ILICITOS INFORMATICOS: Reseña normativa en nuestro derecho.

Por Valentin Acuña[1]

ÍNDICE GENERAL

[1] Abog. Especialista en Derecho Penal por la UNL. Esp. En Garantias Contitucionales del Poceso Penal por la

INTRODUCCIÓN

Debemos recordar que al momento de la sanción de nuestro Código Penal la tecnología informática, no existía, las comunicaciones se producían de manera totalmente distinta, así también como el manejo de la información; por lo tanto el legislador de ningún modo hubiera podido preveer las acciones delictivas relacionadas con la informática y demás tecnologías que fueron luego surgiendo a través de los años.

La aparición de las computadoras y su uso cotidiano ha tenido innumerables efectos positivos sobre la sociedad, también es cierto que ha tenido diversos efectos negativos como lo son la aparición de diversas actividades ilícitas, llevadas a cabo mediante estas nuevas tecnologías, haciendo necesaria su regulación legal.

Así aparecieron individuos dedicados a actividades ilegales, o al menos contrarias a lo que es legal para el sentimiento de la sociedad tales como los llamados hackers quienes acceden sin autorización a sitios informáticos ya sea en busca de información, estos aparecieron en los años 80 con otro objetivo o a veces con el solo propósito de desafiar los sistemas de seguridad; los crackers quienes desafían los sistemas de seguridad pero con la finalidad de hacer daño, o los llamados phreakers que son aquellos que utilizan técnicas de fraude en telefonía, también la introducción de virus, la piratería, ya sea ésta realizada a nivel de las empresas que se dedican al comercio de equipos informáticos, de profesionales, o aún la de uso doméstico.

Otro medio fundamental de comisión de hechos ilícitos es hoy internet ya sea en una página web o mediante un e e-mail, etc., así la delincuencia informática comenzó a cometer no solo ataques contra el patrimonio, sino tambien contra otros bienes jurídicos como

ser la privacidad, la salud, las comunicaciones, llegando incluso a poner en peligro la vida.

La falta o la lentitud en la regulación de este nuevo fenómeno ha ido provocando la impunidad de ciertas conductas que para el sentimiento colectivo eran ilícitas o bien otras veces mediante grandes esfuerzos por llenar este vacío legal se recurría a interpretaciones judiciales que traían como consecuencia falta de previsibilidad y seguridad jurídica, con el consiguiente descreimiento de los ciudadanos en la justicia,[2] "y si bien es cierto que la legislación va siempre un paso atrás de las situaciones que pretende contemplar. Así primero existe la conducta que provoca el hecho dañoso, y luego se la tipifica y penaliza. Pero cuidado, no nos quedemos tantos pasos atrás y tengamos luego que correr una larga carrera para alcanzar nuestros objetivos, y cuando lleguemos, ya no estén allí"[3]

El objeto del presente trabajo es realizar un breve análisis de este fenómeno del delito informático y sus características así la forma como se ha regulado el mismo dentro de nuestro sistema penal.

[2] CARBONE, Rolando Diego, Microjuris.com.

[3] BIBIANA, Luz Clara, Manual de Derecho Informático, Editorial Jurídica Nova Tesis, Rosario, Santa Fe, 2.001.

EL ILICITO INFORMATICO

Los ilícitos cometidos pueden ser de carácter civil los cuales generaran la responsabilidad de reparar el daño causado a quien llevare a cabo la conducta ilícita o penal, generadores de una responsabilidad tanto resarcitoria como punitiva.

En el presente trabajo nos ocuparemos solamente de los ilícitos penales, el tema que hoy nos ocupa son los "llamados delitos informáticos"

En el lenguaje coloquial y también en el lenguaje técnico es de uso extendido la voz "delito informático"

A pesar de ello la Doctrina (tanto nacional como internacional) se ha preguntado acerca de la conveniencia de emplear el término delito informático. "Anticipo que estas dudas no son originales de la doctrina argentina, sino comunes en el ámbito del derecho comparado, incluso en aquellos países con mayor tradición legislativa en la materia, que no son otros que en los que primero se enfrentaran con las novedosas modalidades de cometer delitos que ofrece el medio informático. Frente a lo problemático que ha tornado el lograr una noción que obtenga consenso para definir al "reato informático" nos indica la italiana Claudia Pecorella que se verifica una suerte de renuncia a lograr un concepto "internacional" del fenómeno y, en su lugar, la consideración como más oportuna de la directa referencia a una precisa tipología de "computer crimes", tendencia en progresiva afirmación favorecida por la Organización para la Cooperación y el Desarrollo Económico" [4]

[4] RIQUERT, Alfredo Marcelo , Delitos Informáticosm, http//www.terragnjurista.com.ar/doctrina/delinfo2.htm, pág. 1.

Así la doctrina tanto nacional como internacional ha venido tratando de establecer que es un delito informático y cuáles son sus caracteres.

Para Pablo Palazzi la computadora puede constituir un medio o puede constituir el objeto para cometer un delito. Se utiliza como un medio por ejemplo en los casos en que en una computadora se lleva una doble contabilidad con fines de evasión fiscal, o se crea un registro falso con la finalidad de cobrar créditos inexistentes, falsedades contables, estafas mediante inversiones de capitales organizadas mediante una computadora. La informática es objeto del delito cuando es aquello sobre lo cual recae el delito y puede ser que este recaiga sobre el hardware o sobre el software, así dice Palazzi "En síntesis, la informática puede constituir un medio o el objeto de una acción típica. En la medida en que se presenten alguno de estos elementos, o ambos, estaremos ante un "delito informático"[5]

Por su parte la organización para la Cooperación y el Desarrollo Económico (OCDE) define al delito informático como "cualquier comportamiento antijurídico no ético o no autorizado, relacionado con el proceso automático de datos y las trasmisiones automáticas de datos"

Ahora bien conforme al derecho si un sujeto realiza un hecho ilícito y de esta manera vulnera un bien jurídico de carácter ajeno, tiene la obligación de reparar el daño provocado volviendo las cosas al estado anterior al hecho; o bien si ello es imposible, compensar el daño causado de alguna otra manera, y esto es así ya sea que la voluntad del agente haya estado dirigida a la vulneración de dicho bien (responsabilidad subjetiva), o no (responsabilidad objetiva).

Pero a veces el derecho no se conforma con imponer solamente una reparación sino que además impone una pena, y es ahí donde aparece la actuación del derecho penal, que

[5] PALAZZI, Pablo A. Delitos Informáticos. Ed. Ad Hoc Buenos Aires, pag. 36

selecciona cuáles de aquellas conductas previstas como ilícitas dentro del ordenamiento jurídico merecen además una pena, aquí no se tiene ya en cuenta la magnitud del daño producido sino la gravedad del ataque al bien jurídico y la voluntad del sujeto que debe ir dirigida a la violación del mandato (exclusión de la responsabilidad objetiva), esta elección varía dentro de cada estado y de cada sociedad y constituye una elección de política criminal.

Si bien la existencia de delito se basa en la existencia de la conducta de un hombre, antijurídica, por ser contraria a un mandato jurídico, y culpable, es decir no se puede atribuir responsabilidad objetiva, y sancionado con una pena, no solamente con la obligación de una reparación; también y necesariamente para que el delito exista este hecho debe haber sido contemplado por un tipo penal.

"El tipo es el instrumento por medio del cual del conjunto de conductas antijurídicas de las que hay que responder subjetivamente (eventualmente culpables) que contiene –expresa o implícitamente- el ordenamiento jurídico, el derecho penal selecciona aquellas que son merecedoras de pena, lo cual hace designándolas por medio de su descripción" [6]

El tipo es limitador del "ius puniendi" y garantizador de los derechos del los individuos contenidos en el principio de legalidad del art.. 18 de la C.N. "Ningún habitante de la nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso…" y de reserva consagrado en el art. 19 de nuestra Carta Magna. "las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública ni perjudiquen a un tercero, están sólo reservadas a Dios y exentas de la autoridad de los Magistrados. Ningún habitante de la nación será obligado a hacer lo que no manda la ley ni privado de lo que ella no prohíbe"

[6] CREUS, Carlos Derecho Penal Parte General, 4ª Edición actualizada y ampliada, Editorial Astrea de Alfredo y Ricardo Depalma, Buenos Aires, 1996

Como derivación del principio de legalidad ya mencionado el derecho penal prohíbe la analogía. Carlos Creus hace una distinción entre la analogía legis y la analogía iuris. La analogía legis la considera como la aplicación a un caso no contemplado por la ley de una norma que regula un caso similar (copiando así una norma). En la analogía iuris, en cambio el caso no contemplado por la ley es regulado por el propio juez con una norma que él crea partiendo de los principios generales que inspiran la legislación vigente (creando así una norma).

La analogía es así fuente de nuestro derecho civil, pero jamás (y en ninguna de estas dos formas) opera en el derecho penal , ya que de ser así vulneraría un principio de jerarquía superior como es el principio de legalidad

Sin embargo la doctrina establece la diferencia entre la aplicación analógica de la ley penal (prohibida por el derecho penal), y la interpretación analógica de la ley (imprescindible para la aplicación del derecho penal), mientras en la interpretación, y aunque sea extensiva se aplica la ley, en la analogía se crea la ley.

Así por ejemplo Zaffaroni nos dice que no debe confundirse la integración analógica con el uso de la analogía sin la cual no sería posible ninguna interpretación. Este piensa que la analogía como regla de la lógica interpretativa no solo no está prohibida sino que es admisible y recomendable. Lo que sí no se puede es hacer decir a la ley lo que esta no dice, "así nadie duda que la violencia del art. 127 del C.P es análoga a la del art. 164 del mismo texto, pero no puede considerarse típica del art. 181 la conducta de alterar los planos que señalan los límites de un fundo argumentando que es análogo a alterar materialmente los límites" [7]

Por su parte Creus sostiene que es válido el empleo de la analogía como instrumento de la lógica jurídica, como argumento que se emplea para interpretar una norma

[7] ZAFFARONI, Eugenio Raúl, Manual de Derecho Penal, Parte General, Ediar, 2.005, Capital Federal, Pag.. 107

por los significados que se han dado a otras, puesto que entonces, pasa a ser base del procedimiento sistemático.

Y si bien el límite entre uno y otro pareciera que puede en algunas ocasiones no aparecer tan claro , será tarea del interprete establecerlo cuidadosamente de manera de lograr una interpretación de la ley que satisfaga a la justicia sin vulnerar un principio fundamental establecido en la C.N. como lo es el mencionado principio de legalidad. [8]

Así dejamos en claro que no hay delito sin tipo penal y los intentos de adaptar las viejas normas existentes en el código penal a las nuevas situaciones de hecho creadas por el avance de la informática son dificultosos y llenar los vacíos legales por interpretaciones jurisprudenciales analógicas es imposible.

Pensamos que la denominación delitos informáticos es apropiada si nos estamos refiriendo a una conducta humana, antijurídica, culpable, seleccionada por el derecho penal mediante su inclusión en un tipo penal por medio del cual se le impone una pena, y que tiene como medio de ejecución o como objeto la informática, si no nos encontramos ante este supuesto deberemos conformarnos con hablar de un hecho ilícito pero no podemos emplear el término delito informático

CARACTERIZACION

La informática trajo consigo una nueva modalidad delictiva que posee características propias, las cuales deben ser tenidas en cuenta al momento de pensar en su regulación legal, ya que las mismas a veces hacen que esta regulación resulte tal vez más dificultosa que cuando se trata de otro tipo de delito.

[8] CREUS, Carlos, Derecho Penal parte general… , obra cit.

1.- EL SUJETO ACTIVO: Puede ser cualquier persona que posea conocimientos mínimos de informática y tenga acceso a una computadora hasta una persona o grupo de personas que posean profundos conocimientos en la materia.

Palazzi los clasifica de la siguiente manera:

. Delitos patrimoniales contra bancos y entidades financieras: Son cometidos por empleados, ex empleados, cajeros, personal del área de sistemas, o terceros en connivencia.

. Delitos de acceso ilegítimo o delito de daños menores: Hackers, phreakers, usuarios descontentos.

. Daño o sabotaje informático: Empleados de la empresa o espías

. Violaciones a la privacidad, tratamiento ilícito de datos personales: Investigadores privados. Empresas de marketing, agencias de informes crediticios.

. Violaciones a la propiedad intelectual del software y bancos de datos con informes o compilaciones de datos: Piratas informáticos, usuarios, empresas que realizan competencia parasitaria [9]

2.- EL SUJETO PASIVO:

Cualquiera que opere con ordenadores, si bien son muy propensas a ser víctimas de estos delitos los bancos y entidades que manejan grandes cantidades de dinero en forma electrónica.

3.- LA DISOCIACIÓN DE LAS CONDUCTAS EN EL ESPACIO: También es dificultosa su investigación por estar disociado en el espacio: Tiene las características de los delitos cometidos a distancia, así un software puede ser realizado en un lugar y producir sus efectos en un lugar muy distante, planteándose además el problema de cuál es el juez que debe entender en la causa.

[9] PALAZZI, Pablo A. Delitos Inf…, obra cit, pag. 68.

La característica de estas conductas que se realizan en un lugar, produciendo efectos en otro, aún en países distintos muchas veces dan lugar al fenómeno de la transnacionalidad.

Internet no posee límites geográficos y traspasa las fronteras. El hecho de no estar Internet bajo el control de ninguna autoridad , se plantea problemas respecto de la ley aplicable así como del juez competente.

3.- LA DISOCIACIÓN DE LAS CONDUCTAS EN EL TIEMPO: Las computadoras poseen un reloj interno que funciona mediante una batería y permite determinar la fecha que pondrá en funcionamiento un programa, incluso podría ser con antelación de meses o de años.

Estas características mencionadas dan a su vez lugar a las siguientes:

a) DIFICULTAD EN SU LEGISLACION: La necesidad de un conocimiento o de una asesoramiento técnico por parte del legislador, a quien esta nueva realidad se le puede presentar como sumamente compleja

Además el constante y rápido avance de este tipo de tecnologías hará necesario que las legislaciones acompañen las modificaciones que se vayan produciendo.

Otro problema es aquel inherente a la trasnacionalidad que a veces trae la falta de consenso internacional acerca de la reprochabilidad de determinadas conductas y las distintas maneras de legislar este fenómeno.

b) DIFICULTAD EN LA INVESTIGACION Y LA PRUEBA.: También puede resultar dificultoso dificultosa su investigación ya que la policía y los tribunales no están preparados, por emplearse técnicas y tecnologías nuevas. Son delitos que no suelen

dejar rastros o por lo menos rastros que no pueden ser detectados a simple vista. Las pericias necesitarán de especialistas en el tema

También estas tecnologías pueden estar puestas al servicio de obstaculizar la investigación de un delito como por ejemplo cuando un programa al detectar un determinado acceso eliminan la información o avisan del intento de acceso al autor del delito

LEGISLACIÓN:

EL DERECHO COMPARADO

Como veremos los países en general han contemplado el fenómeno que nos ocupa mucho tiempo antes de lo que lo ha hecho nuestro legislador, y así por ejemplo:

- Chile: En el año 1993 mediante la ley 19.223 había tipificado una serie de conductas como delitos informáticos por estar referidas a medios informáticos o haber sido cometidas mediante los mismos.

- España: Desde 1995 se hallan tipificados dentro del código penal delitos informáticos o cometidos a través de internet tales como violación de secretos y apoderamiento, utilización o modificación ilegítima de datos reservados contenidos en medios informáticos públicos o privados, calumnias e injurias propagadas por internet, Estafa cometida por internet, Destrucción, alteración, inutilización o daño de datos programas o documentos electrónicos contenidos en redes o soportes informáticos, Reproducción o plagio, sin autorización y con ánimo de lucro de obras literarias, artísticas o científicas fijadas en cualquier tipo de soporte, Exhibición obscena, Apología de delitos.

- Estados Unidos: Existe también una numerosa legislación tanto a nivel federal como estadual, entre ella el Acta Federal de Abuso Computacional de 1994 y 1996 que modificó el Acta de Fraude y Abuso Computacional de 1986.

- Alemania: La Segunda Ley contra la Criminalidad Económica del año 1986 contempla algunos delitos como espionaje de datos, estafa informática, falsificación de datos probatorios, engaño en el tráfico jurídico mediante elaboración de datos, falsedad ideológica, uso de documentos falsos, alteración de datos , sabotaje informático, utilización abusiva de cheques o tarjetas de crédito

- Austria: La Ley de Reforma del Código Penal de diciembre de 1987 incorporó los delitos de destrucción de datos personales, no personales y contenidos en programas y la estafa informática.

- Francia desde 1988 existe una ley sobre fraude informático[10]

TRATADO DE CIBERCRIMINALIDAD DE BUDAPEST.

El Consejo Europeo desde el año 1997 se encontraba trabajando en un tratado que versara sobre ciberdelitos, finalmente el consejo aprobó un borrador al cuál se opuso la Cámara de Comercio de los Estados Unidos, así como numerosas organizaciones internacionales promotoras de los ciberderechos por considerarlo violatorio de los derechos de los consumidores y contrario al crecimiento económico de la industria de las tecnologías de la información. El 29 de junio de 2.001 el Comité Europeo de Problemas Criminales del Consejo de Europa, con el apoyo de los Estados Unidos aprobó el borrados final del tratado. El convenio sobre Cibercriminalidad se aprobó en Budapest el 23/11/2.001.

En el preámbulo se manifiesta la preocupación por los profundos cambios suscitados por el incremento, la convergencia y mundialización de las redes informáticas y la información electrónica sean utilizadas para cometer infracciones penales

---

[10] FERNANDEZ DELPECH, Horacio, Internet: Su Problemática Jurídica, Buenos Aires, Abeledo Perrot, pag. 151.

Reconoce a los fines de prevenir la cibercriminalidad la necesidad de llevar a cabo una política común adoptando una legislación apropiada.

Reconoce la necesidad de una cooperación entre los Estados y la industria privada en la lucha contra la cibercriminalidad y la necesidad de proteger los intereses legítimos vinculados con el desarrollo de estas tecnologías.

Habla de la necesidad de garantizar un equilibrio adecuado entre los intereses de acción represiva y el respeto de los derechos fundamentales del hombre plasmados en los convenios internacionales.

En su articulado luego de establecer en su artículo 1 el significado de algunos conceptos básicos tales como "sistema informático", "datos informáticos" , "prestador de servicio", datos de trafico" establece una serie de artículos en donde compromete a las partes a tomar medidas respecto a las siguientes infracciones (art. 2 a 11): acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la seguridad del sistema, abuso de equipos e instrumentos técnicos, falsedad informática, estafa informática, pornografía infantil, atentados a la propiedad intelectual.

Además incorpora en sus arts. 11 y s.s. normas regulatorias de la tentativa y complicidad, responsabilidad de las personas jurídicas, sanciones las cuales establece deberán ser "efectivas, proporcionadas y disuarorias, incluidas las penas privativas de la libertad", adopción de normas procesales necesarias.

El artículo 15 se refiere a las condiciones y garantías y establece: "Las partes velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y , en particular de los derechos derivados de la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto

Internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre y que debe integrar el principio de proporcionalidad". . ."

En sus arts. 16 al 21 habla de medidas para la conservación, divulgación, comunicación, registro y decomiso, interceptación de datos.

Así como normas referentes a competencia, cooperación internacional, extradición, colaboración, adhesión e implementación del convenio, etc.

ANTECEDENTES NACIONALES ANTERIORERS A LA LEY 26.388

Además de los antecedentes de las legislaciones de otros países contamos desde el año 2.001 con un instrumento capaz de brindar un marco, una guía para la elaboración de una legislación a nivel nacional que contemple esta nueva realidad, sin embargo nuestro legislador no dio sanción a una ley que contemplara los delitos informáticos hasta el año 2.008.

Sí, existían en nuestro país algunas leyes que regulaban alguna materia especial y dentro de estas se encontraba alguna regulación parcial de la materia informática.

- En el año 1997 ley penal tributaria y previsional nro 24769, su art. 12 reza. "será reprimido con prisión de dos a seis años, el que de cualquier modo sustrajere, suprimiere, ocultare, adulterare, modificare o inutilizarse los registros o soportes documentales o informáticos del fisco nacional relativos a las obligaciones tributarias o de recursos de la seguridad social, con el propósito de disimular la real situación fiscal de un obligado"

El bien jurídico protegido es la intangibilidad de los registros o soportes informáticos del Fisco nacional que se encuentren ligados con obligaciones de orden

tributario o con recursos destinados al sistema de seguridad social. Se protege el soporte informático en paridad con el soporte documental

- En el año 1997 en la ley 24766 de "Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos" se introdujo la protección del secreto de las informaciones de personas físicas o jurídicas almacenadas en medios informáticos (bases de datos), Art. 2. "la presente ley se aplicará a la información que conste en documentos, medios electrónicos o magnéticos, discos, ópticos, microfilmes, películas u otros elementos similares." Consagrando así la protección de la información contenida en bases de datos ya no estatales sino de la empresa y personas físicas.

- En el año 1998, la ley 25036 modifico la ley 11723 de propiedad intelectual brindando protección legal al software.

- En el año 2.000, a ley 25.286 de protección de datos personales (reglamentaria del proceso constitucional de Habeas Data, art. 43 C.N.) incorporó al Código Penal:

Uno dentro de los "delitos contra el honor" cuyo art. 117 quedo redactado de la siguiente manera: 1º Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales. 2ª la pena será de seis meses a tres años, al que proporcionar a un tercero a sabiendas información falsa contenida en un archivo de datos personales 3º la escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona. 4º cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el ejercicio de cargos públicos por el doble del tiempo que el de la condena". Este artículo fue criticado por su ubicación dentro de los delitos contra el honor porque el hecho de hacer insertar datos

falsos no necesariamente implica que se perjudique el honor de alguien, que incluso podría verse beneficiado pareciera que pudieran verse afectados con mayor claridad otros bienes como por ejemplo la fe pública, ya que hay un falseamiento de datos destinados a suministrarse cuando son requeridos debidamente. Cabe aclarar que el inciso 1 de este artículo hoy se encuentra derogado por la ley 26.388.

El otro artículo incorporado por esta ley se encuentra en el título V del código penal "Delitos contra la libertad", Cap. III "Violación de secretos" y es el art. 157 bis, el cual establece: "Será reprimido con la pena de prisión de un mes a dos años el que: 1º A sabiendas o ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos accediere, de cualquier forma a un banco de datos personales; 2º Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviera obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además pena de inhabilitación especial de uno a cuatro años.". Este artículo hoy se encuentra modificado por la ley 26.388. [11]

- La ley 25506 de firma digital:

Como ya dijimos en el año 2.001 la mayoría de los Códigos Penales modernos contemplaban este fenómeno de la criminalidad informática además de existir una Convención Internacional en la materia. En el año 2.006 se desata una polémica debido a la violación de correos electrónicos de varios periodistas y jueces. En junio de 2.006 se comenzó a debatir en las Comisiones de legislación penal, comunicaciones y Libertad de expresión de la Cámara de Diputados un proyecto de modificación al Código Penal presentado por la Diputada Diana Conti pero solo referida al correo electrónico, pero con el correr de los meses el congreso pensó que era conveniente ampliar el proyecto extendiendo el mismo a la regulación de otros delitos informáticos. A fines del año 2.006 la Cámara de Diputados

[11] RIQUERT, Marcelo Alfredo, Delitos Informáticos, http.7/wwwterragnijurista.com.ar/doctrina/delinfo2.htm,

aprobó el proyecto de ley, proyecto que fue estudiado durante el año 2.007 por algunas comisiones del Senado. Finalmente el Senado el 28/11/2.007 aprobó el proyecto con reformas y el 4/6/2.008, éste fue aprobado el proyecto por Diputados con lo que la ley obtuvo finalmente su sanción.

LEY 26.388

El 23 de noviembre de 2.001 se firma el Convenio de Cibercriminalidad de Budapest. Recién el 4 de junio de 2.008 (7 años después) se dicta la ley 26.388 de delitos informáticos " conforme a lo establecido por el convenio y la tendencia mundial que era la de adoptar por parte de los países medidas para penar y combatir la cibercriminalidad.

A los fines de una mejor comprensión de la reforma realizada por la ley 26388 a nuestro Código Penal realizare primero una enumeración de aquellas partes que fueron modificadas, para luego entrar en el análisis de cada una de ellas:

- LIBRO I: DISPOSICIONES GENERALES el TITULO XIII Significación de conceptos empleados en el Código.. Se incorpora un último párrafo al art. 77 y se diroga el art. 178 bis que había sido incorporado por la ley 25506

- LIBRO II: DE LOS DELITOS

. TITULO II- Delitos contra el honor. Deroga el inciso 1 del art. 117 bis

. TITULO III- Delitos contra la integridad sexual: Sustituye el art. 128

. TITULO V- Delitos contra la libertad:

Capítulo II:Violación de secretos: Sustituye el epígrafe que antes era Violación de secretos por el de Violación de Secretos y de la Privacidad. Sustituye el art. 153, 155, 157 y 157 bis e incorpora el art. 153 bis.

. TITULO VI: Delitos contra la Propiedad:

Capítulo IV: Estafas y otras defraudaciones: Incorpora al art. 173 un inciso .

Capítulo VII- Daños: Incorpora un segundo párrafo al art. 183 y sustituye el art. 184.

. TITULO VII- Delitos contra la seguridad pública:

Capítulo II: Delitos contra la seguridad de los medios de transporte y de comunicación: Sustituye el art. 197

. TITULO XI: Delitos contra la administración pública:

Capítulo V: Violación de sellos y documentos: Sustituye el art. 255

.

MODIFICACIÓN AL LIBRO I TÍTULO XIII

Incorpora algunos conceptos que van a repercutir en las descripciones contenidas en algunos tipos del código. Si bien la acción típica en estas figuras no va a cambiar, al modificarse estos conceptos aumentará la posibilidad que surjan nuevos hechos que queden bajo el ámbito de estos tipos penales.

El último párrafo del art. 77 incorporado establece: "El término documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento archivo o trasmisión. Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos instrumento privado y certificado comprende el documento digital firmado digitalmente."

O sea los conceptos ampliados son los de: DOCUMENTO, FIRMA y SUSCRIPCION e INSTRUMENTO PRIVADO y CERTIFICADO

La modificación del concepto de documento concuerda con el significado que la doctrina le venía dando con anterioridad a la reforma. El documento es ahora "toda representación de actos o hechos con independencia del soporte utilizado para su fijación."

El soporte tradicional utilizado para fijar el contenido de un documento era el papel, hoy el papel es solo uno de los tantos. Al respecto debemos tener en cuenta que el surgimiento de estas nuevas modalidades de soportes del contenido de un documento podrían plantear problemas tales como la durabilidad del mismo, la autenticidad, la inalterabilidad etc.[12]

La doctrina venía realizando esta interpretación del término documento que excedía al concepto tradicional en donde el soporte del documento era necesariamente el papel y algunas leyes anteriores, como las que hemos comentado supra venían considerando también este fenómeno del documento digital o electrónico.

La ley 25.506 de firma digital en su art. 6 establecía: "Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo,. Un documento digital también satisface el requerimiento de escritura"

Y en su art. 11 estableció: " Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales…"

En cuanto a las modificaciones realizadas al Código penal la ley 25506 de firma digital había equiparado el concepto de documento con el de instrumento exigiendo para la existencia de documento que éste estuviera firmado digitalmente. (art. 78 bis seg. Ley

[12] AGÜERO ITURBE, José Luis , El Dial .com, pág. 2.

25.506 hoy derogado: "… Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente" Con la derogación del art. 178 bis se suprime este requisito constituyendo el documento el género y el instrumento la especie.

En cuanto a la firma digital el art. 2 de la ley 25506 establece: "Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control"

Y el art. 5 de la misma ley dice: "Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerara como firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez"

En la práctica consiste en una clave que pertenece y es de exclusivo conocimiento del firmante de manera que se garantiza su autenticidad.

La diferencia entre firma digital y firma electrónica es que mientras aquella es el género , ésta es la especie, ya que la firma digital debe originarse en un certificado emitido por una autoridad habilitante y que debe tener vigencia en el tiempo, sin el cumplimiento de este requisito constituirá una firma electrónica, en cuyo caso la ley pone la carga de la prueba en caso de desconocimiento de su existencia en aquel sujeto que invocara su validez.

La Ley 25506 establece "Las disposiciones de esta ley no son aplicables: a) a las disposiciones por causa de muerte, b) A los actos jurídicos del derecho de familia; c) A los actos personalísimos en general; d) A los actos que deben ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de parte" por lo tanto ante la presencia de

alguno de estos casos no nos encontraríamos frente a un caso de falsificación, sin perjuicio que se pudiera configurar otro delito, como por ejemplo una estafa.

Como ya dijimos anteriormente algunas figuras que no son modificadas expresamente en su tipo van a verse modificadas en su extensión por la variación de los conceptos analizados, así por ejemplo: en el TítuloVI :Delitos contra la propiedad Capítulo III Extorsión: Art. 168: "Será reprimido con reclusión o prisión de cinco a diez años, el que con intimidación o simulando autoridad pública o falsa orden de la misma obligue a otro a entregar, enviar, depositar o poner a su disposición o la de un tercero, cosas dinero o documento, que produzcan efectos jurídicos. Incurrirá en la misma pena el que por los mismos medios o con violencia, obligue a otro a suscribir o destruir documentos de obligación o de crédito

También la incorporación de este nuevo alcance del término documento al art. 77 aumenta la cantidad de conductas que podían incluirse del Capítulo IV Estafas y otras defraudaciones ampliando de esta manera casi todos los incisos del art. 173.

O por ejemplo en el Título XII- Delitos contra la fe pública: el Capítulo I: Falsificación de moneda, billetes de banco títulos al portador y documentos de crédito los artículos 285 y 287 o el Capítulo III Falsificación de documentos en general. Art. 292 y ss etc.

MODIFICACIONES AL LIBRO II DEL CODIGO PENAL

DELITOS CONTRA LA INTEGRIDAD SEXUAL: PORNOGRAFÍA INFANTIL

El Convenio de Cibercriminalidad de Budpest en su artículo 9 establece que las partes adoptarán medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno la producción con la intención de difundir, el ofrecimiento o la puesta a disposición la difusión o trasmisión el hecho de procurarse o procurar a otro, pornografía infantil a través de un sistema informático.

Y define como pornografía infantil: "cualquier material pornográfico que represente de manera visual: a- un menor adoptando un comportamiento sexualmente explícito, b- una persona que aparece como un menor adoptando un comportamiento sexualmente explícito c- unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito.

Considera menor a los menores de 18 años, pero las partes podrán exigir un límite de edad inferior que debe ser como mínimo 16 años

Respecto del artículo 128 del código penal ha quedado redactado conforme a la ley 26.388 del siguiente modo: "Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un(1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a un menor de catorce (14) años.

La modificación es solo de los dos primeros párrafos del artículo, quedando el tercero como estaba en su redacción anterior.

Es un tipo de peligro abstracto y doloso

- En primer lugar el art. amplía las conductas típicas que en su redacción anterior solo eran la producción y la publicación agregando además la ***financiación,*** *ofrecimiento, comercialización,* ***facilitación****, divulgación y distribución.*

Las conductas de ***financiar y facilitar*** se encontraban ya de algún modo previstas ya que son conductas que encuadran dentro de la participación criminal y por lo tanto quedaban cubiertas por los arts. 45 y 46 del Código Penal.

En cuanto al *ofrecimiento, comercialización, divulgación y distribución* las mismas entraban dentro de los conceptos de producción y publicación.

- Además cambia el término "imágenes pornográficas por el de "toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales" y esto de acuerdo al protocolo relativo a la venta de niños, la prostitución infantil y la utilización de los niños en pornografía que complementa la convención de las Naciones Unidad sobre los Derechos del Niño al cuál adhirió nuestro país mediante la Ley 25.763, que en su artículo primero establece "Los Estados Parte prohíben la venta de niños, la prostitución infantil y la pornografía infantil, de conformidad con lo dispuesto en el presente Protocolo". En su artículo segundo: " A los efectos del presente Protocolo: c) Por pornografía infantil se entiende toda representación, por cualquier medio de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales" (igual fórmula utilizada por el nuevo artículo de nuestro Código Penal; y el artículo tercero establece: "Todo Estado Parte adoptará medidas para que, como ínimo, los actos y actividades que a continuación se enumeran queden íntegramente comprendidos en su legislación penal, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente: c) La producción distribución divulgación, importación, exportación, oferta, venta o posesión, con los fines antes señalados, de pornografía infantil, en el sentido en que se define en el artículo 2" Obligando en el punto 3 a que todo Estado Parte castigue estos delitos con penas adecuadas a su gravedad

A diferencia del protocolo no menciona la formulación del artículo de la ley no se refiere a actividades sexuales simuladas como estaban en el anteproyecto de la Cámara de Diputados, dicha exclusión se realizó por considerárselo controvertido.[13]

Toda representación incluye filmaciones, fotos, dibujos, dibujos digitalizados, caricaturas, pinturas, esculturas

Entendemos que cuándo el artículo habla de "la representación de sus partes genitales con fines **con fines predominantemente sexuales**" excluye del tipo aquellas situaciones que quedarían atrapadas sin esta frase como por ejemplo la imagen de un angelito desnudo en una iglesia o en un museo

En el segundo párrafo incorporado por la ley, ésta establece una figura atenuada con una pena de uno a cuatro años "al que tuviere en su poder imágenes de las descriptas en el párrafo anterior con fines inequívocos de comercialización o distribución." Este agregado "con fines inequívocos de comercialización o distribución". El Senado agregó este requisito que no existía en el proyecto de Diputados empresas tales como proveedoras de internet, empresas de telecomunicaciones etc. habían resistido duramente esta reforma, estas empresas pensaban que podía llegar a atribuírseles responsabilidad penal por los contenidos que transitaban o alojaban en sus servidores. El convenio de Budapest al establecer que conductas deben prever los estados como infracción penal, establece que los estados partes pueden reservarse el derecho de no aplicar la penalización de procurarse o procurar a otro pornografía infantil y la posesión de pornografía infantil

[13] PALAZZI, PABLO, Análisis del proyecto de ley de delitos informáticos aprobado por el Senado de la Nación en el año 2.007, Revista de Derecho Penal y Procesal Penal, Abril-Mayo 2.008, Lexis Nexis, Argentina, pág. 1.214.

Esta es una figura dolosa, por lo tanto quedan excluidos del tipo penal quienes no sabían que alojaban dichos contenidos en sus equipos y tampoco se reprime el consumo de pornografía aún cuando sea infantil, ni su mera tenencia si no es con esta finalidad [14]

DELITOS CONTRA LA LIBERTAD: VIOLACION DE SECRETOS Y DE LA PRIVACIDAD

La Constitución Nacional y los pactos internacionales con jerarquía constitucional protegen la inviolabilidad de la correspondencia y la privacidad, así los arts. 18 y 19 de la Constitución Nacional, el art. 11 apartado 2 del Pacto de San José de Costa Rica, el art. 17 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 12 de la Declaración Universal de Derechos Humanos y el art. 10 del Pacto sobre Derechos y Deberes del Hombre.

El artículo 3 de la ley sustituye el epígrafe del Capítulo III del Título V del Libro II del Código Penal que anteriormente era Violación de Secretos por el de Violación de secretos y de la privacidad.

A partir de Carmignani se han agrupado los tipos según el bien jurídico protegido. Los códigos han seguido este criterio. A veces en un mismo tipo penal existe la protección de no uno solo sino varios bienes jurídicos, pero el legislador los encuadra dentro del bien jurídico que fundamentalmente se protege, por esto los títulos del Código Penal nos marcan los bienes jurídicos que predominantemente protege el tipo penal, pero no exclusivamente

---

[14] CARBONE, Rolando Diego, Comentario a la Ley de Delitos Informáticos 26.388, Nuevos Delitos Viejos Delitos, Microjuris Argentina, Pág. 4..

En el título V se protege el bien jurídico Libertad, y en este Capítulo II la libertad en cuanto el derecho de los individuos a no sufrir intromisiones de terceros en su esfera de intimidad, o privacidad, y la prohibición de comunicación de sus secretos a otros. Es por este motivo que si bien éste no es un cambio sustancial porque como ya explicamos que el tipo penal aparezca como violatorio de un determinado bien jurídico no implica que se excluyan otros, y esto no va a influir en su interpretación , sin embargo aparece como más correcto: "La esfera de reserva de la persona, dentro de la cual tiene que poder vivir su intimidad sin la intromisión ilícita de terceros, se completa respecto de todo lo que desea mantener fuera del conocimiento de extraños o reducirlo al conocimiento de un número limitado, ya se trate de sus pensamientos, sus acciones o acontecimientos o circunstancias que le conciernan." Dentro de este capítulo se han modificado los artículos 153, 155, 157 y 157 bis, incorporándose además el artículo 153 bis.

Conforme al art. 73 C. P. los delitos de violación de secretos son delitos de acción privada , excepto los artículos 154 y 157 que regulan supuestos en los que el sujeto activo son empleados o funcionarios públicos , y por lo tanto el estado les impone una responsabilidad y tiene interés en que la misma se cumpla.

Artículo 153 según ley 26.388- "Será reprimido con prisión de quince (15) días a seis (6) meses que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente surpimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de

carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además inhabilitación especial por el doble del tiempo de la condena."

La ley no crea un nuevo tipo penal, sino que incorpora el delito de violación de correspondencia digital manteniendo prácticamente su redacción original y manteniendo su pena.

Agrega el término comunicación electrónica que antes había provocado problemas respecto a su tipicidad o atipicidad "… si bien en el caso "Lanata" se concluyó que el correo electrónico podía ser equiparado a la correspondencia tradicional en los términos de los arts. 153 y 155 la lectura del fallo dejaba un sabor de interpretación analógica de la ley penal"[15]

A la primera acción típica que consiste en "abrir" se le agrega la de "acceder indebidamente"

La palabra "indebidamente" significa sin derecho, y torna atípico el accionar de los proveedores de servicios de internet que conforme a las condiciones de sus contratos bloquean o filtran correo basura o virus.

Artículo 153 bis- "Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, al que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea a un sistema de datos informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión , si el acceso fuere en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."

[15] PALAZZI, PABLO, Análisis del proyecto... , obra cit, pag.1.218.

Este delitos podría constituir un paso previo a la comisión de otros delitos tales com la estafa, el daño, la sustracción de datos personales, etc. Es un delito doloso y de peligro abstracto , ya que no requiere el daño, que de producirse quedaría encuadrado dentro del tipo penal de la figura del daño.

Artículo 155- " Será reprimido con multa de pesos un mil quinientos ($1.500) a pesos cien mil ($100.000) , el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otro naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está excento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público"

El tipo penal dice "el que hallándose en posesión" tengamos en cuenta que si además hubiera habido apoderamiento ilegítimo esta figura se vería desplazada por el párrafo 3 del artículo 153.

Comunicar significa poner por cualquier medio ese contenido al alcance de un número indeterminado de personas[16]

Es una figura dolosa que requiere que quien publica conozca que la información no estaba destinada a la publicación.

El final del art. exime de responsabilidad a quien cometiere el hecho con el propósito inequívoco de proteger un interés público. Esta cláusula está destinada a proteger ala prensa. Quien invoque este extremo deberá acreditarlo y queda a criterio del juez la valoración del interés ya que la ley no aclara de que interés se trata.

---

[16] CREUS, Carlos, Derecho Penal Parte Especial, 3ra Edición Actualizada, Ed. Astrea 1991, Tomo I, pág. 380.

Artículo 157- "Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos actuaciones, documentos o datos, que por ley deben ser secretos"

La única modificación al artículo 157 es el agregado de la palabra "datos". Así se actualiza esta figura en la cual el sujeto debe ser un funcionario público que tomare conocimiento de datos, actuaciones, hechos o documentos que por ley sean secretos y que además el funcionario los revelare a pesar de conocer esta circunstancia.

Artículo 157 bis- "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos accediere , de cualquier forma, a un banco de datos personales.

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años."

Este artículo 157 bis regula la protección penal de los Bancos de Datos Personales

Unifica los artículos 117 bis (que dentro del título de los delitos contra el Honor penaba a quien hiciera insertar datos falsos en un archivo de datos personales) derogado por esta ley, y el artículo 157 bis, modificado.

Se consideró que los casos que encuadraban dentro del artículo 117 bis no siempre vulneraban el bien jurídico honor (no siempre hacer insertar datos falsos vulnera el honor de una persona, a veces hasta puede favorecerlo), por eso se entendió más acertado

incluírlo dentro de los delitos contra la privacidad derogando el art. 117 bis e incluyendo el contenido del mismo dentro del 157 bis.

Dentro del anteproyecto los delitos de insertar datos falsos y revelar información se trataban en dos artículos separados y consecutivos, pero la Cámara de Senadores consideró más correcto el tratamiento en un solo artículo penando con prisión de un mes a dos años al que – accediere (ilegítimamente o violando sistemas de confidencialidad y seguridad)

- proporcionare o revelare información.
- Insertare o hiciere insertar.

Recordemos que como mencionamos anteriormente el art. 73 establece a la violación se secretos, como así también a las calumnias e injurias como delitos de acción privadas con las excepciones contempladas en los arts. 154 y 157 C.P., podría plantearse el problema de si el art. 157 bis debe ser considerado un delito de acción pública o privada. Palazzi dice que se trata de un delito de acción privada ya que si el legislador de la ley 25326 hubiera querido contemplarlo dentro de las excepciones , así lo hubiera hecho expresamente[17]

Por último con respecto a la violación de secretos y de la privacidad, el proyecto de la Cámara de Diputados incluía un delito cuya acción típica era la obtención o captación de la imagen, sonidos o datos de una persona en forma ilegal y su posterior difusión. El senado no incluyó esta norma por considerar que constituía una punición exagerada y por el impacto que hubiera podido causar en el periodismo investigativo que utiliza las cámaras ocultas como medio para dar a conocer y detener los casos de corrupción.

DELITOS CONTRA LA PROPIEDAD

ESTAFA

[17] PALAZZI, PABLO, Análisis del proyecto... , obra cit, pag 1.118.

Artículo 172: “Será reprimido con prisión de un mes a seis años el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.”

Artículo 173: “Sin perjuicio de la disposición general del art. precedente se considerarán casos especiales de defraudación y sufrirán la pena que él establece:

Inc. 16: El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la trasmisión de datos.”

La estafa (incluida dentro del Título VI Delitos contra la Propiedad) se caracteriza por una disminución en el patrimonio por el error provocado en una persona que dispone del bien sustrayéndolo del patrimonio afectado sin saber que su acción es perjudicial para dicho patrimonio.

La estafa es “el hecho por medio del cual una persona toma a raíz de un error provocado por la acción del agente, una disposición patrimonial perjudicial, que dicho agente pretende convertir en beneficio propio o de un tercero”[18]

La estafa está caracterizada por la existencia de:

. Deterioro del patrimonio

. Fraude mediante ardid o engaño

. El fraude tiene que haber causado el error del sujeto.

. Debe existir una relación causal entre el error y la disposición patrimonial.

Antes de la reforma se perseguía penalmente la estafa mediante la interpretación que para algunos resultaba un poco forzada de considerar al ordenador como una voluntad susceptible de ser engañada, o sea se equiparaba a la computadora a una

[18] CREUS, Carlos, Derecho Penal Parte Especial… obra cit, pág. 490.

personal física víctima del engaño. Este problema se solucionó con la incorporación del inciso 16dentro de las defraudaciones especiales del art. 173.

Con respecto al proyecto de la Cámara de Diputados, la sanción definitiva de la ley suprimió la fórmula que decía "actuado sin autorización del legítimo usuario" por entenderse que agregaba un elemento confuso e innecesario al tipo , como así también suprimió "luego de su procesamiento" porque no se creyó conveniente fijar el momento técnico de una etapa de trasmisión de datos.

DAÑO

La jurisprudencia venía debatiendo desde hacía tiempo acerca de la tipicidad de los daños informáticos cuándo la destrucción o eliminación se producía sobre datos archivos o programas, y a discusión se producía en torno de sí podían estos ser considerados "cosas".

La exigencia de una cosa para la configuración de ciertos delitos dentro de nuestro Código Penal era una de las causas de inadecuación con anterioridad de la sanción de la ley. Había casos en los que el delito no quedaba configurado cuando se trataba de bienes intangibles como ser el delito de hurto o robo cuando se trataba de una sustracción de datos , o el delito de daño en los casos en que la destrucción se produjera sobre bienes inmateriales aún siendo a veces ésta tanto o más grave que el perjuicio que se pudiera causar por la destrucción de bienes materiales .[19]

[19] ALTMARK, Daniel R., Informática y Deerecho, Aportes de doctrina Internacional, Ed. De Palma, 1988, pág. 24.

En el caso “Pinamonti” la jurisprudencia entendió que el borrado o destrucción de un programa de computación no es una conducta aprehendida en el art. 183 pues el concepto de cosa es aplicable al soporte y no a su contenido.[20]

Algunos autores entendieron que a partir de la incorporación del segundo párrafo al art. 2311 de nuestro Código Civil por la ley 17711, que expresa que las disposiciones referentes a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de tener un valor, el concepto de cosa estaría más cercano al concepto francés citado por Velez Sardfield en su nota “todo aquello que existe se denomina cosa” , y no al de Freitas (citado en la misma nota.)[21], más aún algunos autores dicen que al adoptar la información de una computadora la forma de energía y la energía tener carácter de cosa conforme al art. 2311 C.C. le sería aplicable el concepto de daño[22].

Lo cierto es que este problema planteado durante largo tiempo en la doctrina y jurisprudencia nacional queda totalmente finalizado con la sanción de la ley que nos ocupa.

El art. 183 del Código Penal establece: “Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito m´s severamente penado”

La ley 26388 incorpora como segundo párrafo del art. 183 el siguiente: “En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños”.

---

[20] CAMARA NACIONAL CRIMINAL Y CORRECCIONAL, sala 6ta , 30 de abril de 1993, Pinamonti, Orlando M. , Jurisprudencia Argentina, 1998, pag. 14.

[21] EMERY, Miguel Angel, Delitos Informáticos, MJ-DOC-1921-AR. ED, 198-514, 0170272.002

[22] FERNANDEZ DELPECH, Horacio, Protección Jurídica del Software, Abeledo Perrot, Buenos Aires , pág.. 6

Esta segunda parte del inciso incluye el verbo “alterar” y excluye “hacer desaparecer” y “o de cualquier modo dañare” , sin embargo pensamos que las acciones típicas no difieren del daño común ya que destruir o inutilizar incluyen el concepto de hacer desaparecer.

La acción de borrar debe considerarse en cada caso ya que muchas veces la información borrada queda en el llamado basurero.

La existencia de back up no altera la configuración del delito de daño [23]

Otro aspecto a tener en cuenta que el segundo párrafo agregado al art. 183 no dice como el primero “total o parcialmente ajeno” con lo cuál podrían estar alcanzados por esta figura penal aquellos sistemas de anticopia introducidos por los propios programadores o fabricantes.

El delito puede recaer sobre datos, documentos, programas o sistemas informáticos.

También la reforma modifica el art. 184 referido al delito de daño calificado, incorporando al daño informático, y constituyéndolo así como una forma agravada del daño del art. 183.

Así el art. establece una pena de 3 meses a 4 años de prisión (no modifica la pena establecida por el código en su redacción anterior , si mediare cualquiera de las siguientes circunstancias:

Conserva intacta la redacción de los primeros cuatro incisos 1) Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones; 2) Producir infección o contagio en aves u otros animales domésticos; 3) Emplear substancias venenosas o corrosivas; 4) Cometer el delitos en despoblado y en banda.

---

[23] PALAZZI, PABLO, Análisis del proyecto... , obra cit, pag. 1.220.

En lo que respecta al inciso 5) que anteriormente decía “Ejecutarlo en archivos, registros, bibliotecas, museos o puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos”; agrega lo siguiente: “o en datos , documentos programas o sistemas informáticos públicos”.

Y además agrega un nuevo inciso: Inciso 6) “Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones de provisión o transporte de energía, de medios de transporte u otro servicio público.”

DELITOS CONTRA LA SEGURIDAD PÚBLICA: CONTRA LA SEGURIDAD DE LOS MEDIOS DE TRANSPORTE Y COMUNICACIÓN

Dentro del Título VII Delitos contra la Seguridad Pública encontramos el Capítulo II: Delitos contra los medios de transporte y comunicación dentro del mismo el art. 197 establecía en su redacción anterior a la ley que nos ocupa: “ Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica o telefónica o resistiere violentamente el restablecimiento de la comunicación interrumpida”.

El artículo en su nueva redacción conserva la pena de seis meses a dos años de prisión al que “interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida”

Con la incorporación de “o de otra naturaleza” agrega a las comunicaciones tradicionales todas las nuevas formas de comunicación (celulares, correo electrónico, chat mensajes de texto ya sea por celulares o computadoras etc.)

DELITOS CONTRA LA ADMINISTRACIÓN PÚBLICA:VIOLACIÓN DE SELLOS Y DOCUMENTOS

Dentro del Título XI, el Capítulo V denominado Violación de sellos y documentos incluye el art. 255 que en su redacción anterior establecía "Será reprimido con prisión de un mes a cuatro años, el que sustrajere, ocultare, destruyere, inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público, Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de doscientos cincuenta pesos como mínimo y doce mil quinientos pesos como máximo".

En su nueva redacción el artículo queda expresado de la siguiente manera: "será reprimido con prisión de un mes a cuatro años , el que sustrajere, alterare, ocultare, destruyere, inutilizare, en todo o en parte, objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble de tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($750) a pesos doce mil quinientos ($12.500).

CONCLUSION

La innovación en lo que a tecnología informática se refiere ha dado lugar a una nueva realidad social que se ha desarrollado súbita e inimaginablemente. Este fenómeno tiene características propias y da lugar a una nueva categoría que hoy denominamos "ilícitos informáticos".

Es correcto entonces hablar hoy del ilícito informático como concepto, pero entendiendo que no cualquier ilícito constituye un delito informático, sino que para su existencia es necesaria una conducta humana, antijurídica, culpable, seleccionada por el derecho penal mediante su inclusión en un llamado "tipo" por medio del cual se le impone una pena, y que tiene como medio de ejecución o como objeto la informática; si no nos encontramos ante este supuesto, no podemos hablar delito informático.

El derecho comparado se había ocupado de este fenómeno con mucha anterioridad respecto de nuestro país, quien a pesar de contar con tales antecedentes, así como con la existencia de un tratado que, desde 1997, hubiera podido servir de modelo para la

elaboración de una legislación propia; demoró la sanción de una ley que se ocupara del tema (no solo de algún aspecto parcial como lo habían hecho leyes anteriores), hasta el año 2.008.

Creemos que la sanción de esta ley constituye un avance positivo de nuestra legislación nacional, pero no debemos olvidar que así como el avance tecnológico es constante, debe el legislador estar atento a los cambios en la realidad para que nuestras leyes se vayan adecuando a la misma. También nos parece importante la consideración por parte de nuestro legislador de temas tales como el que se refiere a la investigación y prueba de los delitos informáticos, evaluando la posibilidad de reformar los códigos procesales.

La elaboración de las normas jurídicas adecuadas y en el tiempo oportuno realizada por el legislador es indispensable, pero además la correcta aplicación de las mismas, la cual se logra mediante la capacitación de los operadores tanto del sistema policial como judicial, es la clave del éxito de la lucha contra este fenómeno que tratamos: el delito informático.

BIBLIOGRAFÍA

* AGÜERO ITURBE, José Luis, El Dial.com.-

* ALTMARK, Daniel R., Informática y Deerecho, Aportes de doctrina Internacional, Ed. De Palma, 1988.-

* BIBIANA, Luz Clara, Manual de Derecho Informático, Editorial Jurídica Nova Tesis, Rosario, Santa Fe, 2.001.-

* CAMARA NACIONAL CRIMINAL Y CORRECCIONAL, sala 6ta , 30 de abril de 1993, Pinamonti, Orlando M. , Jurisprudencia Argentina, 1998.-

* CARBONE, Rolando Diego, Microjuris.com.-

* CARBONE, Rolando Diego, Comentario a la Ley de Delitos Informáticos 26.388, Nuevos Delitos Viejos Delitos, Microjuris Argentina.-

* CREUS, Carlos Derecho Penal Parte General, 4ª Edición actualizada y ampliada, Editorial Astrea de Alfredo y Ricardo Depalma, Buenos Aires, 1996.-

* CREUS, Carlos, Derecho Penal Parte Especial, 3ra Edición Actualizada, Ed. Astrea 1991.-

* EMERY, Miguel Angel, Delitos Informáticos, MJ-DOC-1921-AR. ED, 198-514.-

* FERNANDEZ DELPECH, Horacio, Internet: Su Problemática Jurídica, Buenos Aires, Abeledo Perrot.-

* FERNANDEZ DELPECH, Horacio, Protección Jurídica del Software, Abeledo Perrot, Buenos Aires.-

* PALAZZI, PABLO, Análisis del proyecto de ley de delitos informáticos aprobado por el Senado de la Nación en el año 2.007, Revista de Derecho Penal y Procesal Penal, Abril-Mayo 2.008, Lexis Nexis, Argentina.-

* PALAZZI, Pablo A. Delitos Informáticos. Ed. Ad Hoc Buenos Aires.-

*RIQUERT, Alfredo Marcelo, Delitos Informáticos. http//www.terragnjurista.com.ar/doctrina/delinfo2.htm.-

* ZAFFARONI, Eugenio Raúl, Manual de Derecho Penal, Parte General, Ediar, 2.005, Capital Federal.-

* Derecho Informática 1: Editorial Juris – Año 2000, Directora Faustina Zarich, pág. 16/19 y 26/28.-

* Revista de Doctrina y Jurisprudencia de la Provincia de Santa Fe N° 53, Editorial Panamericana – Año 2003, Director Jorge Walter Peyrano.-