **Cibercriminalidad y Derecho Penal,** Editorial B. de F. Buenos Aires, 2006

ALTMARK, Daniel/ BIELSA, Rafael. **Informática y Derecho**, **Aportes de Doctri**na **Internacional,** Depalma, Buenos Aires, 2002.

ALVAREZ, José Ma./ CIENFUEGOS SUÁREZ, **La defensa de la intimidad de los ciudadanos y la tecnología informática avanzada**, Aranzadi editorial, Pamplona, 1999.

ARBOLEDA VALLEJO, Mario/ RUIZ SALAZAR, José Armando, **Manual de Derecho Penal, Parte Especial,** Leyer, Bogota, 2001

BAJO FERNÁNDEZ, Miguel, **Compendio de Derecho Penal** (Parte Especial) Volumen III, Editorial Centro de Estudios Ramón Areces, S.A. Madrid, 1998

BUSCH, Cristina, **La protección penal de los derechos de autor en España y Alemania, C**edecs, Barcelona, 1995.

BUSTAMANTE, Javier y otros, "Derechos Humanos en el ciberespacio", en **Derechos Humanos. La condición humana en la sociedad tecnológica**, Tecnos, Madrid, 1999.

CAMACHO, Luis, **El Delito informático. Un análisis en profundidad del mayor riesgo con que se enfrenta la sociedad moderna informatizada**, Gráficas Condor, Madrid, 1987.

CAMPUZANO TOMÉ, Herminia, **Vida privada y datos personales**, editorial Tecnos, Madrid, 2000.

CARMONA SALGADO, Concepción, **La nueva ley de propiedad intelectual**, editorial Montecorro S.A., Madrid, 1988.

CARMONA SALGADO, Concepción, "El tipo básico del nuevo delito contra la propiedad intelectual", en **Comentarios a la Legislación Penal,** tomo XII, Edersa, Madrid, 1991.

CORCOY , Mirentxu, "Protección penal del sabotaje informático. Especial consideración al delito de daños" en **Delincuencia Informática**, Barcelona, 1992.

CORCHO DÍAZ, Boris, **La responsabilidad civil y derechos del consumidor**, Editorial Portobelo, Librería Campus, Panamá, 2000.

CORREA, Carlos/ BALTO, Hilda/ CZAR DE ZALDIVIESO, Susana/ NAZAR ESPECHE, Félix,. **Derecho Informático**, ediciones De Palma, Bujenos aires,1994,

DAVARA RODRÍGUEZ, Miguel Ángel, **Manual de Derecho informático**, Thomson-Aranzadi, Navarra, 2003.

DEL MORAL, Octavio, **Almacenamiento tecnológico de documentos**, No.8, Editorial Portobelo, Panamá, 1998.

FERNÁNDEZ DELPECH, Horacio, **Internet: su problemática jurídica**, Abeledo-Perrot, Buenos Aires, 2001.

FERRE OLIVE, Juan Carlos, "Delitos contra los derechos de autor", en **Anuario de Derecho Penal y Ciencias Penales**, Tomo XLIV, enero-abril 1991.

GALÁN MUÑOZ, Alfonso, **El fraude y la estafa mediante sistemas informáticos (análisis del artículo 248.2C.P.,** tirant loblanch, Valencia, 2005.

GARCÍA-BERRIO HERNÁNDEZ, Teresa, **Informática y libertades. La protección de datos personales y su regulación en Francia y España**, Universidad de Murcia, 2003.

GIANNANTONINO, Ettore, **Manuale di diritto dell informatica**, Cedom, Padova, 2005

GONZÁLEZ MONTENEGRO, Rigoberto, **El Habeas Data**, Instituto de Estudios Políticos e Internacionales de Panamá, Panamá, 1999.

GONZÁLEZ RUS, Juan y otros, **Derecho Penal. Parte Especial,** Marcial Pons, Madrid, l999.

GUERRA DE VILLALAZ, Aura, ¿Están tipificados los delitos informáticos en la Legislación Panameña? en **Revista Lex (**Revista del Colegio Nacional de Abogados de Panamá) No.4, abril-agosto 1993.

GUTIÉRREZ FRANCES, María Luz **Fraude Informático y Estafa,** Ministerio de Justicia, Madrid, 1991.

HÉRRAN ORTIZ, Ana Isabel **La violación de la intimidad en la protección de datos personales**, Dykinson, Madrid, 1999.

JIJENA LEIVA, Renaro Javier, **La protección penal de la intimidad y el delito informático**, Editorial Jurídica de Chile, Santiago, l992.

JORGE BARREIRO, Agustín, "Delitos contra el Patrimonio", en **Comentarios al Código Penal,** Civitas, Madrid, 1997.

LANDECHO, Carlos Maria, **Derecho Penal, Parte Especial,** Tecnos, Madrid, 1996.

LATORRE, Virgilio, **Protección penal del Derecho de autor**, tirant monografías, Valencia, 1994

LEDESMA, Julio**, Derecho Penal Intelectual,** Editorial Universidad, Buenos Aires, 1992.

LIMA, María " Delitos electrónicos" en **Anuario de Derecho** No. 12, Facultad de Derecho y Ciencias Políticas, Universidad de Panamá,1983.

LUZ CLARA, Bibiana, **Manual de delito informático**, Nova tesis Editorial jurídica, Rosario, Santa Fe, 2001.

LUZÓN CUESTA, José María/ SOTO NIETO, Francisco/ VARGAS CABRERA, Bartolomé/ BENYTEZ MERINO, Luis. **Las falsedades documentales**, Editorial Comares, Granada, 1994.

LLANEZA GONZÁLEZ, Paloma, **Internet y comunicaciones digitales**, Bosch, Barcelona, 2000.

MANERA, Alberto, **Falsedades documentales por computadora**, Edic La Rocca, Buenos Aires, 2002.

MARCHENA GÓMEZ, Manuel, "El sabotaje informático entre los delitos de daño y desordenes públicos" en **Internet y Derecho Penal, Cuadernos de Derecho Judicial**, Consejo General del Poder judicial, Madrid, 2001

MARTOS, Juan Jesús, "Defraudación fiscal y nuevas tecnologías" en **Revista Aranzadi de Derecho y Nuevas tecnologías,** Thomson-Aranzadi, Pamplona, 2007.

MATA MARTÍN, Ricardo, **Estafa convencional, Estafa informática,** Thomson Aranzadi, Pamplona, 2007

MÖNHKENSCHLAGER, Manfred, "El nuevo derecho penal informático en Alemania" en **Delincuencia Informática**, PPV, Barcelona, 1992.

MOLES, Ramón, **Derecho y control de internet. La regulabilidad de Internet**, Ariel Derecho, Madrid, 2004.

MORALES GARCÍA, Oscar, "Delincuencia informática. Problemas de responsabilidad" en **Cuadernos de Derecho Judicial** IX, Consejo General del Poder Judicial, Madrid, 2002.

MORALES PRATS, Fermin, "El derecho penal ante la pornografía infantil" en **Revista Aranzadi de Derecho y Proceso Penal** No. 8, Aranzadi- Navarra, 2002.

MORALES PRATS, Fermin, "Internet: Riesgos para la Intimidad", en **Internet y Derecho Penal**, **Cuadernos de Derecho Judicial,** Consejo General del Poder judicial, Madrid, 2001

MORÓN LERMA, Esther, **Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red**, Aranzadi, S.A., Pamplona, 1999.

MUÑOZ CONDE, Francisco/ GARCÍA ARAN, Mercedes, **Derecho Penal, Parte General**, tirant lo blanch, Valencia, 1996.

MUÑOZ POPE, Carlos, **Estudios de la Parte Especial II,** Ediciones Panamá Viejo, Panamá, 2006.

ORTIZ VALLEJO, Antonio, **Derecho a la intimidad e informática, Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada**, Editorial Comares, Granada, 1994

ORTS BERENGUER, Enrique/ ROIG TORRES, Margarita, **Delitos informáticos y delitos comunes cometido a través de la informática**, tirant lo blanch, Valencia, 2001.

PALAZZI, Pablo, **La transmisión internacional y la protección de privacidad de datos personales**, ad-hoc, Buenos Aires, 2002,
- **Delitos informáticos**, ad-hoc, Buenos Aires, 2000.

PEGUERA POSCH, Miguel (Coordinador) **Derecho y nuevas tecnologías,** editorial uoc., Barcelona, 2005.

PÉREZ LUÑO, Antonio, **Problemas actuales de la documentación y la informática jurídica**, Tecnos, Madrid, 1987.

PÉREZ LUÑO, Antonio, "Intimidad y protección de datos personales del Habeas Corpus al Habeas data", en **Estudios sobre el Derecho a la Intimidad**, Edición dirigida por Luis García San Miguel, Tecnos, Madrid, 1992.

PÉREZ LUÑO, ANTONIO, **Derechos Humanos, Estado de Derecho y Constitución,** Tecnos Madrid,1980.

PEYRANO, Guillermo, **Régimen legal de los datos personales y habeas data,** Lexi Nexis, De Palma, Buenos Aires, 2002

QUERALT JIMÉNEZ, J. J., **Derecho Penal Español, Parte Especial,** 3a edición, bosch, editor, Barcelona, ´1996.

RIBAS ALEJANDRO, Javier, "La sociedad digital: Riesgos y Oportunidades" en **Informática y Derecho**, Nos. 27-28-29, Revista Iberoamericana de Derecho informático, Uned, Mérida,

RIQUERT, Marcelo, **Informática y Derecho Penal Argentino**, Ad hoc, Buenos Aires, 1999.

RODRÍGUEZ MOURULLO, (director), BARREIRO, Jorge (Coordinador),**Comentarios al Código Penal,** Civitas, Madrid, 1997.

RODRÍGUEZ RAMOS, Luis, "Descubrimiento y revelación de secretos en el nuevo Código penal", en Derecho al honor, a la intimidad y a la propia imagen", en **Cuadernos de Derecho Judicial**, Consejo General del Poder Judicial, Madrid, 1999.

ROMEO CASABONA, Carlos, **Poder Informático y seguridad jurídica**, Fundesco, Madrid, 1988.

ROMEO CASABONA, Carlos (coord) **El cibercrimen nuevos retos jurídicos-penales, nuevas respuestas, político criminales, Estudios de Derecho Penal y Criminología,** Editorial Comares, Granada, 2006

ROVIRA, Enrique del Canto, **Delincuencia informática y fraudes informáticos**, Editorial Comares, Granada, 2002.

SÁEZ CAPEL, José, **Informática y delito**, Proa XXI editores, Buenos Aires, 2001.
Informática y Derecho, Talleres Gráficas Sur, Buenos Aires, 2001

SALT, Marcos, "Delitos informáticos", en **Justicia Penal y Sociedad**, **Revista Guatemalteca de Ciencias Penales**, Año 4, No.6, abril de 1997

SANCHIS CRESPO, Carolina, **La prueba por soportes informáticos**, tirant lo blanch, Valencia, l999.

SERRANO GÓMEZ, Alfonso, **Derecho Penal, Parte Especial**, Dykinson, Madrid, 1997

SIEBER, Ulrich, "Criminalidad Informática Peligro y prevención", en **Delincuencia Informática** (Mir Puig, Coordinador)**,** PPU, Barcelona, 1992.

SOLANO, Orlando, **Manual de informática jurídica**, ediciones Jurídicas, Santa Fé de Bogotá, 1997.

UICI, Rodolfo Daniel, **Los bancos de datos y el derecho a la intimidad,** Ad-hoc, Buenos aires, 1999.

VILLALOBOS, Edgardo, **Introducción a la Informática Jurídica y Derecho Informático**, Facultad de Derecho, Universidad de Panamá, l997.
- **Responsabilidad Civil en la actividad informática**, No. 16, editorial Portobelo, Panamá, 1998.
- **Diccionario de Derecho Informático**, Editorial Chen, S.A., Panamá, 2002.

VIVES ANTON, T.S./ Boix Reig, J. **Derecho Penal, Parte Especial,** tirant lo blanch, Valencia, 1996.

WALDEN, Ian, Computer crimes and digital investigations, Ox f**ord University press, New York, 2007**