UNIVERSIDAD NACIONAL DE LA PAMPA

Facultad de Ciencias Económicas y Jurídicas

Seminario Sobre Aportaciones Teóricas y Técnicas Recientes

TITULO:"DELITOS INFORMATICOS: CUESTIONES DOGMATICAS Y DESAFIOS POLITICO CRIMINALES DE LA MODERNIDAD TARDIA"

Alumno: PEREZ, Mauro Nicolás
MEZZASALMA, Marco Daniel

Asignatura sobre la que se realiza el trabajo:

Encargado de curso Prof:

Año que se realiza el trabajo: 2009

Introducción

Con el importante avance que ha experimentado la tecnología en los últimos tiempos, la informática se ha convertido en un poderoso instrumento que proporciona infinitas posibilidades de desarrollo y progreso. Pero al compás de su irrupción y con el devenir de los mismos, también se aprecia a la par una faz negativa en cuanto a su implementación.

Así, el desarrollo obrado en este campo específicamente ha otorgado a la delincuencia, primordialmente, un nuevo medio comisivo para alcanzar sus fines, a lo cual el legislador ha debido reaccionar ante esta nueva realidad.

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas tradicionales tales como robo, hurtos, fraudes, falsificaciones, perjuicios, estafas y sabotajes. Sin embargo debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Este trabajo se encamina realizar un análisis de alguno de los delitos incorporados en el código penal en el marco de la nueva ley 26.388/08 acompañando la tendencia mundial de repudiar este tipo de conductas que generaban incertidumbre legislativa.

Asimismo, repasaremos la legislación de los países más importantes que han decidido incorporar los delitos informáticos.

Por último brindaremos nuestra conclusión atento lo expuesto en el presente trabajo.

CAPITULO I

ASPECTOS GENERALES DEL DELITO INFORMATICO

1. ¿Qué es el delito informático?

Se estima que no existe una definición universal y formal de delito informático, pero se han formulado conceptos respondiendo a realidades nacionales concretas: “no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que hablar de “delitos” como acción típica, es decir tipificada o contempladas en textos jurídicos penales, se requiere que la expresión “delitos informáticos” este consignada en los códigos penales,

lo cual nuestro país al igual que en otros no ha sido objeto de tipificación aún"[1].

El italiano Carlos Sarzana, sostiene que los delitos informáticos son cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo.

La Organización de Cooperación y Desarrollo Económico (OCDE) publicó un estudio sobre delitos informáticos y lo define como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos"[2].

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma".[3]

Este organismo elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los distintos países pudieran constituir un marco de seguridad para los sistemas informáticos:

- en esta delincuencia se trata de especialistas capaces de efectuar el crimen y borrar toda huella de los hechos haciendo dificultosa o imposible su investigación;

[1] TELLES VALDEZ, Julio. *Derecho Informático*. 2ª edición. Mc Graw Hill. México. 1996 página. 103-104.
[2] MOLINER, Maria. *Diccionario de Maria Moliner*. Edición Digital.
[3] Definición elaborada por un grupo de expertos invitados por la OCDE a París en mayo de 1993

- la legislación sobre sistemas informáticos debería acercarse a los distintos medios de protección existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

2. Clasificación

Téllez Valdez los clasifica en base a dos criterios:

I. Como instrumento o medio: conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito (Ej: falsificación de documento vía computarizada: tarjetas de créditos, cheques, etc.).

II. Como fin u objetivo: conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física (Ej: secuestro de soportes magnéticos con información valiosa, para ser utilizadas con fines delictivos).

María Luz Lima presenta la siguiente clasificación de "delitos electrónicos"[4]:

I. Como método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

II. Como medio: conductas criminales en donde para realizar un delito utilizan una computadora como medio a símbolo.

[4] LIMA de la LUZ, María. *Delitos electrónicos.* Criminalia Nº 1-6 año L.. Ediciones Porrua .México. Enero-Julio 1984

III. Como fin: conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla

3. Características

Téllez Valdez sostiene las siguientes características:

I. Solo determinada cantidad de personas con conocimientos técnicos específicos pueden llegara a cometerlos.

II. Son conductas criminales del tipo "cuello blanco"[5], en cuanto al sujeto que los comete atento que generalmente los comete alguien con cierto status socioeconómico no vinculado con la pobreza, carencia de recursos, baja educación, poca inteligencia ni inestabilidad emocional.

III. Generalmente se realizan cuando la víctima esta trabajando.

IV. Provocan perdidas económicas.

V. Son muchos los casos y pocas las denuncias por la falta de regulación y por el miedo al descrédito de la entidad atacada. Generalmente son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

VI. Son de difícil comprobación.

4. Delincuente y Víctima.

- **Sujeto Activo**

[5] Término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año 1943

Se llama así a las personas que cometen delitos informáticos. Presentan características que no poseen el denominador común de los delincuentes. Tienen habilidades para el manejo de sistemas informáticos y generalmente por su situación laboral, se encuentran en lugares estratégicos donde manejan información de carácter sensible.

A las personas que cometen esta clase de delitos no se los considera delincuentes, no se los segrega, no se los desprecia ni desvaloriza; por el contrario, es considerado y se considera a sí mismo “respetable”.

- **Sujeto Pasivo**

Es la víctima del delito, ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, ya que puede presentar diferentes características e identificarse como personas físicas, instituciones crediticias, militares, gobiernos, etc., que utilizan sistemas automatizados de información, generalmente conectados a otros.

CAPITULO II

LEGISLACION

1. Derecho Comparado

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de

computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

a) Alemania

En este país, para hacer frente a la delincuencia relacionada con la informática, se adoptó el 15 de mayo de 1986, la Segunda Ley contra la Criminalidad Económica, reformando el Código Penal, incorporando los siguientes delitos:

- Espionaje de datos
- Estafa Informática
- Falsificación de datos probatorios junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica y uso de documentos falsos
- Alteración de datos
- Sabotaje informático
- Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa
- Utilización abusiva de cheques o tarjetas de crédito

b) España[6]

[6] http://www.delitosinformaticos.com/delitos/codigopenal.shtml

España quizás sea el país con mayor experiencia en la materia en toda Europa.

Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP), aprobada el 15 de diciembre de 1999, contempla la mayor cantidad de acciones lesivas sobre la información, aplicando penas de prisión y multa, agravándolas cuando existe intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.

Descubrimiento y revelación de secretos: Artículo 197 C.P.

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

Se trata de un delito contra la intimidad, por ello la interceptación del correo electrónico se asimila a la violación de la correspondencia.

El código penal no había previsto las modalidades comisivas consistentes en el uso de las tecnologías de la información para invadir la intimidad de las personas o para violar, acceder o descubrir sus secretos.

Mero acceso no consentido: Conocido como hacking directo: acceso indebido o no autorizado con el único ánimo de vulnerar el password sin ánimo delictivo adicional.

No se encuentra penado en el código penal.

Hacking indirecto: Supone un acceso no consentido al ordenador o sistema informático como medio para cometer diferentes conductas delictivas. Se castiga por el delito finalmente cometido. (ej, daños, interceptación del correo electrónico, etc).

Espionaje informático empresarial: Artículo 278 C.P. Aquí el bien jurídico protegido es el secreto empresarial, la información almacenada informáticamente que supone un valor económico para la empresa porque confiere al titular una posición ventajosa en el mercado.

Daños informáticos o sabotaje: Artículo 264.2 C.P.

La misma pena se impondrá 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.

Se trata de los daños causados en el sistema informático mediante la introducción de virus y bombas lógicas.

En el código penal anterior sólo se preveía la destrucción de bienes materiales, por lo que los daños causados a bienes inmateriales no estaban incluidos en este delito.

Pornografía infantil: Artículo 189 C.P. En este caso se incluye la expresión "el que por cualquier medio" con el fin de incluir Internet como medio para cometer este delito.

Delitos tradicionales existentes hasta ahora en el código penal y que son de perfecta aplicación a los cometidos por medios informáticos:

Difusión y exhibición de material pornográfico a menores: El artículo 186 C.P castiga el hecho de exhibir material pornográfico a menores a través de cualquier medio, por ejemplo el correo electrónico.

Calumnia: Artículos 205 y 206 C.P

Injuria: Artículo 208 y 209 C.P. Es posible llevar a cabo estos delitos a través del correo electrónico o incluso a través de terminales móviles.

Calumnias e injurias hechas con publicidad: Artículo 211 C.P. En este supuesto cabe perfectamente la difusión de mensajes injuriosos o calumniosos a través de Internet.

Delito tradicional de daños: Artículo 263 C.P

Hurto: Artículo 234 C.P

Robo: Artículo 237 C.P. Se requiere el uso de la fuerza en las cosas. El artículo 238 establece que se realiza el robo con fuerza cuando se llevan a cabo con llaves falsas, que según el artículo 239 llaves falsas son las tarjetas, y los mandos o instrumentos de apertura a distancia.

Defraudaciones de fluido eléctrico: Artículo 255 C.P. Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones (televisión, teléfono, etc) u otro elemento, energía o fluido ajenos

Defraudación a través de equipo terminal de comunicaciones: Artículo 256 C.P Se refiere al uso no autorizado o abusivo de terminales de telecomunicaciones.

Delitos contra la propiedad intelectual: Artículo 270 C.P.

Delitos contra la propiedad industrial. Artículo 273 C.P.

Publicidad ilícita: Artículo 282 C.P.

Falsedad de documento público: Artículo 390 C.P.

Falsedad de documento privado: Artículo 395 C.P.

c) Francia

El 5 de enero de 1988 sanciona la ley 88/19 sobre fraude informático que contempla:

- Acceso Fraudulento a un sistema de elaboración de datos
- Sabotaje Informático
- Destrucción de Datos
- Falsificación de Documentos Informatizados con intención de causar un perjuicio a otro

El Parlamento francés ha aprobado recientemente la reforma de la ley de propiedad intelectual que, entre otras cosas, regulará las descargas a través de Internet. La nueva normativa establece multas para quienes descarguen música sin permiso y crea una nueva autoridad encargada de vigilar que se cumpla la norma. A partir de ahora, el titular de una conexión a Internet debe vigilar que su acceso no sea usado para descargar obras intelectuales de la red.

d) Inglaterra

En agosto de 1990 la Computer Misuse Act (Ley de Abusos Informáticos) comenzó a regir en Inglaterra, por la cual todo intento de alterar datos informáticos con fines delictivos se castiga con hasta cinco años de cárcel o multas sin límite.

La ley se puede considerar dividida en tres partes:

- Hackear: Ingresar sin permiso a una computadora,
- Hacer algo con la computadora hackeada,
- Realizar alguna modificación no autorizada.

e) Estados Unidos

En 1976, el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985. Esta ley significó el antecedente para que Estados como Rhode Island, Florida, Michigan, Colorado y Arizona se constituyeran en los primeros con legislación específica, anticipándose al dictado de la Computer Fraud and Abuse Act de 1986. Esta última se refiere a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales.

En 1994 se adoptó el Acta de Abuso Computacional, modificando el Acta de 1986, introduciendo la regulación de los virus y conceptualizándolos. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

A nivel Institucional, cuentan con la Federal Computers Investigation Comitee (FCIC), organización más importante e influyente referente a delitos computacionales, es la entrenadora de las restantes fuerzas

policiales a nivel informático y el primer organismo establecido a nivel nacional.

Asimismo existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), que investiga nuevas técnicas para dividir un sistema en partes, sin destruir las evidencias, actuando en países como Canadá, Taiwán e Irlanda.

f) Chile

Fue el primer país Latinoamericano en sancionar una Ley contra Delitos Informáticos (Ley 19223) el 7 de junio de 1993.

Señala que la destrucción o inutilización de un sistema de tratamiento de información, puede ser castigado con prisión de un año y medio a cinco.

Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y cinco años.

El Hacking, definido como el ingreso a un sistema, o su interferencia con el ánimo de apoderarse, usar, o conocer de manera indebida la información contenida en éste, también es pasible de condena de hasta cinco años de

cárcel; pero ingresar en este mismo sistema si permiso y sin intenciones de ver su contenido, no constituye delito.

Dar a conocer la información almacenada en un sistema, puede ser castigado con prisión de hasta tres años, pero si el que o hace es el responsable de dicho sistema, puede aumentar a cinco años.

2. Evolución en el Derecho Argentino

Nuestra legislación regulaba Comercial y Penalmente las conductas ilícitas relacionadas con la informática, pero no contemplaban en sí los delitos informáticos. En efecto la misma se regía por las siguientes disposiciones:

- La Ley 111 de Patente de Invención que regula la protección a la Propiedad Intelectual
- La Ley Penal 11.723 de Propiedad Científica, Literaria y Artística. Por ella solo estaban protegidos los lenguajes de bases de datos, planillas de cálculos, el software y su documentación dentro del mismo.

De acuerdo con los artículos 1072 y 1311 del Código Civil y 183 del Código Penal se especifica para que exista robo o hurto debe afectarse una “cosa”, y las leyes la definen como algo que ocupa lugar en el espacio; los datos son intangibles.

En resumen, si alguien destruía, mediante los métodos que sean, la información almacenada en una computadora, no cometía delito; pero si rompió el hardware o el disquete será penalizado: en ese caso, deberá hacerse cargo de los costos de cada elemento pero no de lo que contenía.

Dentro del Código Penal se encuentran sanciones respecto de los delitos contra el honor (Arts. 109 a 117 C.P.); instigación a cometer delitos (Art. 209 C.P.); instigación al suicidio (Art. 83 C.P.); hurto (Art. 162 C.P.); estafas (Art. 172 C.P.), además de los de defraudación, falsificación, tráfico de menores, narcotráfico, etc., todas conductas que pueden ser cometidas utilizando como medio la tecnología electrónica, pero nada referente a delitos cometidos sobre la información como bien.

Así las acciones comunes de hurto, robo, daño, falsificación, etc., NO podían aplicarse a los datos almacenados por considerarlos intangibles.

Hablar de estafa (Art. 172 C.P.), no era aplicable a una máquina porque se la concibe como algo que no es susceptible de caer en error.

En función del Código Penal se considera que entrar en un domicilio sin permiso o violar correspondencia constituye delito (Art. 153 C.P.), pero el acceso a una computadora, red de computadoras o medios de transmisión de información sin autorización, no constituían un acto penable, aunque si el daño al mismo.

Por otra parte, si ocurría un hecho delictivo por medio del ingreso a varias páginas de un sitio distribuidas por distintos países: ¿qué juez sería

competente en la causa?. ¿Hasta qué punto se pueden regular los delitos a través de internet sabiendo que no se pueden aplicar las leyes en forma extraterritorial?. Todos ellos, interrogantes que hasta el momento no tienen respuestas.

En febrero de 1997 se sancionó la Ley 24.766 por la que se protege la información confidencial a través de acciones penales y civiles. Por medio de ellas la sustracción de disquetes, acceso sin autorización a una red o computadora que contenga información confidencial, será sancionado a través de la pena de violación de secreto. Los posibles hechos de hacking se encuadran en la categoría de delitos comunes como defraudaciones, estafas o abuso de confianza, y la existencia de una computadora no modifica el castigo impuesto por la ley.

Lo gracioso y paradójico es que no existía sanción legal para la persona que destruía información almacenada en un soporte, pero sí para la que lo hacía respecto de la impresa en un papel.[7]

Este era el panorama jurídico que se planteaba antes de la reforma al Código Penal en el año 2008 que posteriormente analizaremos.

Asímismo comentaremos un fallo que reflejaba la situación a que hacíamos referencia:

[7] ARDITA, Julio Cesar. Director de Cybsec S.A.. Security System ex Hacker. Entrevista personal, 15 de enero de 2001. http://www.cybsec.com

Según la jueza correccional porteña Ana Elena Díaz Cano, hackear una cuenta de mail no es delito. Fue a raíz de la denuncia de un abogado, quien dijo que su cuenta de correo electrónico fue violada y que la información se usó en su contra en un juicio civil. La magistrada sostuvo que la legislación actual no prevé ese tipo de conductas y desestimó la querella.

El denunciante entendió que los hechos podían ser enmarcados en las previsiones del art.153 del Código Penal. Sin embargo, el fiscal dijo que el injusto denunciado encontraría, “prima facie” adecuación típica, en el Art. 157 bis del citado texto legal, por lo que al ser privado el ejercicio de la correspondiente acción penal, postuló que no le correspondía a dicho Ministerio Público, intervenir en su tramitación.

La jueza de la causa en su análisis del artículo 153 C.P. explica: “Si bien todo permite afirmar que la ley dibuja qué cosas son objeto de tutela, refiriéndose de modo principal a la correspondencia postal y a los papeles privados, exige que se hallen en la esfera de custodia o en propiedad de determinada persona. La literalidad del primer aspecto de la norma plantea algunos inconvenientes, a la hora de ajustarlos a las conductas denunciadas”. Tras manifestar que “la caracterización del mensaje que se envía por la red es parecida a la postal, en el sentido en que ambas son formas de comunicación de ideas, no son exactamente iguales”, de esa manera, “lo violado no fue una correspondencia de e mail, sino

simplemente datos almacenados o archivados en el sistema informático del agraviado".

Sin embargo, y tomando en cuenta una visión amplia de la cuestión, "lo cierto es que el verbo típico relacionado con ellos resulta ser el de apoderarse de manera indebida de los mismos, es decir sacarlos de la esfera de custodia, lo que tampoco sucede en el caso de autos, ya que en ningún momento por más que se haya conocido de los datos informáticos de la víctima, por parte del o los intrusos, lo real es que dichos datos, por el mecanismo propio de esa clase de información, no dejaron de encontrarse en el ámbito de vigilancia de su creador".[8]

3. Proyecto de Ley

En el año 2006, se desató la polémica por la violación de correos electrónicos de varios periodistas y jueces, a raíz de una denuncia realizada por un importante diario de la Capital Federal. Inmediatamente se presentaron en el Congreso varios proyectos de leyes relacionados con el correo electrónico. En junio de ese año, comenzó a debatirse en las comisiones de Legislación Penal, Comunicaciones y Libertad de Expresión de la Cámara de Diputados, un proyecto de modificación del Código Penal, presentado por la diputada Diana Conti. La iniciativa, que igualaba la intromisión en correos electrónicos con las misivas en papel, proponía

[8] Juzgado en lo Correccional Nº 9. Provincia de Buenos Aires. 11/04/2007. "*Esteban Gálvez s/denuncia*", Expte. Nº 68.243. http://www.portaldeabogados.com.ar.

penas de hasta diez años de prisión para la violación del correo electrónico por parte de funcionarios públicos o miembros de fuerzas de seguridad. Con el correr de los meses, el Congreso creyó que era mejor introducir una reforma no sólo referida al correo electrónico, sino a otros delitos informáticos.

A fines del 2006, luego de un amplio debate de sus comisiones, la cámara de diputados aprobó el proyecto de ley. El mismo contemplaba los delitos más tradicionales como la estafa informática, el daño informático, el acceso no autorizado a un ordenador, falsificación de documentos digitales, y la violación de correspondencia digital, correo electrónico y cualquier medio de comunicación moderno, así como su interrupción, delitos relacionados con la pedofilia y distribución de virus informáticos.

El 28 de noviembre de 2007, el Senado aprobó con reformas el proyecto que había sido aprobado con media sanción en el año anterior. La reforma del Senado conserva la factura inicial que le dio la Cámara de Diputados.

Se trata de una reforma al Código Penal, no de una ley de delitos informáticos. Por eso, no crea nuevos delitos sino que se modifican ciertos aspectos de los existentes para receptar las nuevas tecnologías.

Finalmente, este proyecto fue sancionado el 4 de junio de 2008, y promulgado de hecho el 24 de junio del mismo año, con las reformas introducidas oportunamente por el Senado de la Nación.

4. Análisis al Proyecto y Ley 26388.

a) Definiciones

La primera reforma, incorpora al artículo 77 del Código Penal las siguientes definiciones:

- El término “documento” comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
- Los términos “firma” y “suscripción” comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
- Los términos “instrumento privado” y “certificado” comprenden el documento digital firmado digitalmente.

2) Ofrecimiento y Distribución de imágenes relacionadas con la pornografía infantil.

Internet se ha convertido en el medio principal para que los pedófilos intercambien archivos y fotografías de menores, superando con su accionar las fronteras locales. Resultaba necesario que el Código Penal contemple esta nueva modalidad delictual, sobre todo para cumplir con los compromisos internacionales que hemos adoptado.

En nuestro país, la ley 25.763 aprobó el Protocolo relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía, que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño (de rango Constitucional). Su primer artículo dispone que “Los Estados Parte prohibirán la venta de niños, la prostitución infantil y la pornografía infantil”. 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.

El proyecto proponía sustituir el artículo 128, por el siguiente: “Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, *por cualquier medio*, toda representación de un menor de dieciocho 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 meses a dos 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 mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años”.

En la versión de Diputados, la reforma del art. 128 había dejado de lado (por error involuntario) la figura del que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren menores. La versión del Senado la incorpora.

Finalmente, en relación al proyecto de Diputados el Senado alteró las penas que el proyecto prevé para la producción y la tenencia, y se agregó un requisito más a la tenencia para penalizar sólo aquella que tenga fines inequívocos de comercialización o distribución.

Esta nueva figura generó preocupación en las empresas que actúan como intermediarios en Internet, quienes consideraron que podría llegar a imputárseles responsabilidad penal por los contenidos que transitan en sus servidores, pese a que usualmente no tiene conocimiento acabado de la ilicitud del contenido. No obstante se considera que se trata de una figura dolosa, como también lo hace casi toda la doctrina y jurisprudencia foránea.[9]

Asímismo por ser una figura de tenencia o posesión, se ha planteado el problema de los usuarios que poseen en sus discos una imagen sin conocimiento de es dicha posesión. Aquí también falta el dolo que hace que no exista delito. Tampoco habría, en principio, finalidad de distribuir o comercializar que exige el art. 128.

---

[9] GOMEZ TOMILLO, Manuel. *Responsabilidad Penal y Civil por delitos cometidos a través de Internet. Especial consideración del caso de proveedores de contenidos, servicios, accesos y enlaces*. Thomson-Aranzadi, 2da edición, pág. 123.

3) Violación de Secretos y de la Privacidad

a) Nuevo epígrafe para el C.P.: El derecho a la privacidad.

La reforma del Senado conservó la propuesta de Diputados de ampliar el epígrafe del capítulo III, del título V, de la parte especial del Código Penal, incluyendo a la privacidad como bien jurídico protegido, explicitando el campo de atentados contra la libertad individual, al consagrar que la persona tiene una esfera de intimidad y privacidad de la cual dispone a su arbitrio, y que no es lícito que terceros se entrometan afectándola.

b) Violación de correspondencia digital.

El proyecto sustituye el art. 153 por el siguiente: “Será reprimido con prisión de quince días a seis meses el 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 suprimiere o desviare de su destino una correspondencia o una *comunicación electrónica* que no le esté dirigida”.

Se agrega asimismo un párrafo que dispone: “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”. “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 razón de este párrafo final es por el origen que tuvo el proyecto, destinado a evitar la interceptación y acceso no autorizado a correos electrónicos de jueces y periodistas.

Salvo el último párrafo, el proyecto no innova creando nuevos tipos penales, sino que a los ya existentes les agrega el término “comunicación electrónica” a fin de adecuarlos a la nueva realidad.

La reforma resuelve el problema de la atipicidad de la violación de correspondencia electrónica.[10] Y 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 C.P., la lectura del fallo dejaba un sabor de interpretación analógica de la ley penal.

Asimismo el art. 153, redactado cuidadosamente, enuncia en varias oportunidades la palabra “indebidamente”, que si bien puede parecer sobreabundante, tiene el claro propósito de diagramar el delito hacia una figura dolosa y realizada sin derecho, excluyendo la forma culposa.

[10] Ver fallo Correccional respecto al apoderamiento de una cuenta de correo electrónico, citado anteriormente.

c) Acceso ilegítimo a un sistema informático.

El proyecto incorpora como art. 153 bis, el siguiente: “Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros”.

Cabe resaltar que esta conducta suele ser la antesala para la comisión de otros delitos como la estafa, daño, sustracción de datos personales, claves o secretos comerciales. Es por eso que el legislador estableció que sólo resultará de aplicación esta figura *“si no resultare un delito más severamente penado”.*

El texto hace referencia a un sistema o dato de acceso restringido, puesto que no se prohíbe acceder a sistemas o redes abiertas, o al contenido publicado en un sitio de Internet público, como son la gran mayoría. El bien jurídico protegido por esta figura es la privacidad.

d) Publicación abusiva de correspondencia.

La nueva redacción del artículo 155 reprime con multa al que “hallándose en posesión de una correspondencia, *una comunicación electrónica**,*** un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere *publicar* indebidamente, si el hecho causare o pudiere causar perjuicios a terceros”.

Así como es grave violar la privacidad de una correspondencia mediante su acceso o interceptación, también lo es publicar el contenido de una carta o correo electrónico que se supone debe quedar en la esfera íntima y no ser divulgada.

“Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público”.

e) Revelación de datos.

En consonancia con las reformas de los arts. 153 y 155, se sustituye el art. 157, por el siguiente texto: “Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos *o datos, que por ley deben ser secretos”.* Se agrega el término datos para actualizar esta figura y proteger penalmente los datos que están en poder de la administración pública y que por ser secretos no deben ser revelado a terceros.

f) Unificación de los tipos penales de los arts. 117 bis y 157 bis del C.P.: acceso a un banco de datos, revelación de información y alteración de datos.

El proyecto modifica el art. 157 bis, por el siguiente:

“Será reprimido con la pena de prisión de un mes a dos años el que:

- A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
- 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;
- 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 uno a cuatro años.

El Senado consideró de adecuada técnica legislativa unificar los arts. 9 y 10 del Proyecto de Diputados (que establecían los delitos de insertar datos falsos y revelar información de un banco de datos respectivamente) en una sola norma, ya que ambos refieren a modificaciones del artículo 157 bis.

Al unificar las normas del art. 117 bis y del art. 157 bis en una sola además se propone derogar el art. 117 bis, pues existía coincidencia que en ciertos casos no protegía el honor pese a su ubicación.[11]

g) Captación ilegal de datos, imágenes y sonidos.

El proyecto de Diputados establecía en forma muy amplia un delito que consistía en la obtención o captación de la imagen, sonidos o datos de una persona en forma ilegal y su posterior difusión. El Senado prefirió no incluir este delito porque se infiere de la misma, la punición de las cámaras ocultas. Asimismo, el proyecto de diputados mereció observaciones respecto de la introducción del verbo típico “obtuviere”, por cuanto ello implicaría extenderla punición a límites exagerados, ya que en tanto el material no sea difundido, revelado o cedido, la lesión al bien jurídico protegido es prácticamente insignificante.

El proyecto de Diputados podría haber impactado en los medios de investigación y en el uso de cámaras ocultas para detener y dar a conocer casos de corrupción. Asímismo habría creado controversias con las actuales medidas de video-vigilancia existentes en el sector público y privado. Hay valores como la libertad de expresión, prensa e información , a los cuales no debe imponérseles límites irrazonables.

En el derecho comparado las cámaras ocultas han sido controvertidas, habiéndose admitido en algunas decisiones judiciales su uso por parte de

[11] D’ALESIO, Andrés José (Director) y DIVITO, Mauro (Coordinador). *Código Penal comentado y anotado*. Parte especial, pág. 153.

la prensa y consideradas ilícitas en otras, sobre todo porque en muchas situaciones significan un avance no consentido sobre la propiedad o la privacidad de terceros.

4) Estafa Informática.

El proyecto proponía como nuevo inciso 16 del art. 173, el siguiente: “El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos”.

El Senado mantuvo la redacción de Diputados con dos supresiones: “actuado sin autorización del legítimo usuario”, porque se entendió que agregaba un elemento al tipo, que resulta confuso e innecesario, ya que la autorización no podría excluir la ilicitud de la conducta de defraudar; y también elimina la frase “luego de su procesamiento”, porque no se encontró justificativo de fijar el momento técnico de una etapa de la transmisión de datos. Por eso en el proyecto de Senadores no se discriminan esos momentos.

5) Daño informático.

El art. 10 del proyecto, incorpora como segundo párrafo del artículo 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”

Con esta norma se soluciona el conflicto generado, en cuanto se consideraba atípica la destrucción de datos o programas de ordenador[12] o incluso la difusión de virus informáticos en redes de computadoras. La pena es la misma que para el daño común.

En este sentido, destruir o inutilizar quiere decir borrar definitivamente sin posibilidad de recuperación. También cabría la posibilidad de destruir el hardware con la finalidad de destruir los datos o software.

La existencia de un sistema de *back up*, en modo alguno altera el delito de daño pues la restauración requiere un esfuerzo tendiente a reparar el daño causado.

El delito puede recaer sobre “datos, documentos, programas o sistemas informáticos”. Esta es la principal modificación que requería nuestro Código. La ausencia de tales objetos en la descripción del art. 183, llevó en numerosos casos a resolver su atipicidad.

[12] *Virus Informático y Delito de Daño*. Revista de Derecho Penal y Procesal. 4 de abril de 2006, pág. 674.

Además se agrega una nueva modalidad de daño. Se penaliza a quien "vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños". Por ende, quien de alguna manera pone en comercio un programa *virus maker* o herramienta específica de destrucción de datos, con conocimiento del daño a producir, ayuda a cometer el delito de daño a quien usará esa herramienta.

Sin embargo no se prohíbe la existencia de estos programas, sino que penaliza a quien los venda, distribuya, los haga circular o introduzca concretamente en un sistema informático. La redacción da a entender que sería un delito de peligro abstracto, y por ende no requerirá un daño concreto, más allá de la exigencia del dolo, en específico el dolo de dañar.

En cuanto a la posibilidad de incriminar a quienes producen una herramienta que puede eventualmente usarse para crear daños informáticos, el tema se plantea con las tecnologías de doble uso como las fotocopiadoras, video casetera, ipod, un disco rígido, software *peer to peer*, etc. Tanto doctrina como jurisprudencia coinciden que estas tecnologías no son ilegales si tienen usos sustancialmente legítimos, aunque de paso también puedan tener usos no legítimos. Si el programa destinado a causar daños encuentra un uso legítimo, tal uso no será ilegal, en cambio si no es posible encontrarle usos legítimos o que no produzcan daño, no se ve porque no debería prohibirse su distribución.

También esta figura tan amplia, plantea otros problemas para la protección de la propiedad intelectual. Si un programador inserta un virus en un programa a fin que, en caso de copia, el mismo se active y destruya la información existente en el ordenador, es posible considerar la situación como un daño informático además de un abuso del derecho (art. 1071 C.C.). Cabe plantearse la situación de que el sistema de seguridad anti-copia, sólo se limite a borrar o detener el programa no original dejando intacto los datos del usuario. En tal situación, el programador no está infringiendo norma de derecho penal alguna.

El proyecto agrega como agravante al art. 184 del C.P., el siguiente: “La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes:…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”.

6) Daño a las comunicaciones.

Pablo Palazzi da este título a la nueva figura del art. 197 porque considera que al incluir cualquier clase de comunicación, no sólo ampara lo público sino cualquier clase de comunicación incluyendo las privadas como el correo electrónico, la voz a través de IP, o los mensajes de Chat o texto a través de celulares (SMS). Lo que quiso el legislador es ampliar el tipo

penal a esos nuevos medios de comunicación con independencia de naturaleza pública o privada.

El nuevo artículo 197 quedaría redactado de la siguiente manera: “Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida”.

Se trata de una figura dolosa. No cabe incluir entonces en este tipo, a los supuestos de caída de redes o sistemas de comunicaciones por diversos problemas técnicos, ajenos a la intención del operario. Sí, en cambio, quedará incluido el ataque por denegación de servicios.

CAPITULO III

CITAS JURISPRUDENCIALES

Fallo Lanata

La Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala VI, decidió confirmar la resolución de Primera Instancia, en cuanto rechazaba la excepción de falta de acción planteada por el periodista, basado en la atipicidad de la violación de correos electrónicos (arts. 153 y 155 C.P.).

La decisión se emitió considerando, entre otros, los siguientes fundamentos:

“El especialista en derecho constitucional Gregorio Badeni ha manifestado que es necesaria una razonable interpretación dinámica de las leyes para que, sin necesidad de recurrir a su reforma, se pueda evitar que queden a la zaga de la realidad social. En este mismo sentido, la Sala admite que no se contemplan en forma explícitamente, en el Capítulo III del Título V de la ley sustantiva, los hechos ilícitos que vulneran la privacidad y divulgación del correo electrónico, pero esta carencia de protección legal es tan solo aparente. Es que el legislador, con amplia visión de los adelantos técnicos y científicos que se producirían luego de incluir la norma del artículo 153, ha dejado abierta la descripción típica a los "despachos de otra naturaleza" y a cualquier "otro papel privado". Este criterio es compartido por Carlos Creus en un reciente artículo comentando el fallo en cuestión, donde sostuviera: "...No parece que estos argumentos puedan tacharse de "analogía" (aunque sí quizás de una interpretación extensiva por imperio histórico, lo que, insisto, no es hacer "analogía"). De lo contrario creamos inútilmente un "vacío" de legalidad que no tiene razón de ser y reduce exageradamente la protección que en la actualidad proporciona nuestro sistema penal, basándonos en un exagerado respeto a las "formas" de la ley”.

Fallo Grimberg

La Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala I, dispuso confirmar la sentencia que resolvía la nulidad del acta de constatación practicado por Escribano Público con testigos pero sin la correspondiente autorización judicial y donde se obtenía información derivada de correos electrónicos.

Al respecto, la Cámara se expresó de la siguiente manera:

"No puede sostenerse la validez de un registro realizado en un recinto que pertenece a un tercero sin la debida autorización judicial que lo habilite. El acta de constatación autorizada por un escribano público con la presencia de testigos hábiles no subsana el vicio detectado, ya que el ingreso a ámbitos privados como son la correspondencia (a la que se extienden los mensajes electrónicos, sean estos particulares o los enviados y recibidos en una cuenta de correo interno) y los papeles privados, sólo puede verse justificado con la autorización de un juez competente, mediante auto fundado. El correo electrónico es, sin lugar a dudas, correspondencia privada que está protegida por la C.N. y otros tratados sobre derechos humanos incorporados a ella. La violación de esta garantía básica conlleva la nulidad de las actuaciones que dependen de ese acto procesal. Por tanto, debe convalidarse la nulidad del acta de constatación realizada por el escribano público".

Fallo Redruello

En un caso de similares características al anteriormente comentado, la Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala IV, en autos caratulados “REDRUELLO, Fabián L. y otros S/Estafa-Nulidad”, sostuvo la decisión de Primera Instancia de declarar la nulidad de la prueba presentada por un empleador apropiándose de correos electrónicos de sus empleados. La Cámara dijo:

"En efecto, y respecto de si el término utilizado en el artículo 18 de la Constitución Nacional resulta abarcativo de la correspondencia electrónica, aparece conducente recordar las conclusiones arribadas por la doctrina, ocasión en la que sostuvo que asegurar la invulnerabilidad de esta forma de comunicación, y todo lo que se entienda por ella, era y sigue siendo una regla capital para el desenvolvimiento del derecho de autonomía o autodeterminación personal en un Estado constitucional y democrático de derecho.”

"En este orden de ideas, no puede menos que concluirse que la apropiación y presentación al proceso de correspondencia privada perteneciente al imputado Redruello transgrede los principios constitucionales arriba expuestos y los que encierra el debido proceso, tildándolos, en consecuencia, de prueba ilícita; lo que aparece como óbice a los efectos de que el tribunal realice una actividad interpretativa respecto del material probatorio cuestionado”.

Conclusión

Como corolario de este trabajo de investigación, hemos visto que las conductas reprochables en torno a la actividad informática, puede traer aparejada lesiones tanto económicas, como pérdida de información, avasallamiento de la intimidad, etc., vinculadas no sólo a grandes empresas o corporaciones, sino también a cualquier particular o persona física. Estas conductas, que no están necesariamente relacionadas con la educación de la persona que las lleva a cabo, característica que las diferencia de la gran mayoría de los restantes delitos del código penal, y que algún sector de la doctrina las ha dado en llamar “delitos de cuello blanco”, merecían el repudio penal.

Si bien creemos que la sanción de la ley 26.388 ha venido a sanear el vacío legal que se presentaba hasta el momento, estimamos que los legisladores han evidenciado una larga dilatación en su incorporación al marco legal nacional, sin antes experimentar gran incertidumbre no sólo a abogados y litigantes, sino también a los mismos jueces a la hora de resolver los conflictos.

Asimismo, estimamos adecuado promover la estimulación popular en denunciar este tipo de delitos, a fin de facilitar su detección, investigación y prevención, ya que en la gran mayoría de los casos, los mismos no son revelados por sus víctimas y por ende, juzgados.

Finalmente, y dado el nuevo panorama legal, creemos conveniente la especialización de profesionales, fiscales, peritos, jueces y demás colaboradores de la justicia para una mayor eficiencia en su prestación, y así brindar más seguridad a la comunidad.

INDICE

Bibliografía

1) ABOSO, Gustavo Eduardo y ZAPATA, María Florencia. *Cibercriminalidad y Derecho Penal*. Editorial Euros, Año 2006.
2) Código Penal de la República Argentina. Editorial Errepar. Año 2008, Séptima Edición,
3) Constitución Nacional de la República Argentina, Editorial Zavalía, Año 2006.

4) LIMA DE LA LUZ, Maria. *Delitos electrónicos*. Ediciones Porrua, México, Año 1984.

5) PALAZZI, Pablo A.. *Los delitos informáticos en el Código Penal – Análisis de la Ley 26.388*. Editorial Abeledo Perrot, Año 2009.

6) TELLEZ VALDEZ, Julio. *Derecho Informático*. Editorial Mc Graw Hill, segunda edición. Año 1996.

7) Website de la Corte Suprema de Justicia de la Nación: *http://www.csjn.gov.ar*

8) Website de la Suprema Corte de Justicia de la Provincia de Buenos Aires: *http://www.scba.gov.ar*

9) http://www.saij.jus.gov.ar

10) http://www.delitosinformaticos.com.ar

11) http://www.segu-info.com.ar

12) http://www.infoleg.mecon.gov.ar