LA CRIMINALIDAD INFORMÁTICA EN EL CÓDIGO PENAL DE 1995

Por D. Francisco Lancho Pedrera

SUMARIO

1. INTRODUCCIÓN Y CONCEPTO

2. FORMAS DE LA COMISIÓN DEL DELITO INFORMÁTICO

3. LA CRIMINALIDAD INFORMÁTICA EN EL CÓDIGO PENAL DE 1995

   a) En la protección a la intimidad

   b) Delitos contra el patrimonio y el orden socioeconómico

      De los Hurtos y de los robos
      De las defraudaciones
      De las estafas
      De la apropiación indebida.
      De los daños
      De los delitos relativos a la propiedad Intelectual e Industrial, al mercado y a los consumidores

   c) De las falsedades documentales

1. INTRODUCCIÓN Y CONCEPTO

Lo primero que tenemos que hacer al entrar en el tema de la criminalidad informática es plantearnos dos cuestiones, la primera es la definición de «delito informático» en términos generales y la segunda es si en nuestro ordenamiento existe realmente el «delito informático» como tal.

En cuanto a la denominación de «delito informático» hemos de precisar que, en sentido estricto, entendemos por delito las conductas tipificadas como tales en la ley penal. Sin embargo, como manifiesta el profesor Pérez Luño[1], bajo el rótulo de «delito informático» se incluyen junto a conductas criminales que encajan dentro del concepto de tipo delictivo, otras que por su menor transcendencia no superan la calificación de faltas. Pero es más, el concepto «delito informático» también se usa en referencia a las infracciones administrativas, e incluso para los ilícitos civiles.

Esta variedad de supuestos ha hecho que se sea más correcto usar el concepto «criminalidad informática» que el de «delito informático», toda vez que dentro del concepto de «criminalidad informática» podemos incluir correctamente supuestos tanto incluidos en el ilícito penal, así como también supuestos que no entran técnicamente dentro del concepto de delito pero que, sin embargo, son reprochables por el ordenamiento jurídico, aunque podemos aceptar el uso de «delito informático» por convencionalismo.

La segunda cuestión que nos planteábamos era analizar si realmente existe o no en nuestro ordenamiento jurídico el llamado «delito informático», y hemos de tener en cuenta que conceptualmente hablando, no existe delito si no hay una ley que le cree, tal y como recoge el art. 10 de nuestro actual Código Penal[2] en el sentido de disponer que «son delitos o faltas las acciones y omisiones dolosas o imprudentes penadas por la ley», y no caigamos en el error de pensar que solamente es norma penal la recogida en el Código Penal, sino que también existen leyes especiales a las que se aplican las disposiciones del Código Penal como supletorias.

Siguiendo la opinión de Davara Rodríguez[3], no es cierto que el nuevo Código Penal introduzca el llamado «delito informático», toda vez que en palabras de dicho autor, ni siquiera existe como tal un delito informático, al no estar tipificado en el Código Penal ni en otra norma especial, cosa distinta es que se use

---

[1] Pérez Luño, Antonio Enrique, *«Manual de Informática y Derecho»*, Ariel Derecho, Barcelona 1996.

[2] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, que se publicó en el «Boletín Oficial del Estado» núm. 281, de 24 de noviembre.

[3] Davara Rodríguez Miguel Angel, «*Manual de Derecho Informático*», Aranzadi, Pamplona 1997.

y acepte la expresión «delito informático» por conveniencia para referirnos a determinadas acciones u omisiones dolosas o imprudentes en la que ha tenido relación un bien o servicio informático.

Entonces, si no hay ley que lo tipifique como delito, ni ley que establezca una pena, y atendiendo al principio de legalidad en materia penal en el sentido que los delitos y las penas existen en cuanto están plasmados en una norma, hemos de llegar a la inequívoca conclusión que no existe en nuestro ordenamiento jurídico ningún tipo que se pueda encuadrar dentro de llamado «delito informático».

Por lo tanto podemos definir el llamado «delito informático», siendo la correcta interpretación dada por el Profesor Davara Rodríguez 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 hardware o software». No debemos incluir en este concepto otros tipos delictivos en los que interviniendo el elemento informático, como por ejemplo la venta de forma fraudulenta de un ordenador, estaría tipificada en dentro de otro supuesto delictivo que nada tiene que ver con el tema que estamos tratando.

2. FORMAS DE COMISIÓN DEL DELITO INFORMÁTICO

Claro es que las dos maneras por las cuales se puede proceder a la comisión del delito que estamos tratando son dos:

1) Acceso y manipulación de los datos.
2) Manipulación de los programas.

En atención a lo anterior podemos clasificar las siguientes formas de ejecución del delito:

a) *Manipulación en los datos o informaciones contenidas en los archivos o soportes físicos informáticos ajenos.* Es el llamado *Data diddling,* que sería las distintas formas de alteración de los datos contenidos en un ordenador antes o durante su proceso informático. En la fase en la cual se suele dar la manipulación es la fase llamada *feedback* o retroalimentación, que es el momento en el cual un ordenador asume, y aprovecha, los resultados de un proceso, como fuente de información para otro nuevo tratamiento. El caso más conocido sobre este asunto es el de una funcionaria que realizó desde una terminal conectada al ordenador central un serie continuada de transacciones económicas falsas.

b) *Introducción de programas o rutinas en otros ordenadores para destruir, alterar o modificar información, datos o programas,* es lo que conocemos como *virus informáticos,* cuya localización del origen y autor es habitualmente imposible de descubrir, y cuya finalidad, habitualmente, no se sabe cual es, aunque es cierto que se ha creado toda un industria económicamente muy lucrativa

para combatir esos *virus informáticos* a través de programas llamados *antivirus* o *programas vacunas,* por lo que la desaparición de los *virus* llevaría que esos programas de protección serían innecesarios, esto ha dado lugar a que se haya planteado la sospecha de que sean las propias empresas que desarrollan el software quienes desarrollen los propios *virus.*

De lo que no cabe duda es que la introducción de estas rutinas, instrucciones o partes de programas que se introducen a través de un soporte físico, habitualmente por medio de un disquette o a través de redes como *internet*, es sin duda una intromisión ilegítima en un derecho básico titular.

Dentro de este epígrafe hemos de incluir los llamados *«Caballos de Troya»* o *Troyan Horses*, consistentes en introducir rutinas o instrucciones que en un principio inofensivas aparentemente, distorsionan el funcionamiento de los sistemas informáticos. Se utiliza principalmente para que el ordenador lleve a cabo operaciones no autorizadas, transferencias bancarias no autorizadas, autorizar pagos, etcétera.

c) Acceso a los datos y/o utilización de los mismos por quien no está autorizado a ello. Entre las modalidades más notorias se debe destacar la llamada fuga de datos (Data Leakage), que podríamos encuadrar dentro del clásico espionaje industrial. Vemos como hoy en día la empresas y organismos oficiales tiene su información importante y vital dentro de soportes informáticos, con lo que cualquier atentado para obtener esa información sería causa de delito. Pero es más, los mismos programas informáticos son hoy en día objetivos de este tipo de delitos dado su alto valor y complejidad.

d) Utilización del ordenador y/o los programas de otra persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otros. Es el caso de los empleados de una empresa o sociedad, que abusando de la confianza prestada, que usas los ordenadores de la empresa para usos fraudulentos o en beneficio de terceros no relacionados con la empresa.

e) Utilización del ordenador con fines fraudulentos. Dentro de este apartado debemos incluir dos técnicas tendentes a realizar fraudes a través de los medios informáticos.

La primera es la que se ha denominado *técnica del salami* o *Salami Technique/Rounding* por la cual se procede a sustraer de cuentas bancarias pequeñas cantidades mediante la técnica del redondeo para ingresarlas en la cuenta del manipulador. Las cantidades son tan pequeñas individualmente, que no llaman la atención ni de la entidad ni del perjudicado y llega a ascender en su monto total a cantidades realmente elevadas.

La segunda técnica, es la definida como *robo de servicios*, dentro del cual destaca el denominado *Scavenging* o *Apropiación de Informaciones Residuales*, consistente en la sustracción de datos que ha sido abandonados por los legítimos usuarios de servicios informáticos como residuo de determinadas operaciones. También tiene relevancia lo que se ha definido como *Parasitismo informático* o

Piggybacking, consistente es usar en beneficio propio, suplantando a legítimo usuario, equipos físicos o programas informáticos.

Dentro de la utilización fraudulenta debemos incluir el uso de nuestro propio ordenador para defraudaciones, enmascaramiento de datos, ocultación de datos para defraudaciones fiscales, etcétera.

f) El acceso no autorizado a sistemas informáticos. Dentro de este epígrafe hemos de incluir diversas modalidades, como señala Pérez Luño[4].

En primer lugar, tenemos las llamadas *Puertas falsas (trap Doors)*. Todos los programas informáticos tienen una serie de rutas de acceso configuradas por los programadores y no contempladas en sus instrucciones de aplicación y cuya utilidad reside en facilitar la revisión o recuperar la información en caso de errores del sistema, para que el lector pueda comprender en que consisten estas puertas falsas, no son más que los conocidos *trucos* de los videojuegos, que permiten manejar el programa informático sin ningún tipo de riesgo y que son ideados por los programadores para poder revisar el programa. El delito consistiría en introducirse en el sistema informático a través de esas puertas falsas, para poder manipularlo a su antojo y en beneficio propio.

Por otra parte, tenemos lo que se ha denominado *Llave maestra (Superzapping)*, consistente en el uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático.

g) Agresión la «privacidad» mediante la utilización y procesamiento informático de datos personales con fin distinto al utilizado. Consiste este delito en la utilización de datos personales procesados en sistemas informáticos con fines distintos a los que estaban destinados y autorizados. En España tenemos sobre esta materia la Ley orgánica de Regulación de Tratamiento Automatizado de Datos de Carácter Personal (LORTAD)[5].

3. LA CRIMINALIDAD INFORMÁTICA EN EL CÓDIGO PENAL DE 1995

Como hemos dicho antes, no podemos admitir que exista en el nuevo Código Penal el denominado «Delito Informático» como tal, como delito autónomo, sino que en diferentes artículos del Código Penal se admite la posibilidad de efectuar conductas dolosas o culposas a través de medios informáticos o relacionados con tales medios.

Vamos a seguir la clasificación que efectúa Jover Padró[6], y que adapta Davara Rodríguez a la sistemática del Código Penal:

---

[4] Pérez Luño, Antonio Enrique, *«Manual de Informática y Derecho»*, pag. 73-74 Ariel Derecho, Barcelona 1996.

[5] Ley Orgánica 5/1992, de 29 de octubre, publicada en el «Boletín Oficial del Estado» núm. 262, de 31 de octubre de 1992.

[6] Jover Padró, J, «*El Código Penal de la informática*» en X *Años de Encuentros sobre Informática y Derecho,* Editorial Aranzadi, Pamplona, 1997. Pgs. 349 y ss.

a) En la protección a la intimidad

Nos referimos en esta apartado al uso de datos personales con un fin distinto para el que se está autorizado.

El art. 18 de la Constitución garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen, dentro del Capítulo dedicado a «Los derechos y libertades», en la Sección «Los derechos fundamentales y de las libertades públicas», y dentro de los derechos especialmente protegidos por el art. 53.2 de la Constitución. Pero es más, el apartado 4 del meritado art. 18 de la Carta Magna, nos dice que *«La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»*.

Penalmente, hemos de acudir Código Penal en su Título X referente a los «Delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio», en concreto en el Capítulo I referente al «Descubrimiento y revelación de secretos» en sus arts. 197 a 201, aunque el de mayor relevancia es el art. 197, que nos dice en sus apartados 1.º y 2.º que:

> «1.º *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, grabación o reproducción de sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de uno a cuatro años y multa de doce a veinticuatro meses».*
>
> «2.º *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 archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien altere o utilice en perjuicio del titular de los datos o de un tercero».*

Vemos como este delito lo que realmente protege es la intimidad de la persona, pero con la peculiaridad de que se puede cometer por medios informáticos o telemáticos. Lo que se ha hecho en realizada por el legislador ha sido adaptar la comisión del delito a los tiempos actuales, en los cuales cada vez es más frecuente las comunicaciones entre ordenadores vía módem o los ficheros o archivos con datos personales se encuentran almacenados en soportes informáticos. Pero vemos como la informática no es más que el medio de comisión del delito, no el fin a proteger, toda vez que la implantación y evolución de los medios informáticos puede llegar a facilitar la consecución de estos delitos, ya que es más difícil localizar a su autor al dejarse menos huellas y poder camuflar el origen de la intromisión.

Por último, solamente plasmar lo que es establece el apartado 4.º del art. 197 del código Penal, que agrava la pena hasta cinco años de prisión y dice:

> «Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, elec-

> trónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior».

B) DELITOS CONTRA EL PATRIMONIO Y CONTRA EL ORDEN SOCIOECONÓMICO

1. De los hurtos y de los robos

En principio, parece que el robo estaría descartado del tema que estamos tratando toda vez que para que exista robo es necesario que se utilice fuerza, violencia o intimidación, y, desde luego, que la acción producida por medios informáticos se pueda llevar a cabo por medio de uno de estos medios, es en principio, muy difícil por no decir imposible.

Ahora bien, no podemos olvidar el art. 238 del Código Penal, dice:

> «Son reos del delito de robo con violencia en las cosas los que ejecuten el hecho:…4.º) Uso de llaves falsas».

Estipulando el art. 239 que en el concepto de «llaves falsas» hemos de incluir «*las tarjetas, magnéticas y perforadas y los mandos o instrumentos a distancia*». Si esta tarjeta tuviera un chip o banda magnética, nos encontraríamos con un delito de robo cometido por medios informáticos[7].

Distinto estudio merece el hurto.

Dice el art. 234 del Código Penal que son reos de hurto los que:

> «con ánimo de lucro, tomare las cosas muebles ajenas sin la voluntad de su dueño».

El problema del hurto es la forma de la comisión del delito por medios informáticos, toda vez que el precepto penal exige que se tomen las cosas, y no olvidemos que tomar equivale a coger, es decir la posesión material de la cosa. Gran parte de la doctrina entiende que no se puede cometer hurto con medios informáticos porque que si se realiza a través del ordenador, no se toma materialmente la cosa, ya que a través del ordenador se efectuaría de manera inmaterial. Sin embargo, entendemos que tal postura es equivocada, a través de la informática se puede cometer hurto, como por ejemplo si utilizamos el ordenador para realizar un traspaso de dinero de una cuenta corriente a otra de forma ilegal, y se dispone físicamente de ese dinero, independientemente de que también pueda ser tipificada la acción como estafa.

2. De las defraudaciones

Comencemos con el estudio de las estafas. Esta figura delictiva plasma su tipificación, a los efectos que nos interesa, en el art. 248.2 que dice que:

---

[7] Corripio Gil Delgado, R, «*Delitos cometidos con la utilización de tarjetas magnéticas*» en *X años de encuentros sobre Informática y Derecho,* Aranzadi, Pamplona, 1996

> «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».

Este delito tiene una particularidad que le caracterizan, así la dificultad de conocer la autoría del hecho cometido por medios informáticos y esto es así porque hasta la fecha es realmente casi imposible detectar el origen de la estafa.

En cuanto a la apropiación indebida, dispone el art. 252 del Código Penal:

> «Serán castigados con las penas del articulo 249 o 250, en su caso, los que en perjuicio de otro se apropiaren o distrajeren dinero, efectos, valores o cualquier otra cosa mueble o activo patrimonial que hubieren recibido depósito, comisión o administración, o por otro título que produzca obligación de entregarlos o devolverlos, o negaren haberlos recibido».

Este supuesto seria cuando, por ejemplo, un empleado bancario, basándose en la confianza, va a trasladar fondos a través de medios informáticos a otra cuenta a que tenia fácil acceso. Pero como vemos la informática es en el medio, no el fin, a no ser que lo que se apropie sean programas informáticos.

3. De los daños

Respecto al delito de daños nos dice el Código Penal en su art. 264.2, que se impondrá la pena de prisión de uno a tres años y multa de doce a veinticuatro meses, al que:

> «por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos».

Es lo que se ha denominado como «Sabotaje informático» y consiste en inutilizar los sistemas informáticos causando daños a los programas o a los sistemas operativos informáticos.

El sistema más usado es el de las *«bombas lógicas» (logic Bombs)*[8], consistentes la introducción de un programa de un conjunto de instrucciones indebidas, que en una determinada fecha, o ante una determinada situación se ponen en marcha, dañando o destruyendo los datos de ordenador, distorsionando el funcionamiento del sistema, o provocando su paralización definitiva o alternativa.

Otra modalidad son los conocidos, y ya mencionados anteriormente, como *virus informáticos,* que sabemos que actúan dañando los sistemas informáticos conectados a redes o sin estar conectados, no nos extendemos más en la explicación de los virus informáticos toda vez que ya se ha tratado.

4. De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores.

En cuanto a los delitos relativos a la propiedad intelectual establece el art. 10.1, i) de la Ley de Propiedad Intelectual:

[8] Perez Luño A-E «manual de Informática y Derecho», Ariel, 1997, Madrid.

> «Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas….i) los programas de ordenador».

El bien jurídico protegido son los derechos de autor, protegiéndose no sólo a los programas de ordenador, sino también a la documentación técnica y manuales de uso del programa y las versiones sucesivas y programas derivados, tal y como se recoge en el art. 96.1 y 3 de la Ley de Propiedad Intelectual.

Ahora bien, como veremos en el tema correspondiente sobre la protección jurídica de los programas informáticos, existen dos tipos de derechos de autor, tenemos por una parte los derechos morales y por otra parte los derechos patrimoniales, que quedan protegidos estos últimos es claro, pero ¿también se protegen los derecho morales? Hemos de decir que en opinión de los máximos exponentes doctrinales de nuestro país, sí se protegen los derechos morales de los autores, aparte de que tal opinión también la comparte la Sentencia del Tribunal Supremo de 13 de octubre de 1988. Y esto es claro, por lo menos a nuestro entender, ya que la valoración de si es más importante el aspecto patrimonial que el moral de una obra es una concepción subjetiva de cada autor, por lo que deberá ser protegidos ambos derechos, los morales y los patrimoniales.

Establece el art. 270 del Código Penal:

> «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 terceros, 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 tipo de soporte o comunicada a través de 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».

Por supuesto, dentro de este precepto se encuentran incluidos los programas informático bien es soporte disquette o bien en soporte lector óptico (CD-ROM), aparte de cualquier otro soporte que se inventara en el futuro.

El tipo se agrava en el caso de que el beneficio obtenido sea de especial trascendencia o que el daño causado revista especial gravedad, como se regula en el art. 271 del código Penal.

Esto no es más que el denominado «pirateo informático», es un intento de frenar tales prácticas toda vez que esta ocurriendo que de algunos programas informáticos existen más copias ilegales que legales en el mercado, de tal forma que el daño que se produce a los autores es muy importante.

El art. 272 del Código Penal que:

> «En el supuesto de sentencia condenatoria, el juez o Tribunal podrá decretar la publicidad de ésta, a costa del infractor, en un periódico oficial».

Como principio nos parece lógico, pero sin embargo lo dispuesto en el mencionado artículo es realmente poco efectivo ya que un periódico oficial tiene escasa trascendencia a nivel de repercusión social, sería más realista y efectivo que esa publicidad se realizara en un medio de difusión de gran transcendencia a nivel de publicidad.

Establece así también el art. 272 que:

> «La extensión de la responsabilidad civil derivada de los delitos tipificados en los dos artículos anteriores, se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios».

Por tanto vemos como se nos remite a la Ley de Propiedad Intelectual para delimitar y cuantificar los daños y perjuicios causados.

En cuanto a los delitos relativos a la propiedad industrial, establece el art. 273.3 del Código Penal que:

> «El que realice cualquiera de los actos tipificados en el párrafo primero de este artículo concurriendo iguales circunstancias en relación con objetos amparados a favor de tercero por un modelo o dibujo industrial o artístico o topografía de un producto semiconductor».

Se hace referencia a este precepto toda vez que las «topografías de productos semiconductor» usan tecnología informática.

Establece, y ya hablando de los delitos relativos al mercado y a los consumidores, el Capítulo XI[9] en su art. 278 del Código Penal que:

> «1.º El que, para descubrir o revelar un secreto de empresa se apodere 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.º del art. 197[10]…3.º- 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».

Podríamos incluir este tipo de delito en lo que hemos denominado como «espionaje industrial» si lo que se logra por el acceso con medios informáticos es la adquisición de secretos industriales.

C) De las falsedades documentales.

En el Código Penal, en su Título XVIII, Capítulo II, Sección I, se regula un

[9] El Capítulo se denomina «De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores».

[10] se refiere a artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación.

tipo de delito que quizás sea en idóneo para cometerse por medios informáticos o telemáticos.

El Código Penal tipifica en su art. 392 la falsificación de documento público, oficial o mercantil, así como la falsedad cometida por autoridad o funcionario sobre cualquier tipo de documento en sus arts. 390 y 391, haciendo una referencia expresa para la falsificación de los documentos privados en los arts. 395 y 396, así como la falsificación por facultativo de certificados del art. 397, por funcionario público o autoridad (art. 398) o por particular (art. 399) y especialmente los encargados de los servicios de Telecomunicaciones en el art. 394.

Todo esto viene a que sí consideramos documento[11] lo reflejado en el Código Penal, dentro de ese concepto se encuentran los soportes informáticos, aunque parte de la doctrina nos dice que el documento informático no es original, y por lo tanto, si no lo es no puede ser falsificado al tratarse de una copia del original.

Existen otras referencia en el Código Penal de la comisión de delitos realizadas por medios informáticos, aunque la más importantes son las que hemos visto hasta ahora; estas otras figuras delictivas que se pueden cometer por medio de la informática o relacionadas con los medios informáticos o telemáticos son en las defraudaciones de fluido eléctrico y análogas, en los delitos societarios, en los estragos, en la infidelidad en la custodia de documentos y de la violación de secretos o en el delito de desordenes públicos.

BIBLIOGRAFÍA

Correa y otros, *Derecho Informático,* Ediciones Depalma, Buenos Aires, 1987.

Corripio Gil Delgado, R., *Delitos cometidos con la utilización de tarjetas magnéticas* en *X años de encuentros sobre Informática y Derecho,* Aranzadi, Pamplona, 1996.

Jover Padró, J., *El Código Penal de la Informática* en *X años de encuentros sobre Informática y Derecho,* Aranzadi, Pamplona, 1996.

Parker, D., *Computer Crimes*, Editorial Scribners, New York, 1980.

Rodríguez Devesa, J. M., *Derecho Penal Español, Parte General,* Dykinson, Madrid, 1996.

Romeo Casabona, C., *Poder Informático y seguridad ciudadana,* Fundesco, Madrid, 1988.

Tellez Valdés, J., *Terrorismo por computadora,* Revista Informática y Derecho, UNED, Mérida, 1992.

Tortras, C., *El delito informático* Revista informático y Derecho, ICADE, Madrid, 1989.

[11] Establece el artículo 26 del Código Penal que «*A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica*».