Voces: CODIGO PENAL ~ COMUNICACIONES ~ DELITO ~ FIRMA DIGITAL ~ FUNCIONARIO PUBLICO ~ INFORMATICA ~ VIOLACION DE SECRETO ~ VIOLACION DE SELLOS Y DOCUMENTOS ~ DAÑO ~ TIPICIDAD ~ DELITO INFORMATICO ~ PIRATERIA INFORMATICA ~ DOCUMENTO DIGITAL ~ PORNOGRAFIA ~ AGRAVANTES ~ POLITICA CRIMINAL ~ PRINCIPIO DE ESPECIALIDAD ~ PRINCIPIO DE LEGALIDAD
Título: Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación (ley 26.388)
Autores: Fillia, Leonardo César Monteleone, Romina Nager, Horacio Santiago Rosende, Eduardo E. Sueiro, Carlos Christian
Publicado en: Sup. Penal2008 (agosto), 15 - LA LEY2008-E, 938

SUMARIO: I. Antecedentes históricos de la ley 26.388. - II. Análisis dogmático a los tipos penales previstos por la ley 26.388. - III. Consideraciones criminológicas a la ley 26.388. - IV. Conclusiones político-criminales de la ley 26.388.

Introducción

El siguiente artículo doctrinario encuentra por objeto de estudio efectuar un análisis sistemático y metódico de la Ley 26.388 (Adla Bol 17/2008, p. 4), que introduce la reforma en materia de criminalidad informática al Código Penal de la República Argentina.

A los fines de encarar dicho estudio con el rigor científico que éste amerita, es que hemos decidido dividir el presente trabajo en cuatro etapas o niveles de análisis.

La primera etapa de análisis estará destinada a efectuar un estudio profundo de los antecedentes históricos de la Ley 26.388. Se relevarán a tales fines cuales han sido los proyectos de ley desde el año 1996 hasta el presente 2008, año en el cual, se ha materializado el dictado y sanción de la Ley 26.388 que introduce la reforma en materia de criminalidad informática a nuestro Código Penal. Es así que esta primera etapa de análisis será bautizada: "Antecedentes Históricos de la Ley 26.388".

El segundo nivel de análisis se encontrará destinado a realizar un estudio sistemático y riguroso a nivel dogmático, de las distintas figuras delictivas que prevén su comisión mediante medios informáticos. De esta forma es que se incursionará en el estudio puntual e individualizado de los tipos penales de Ofrecimiento y Distribución de Imágenes relacionadas con Pornografía Infantil (artículo 128 C.P.N), Violación de Secreto y Privacidad (artículos 153, 153 bis, 155, 157, 157 bis C.P.N), Estafa y otras Defraudaciones (artículo 173, inciso 16, C.P.N.), Daño (artículos 183 y 184, C.P.N.), Interrupción de Comunicaciones (Artículo 197 C.P.N.), Destrucción de Prueba (artículo 255 C.P.N.) y a su vez del artículo 77 del Código Penal de la Nación, que incorpora la terminología y definiciones conceptuales indispensables para permitir una interpretación precisa de los tipos penales a la luz del principio de legalidad, respecto de la reforma producida en relación a la criminalidad informática como modo comisivo de los tipos penales recientemente enunciados. Por esta razón es que este segundo nivel de análisis será designado: "Análisis dogmático a los tipos penales previstos por la ley 26.388".

La tercera etapa de análisis ahondara en consideraciones de carácter netamente criminológicas sobre la ley 26.388. Será de esta forma que se examinará si la ley ha recurrido o no, a efectuar una denominación de carácter biotipológica de autores de este tipo de delitos que pueden perpetrarse a través de medios informáticos o, por el contrario, ha prescindido de este tipo de definiciones. Es así que hemos designado a esta cuarta etapa de análisis: "Consideraciones Criminológicas a la Ley 26.388".

Finalmente, la cuarta y última etapa de análisis se encontrará destinada a escudriñar cuáles son las consideraciones de carácter político-criminal que pueden formulársele a la ley 26.388. Así, constataremos la técnica legislativa empleada, el modelo político criminal escogido y los tipos penales que se han seleccionado para incluirlos dentro de esta ley de reforma al Código Penal de la Nación de la República Argentina. Por estas razones, hemos decidido referir a esta quinta etapa analítica: "Consideraciones Político-Criminales a la ley 26.338". En la misma también se trataran las conclusiones arribadas en cada una de las etapas o niveles de análisis del presente trabajo, para lo cual extraeremos una conclusión final que nos permita en forma global y general establecer cuáles son las ventajas y beneficios que reporta esta ley de reforma en materia de criminalidad informática, como así también las desventajas e inconvenientes que esta reforma implementada e instrumentada en estos términos puede ocasionar al sector privado, sector público, la comunidad científica, la administración de justicia y la sociedad en general.

I. Antecedentes históricos de la ley 26.388

El innegable avance de la tecnología en las sociedades de fines de siglo XX y principios del siglo XXI, dentro del cual, la informática se ha situado en un rol protagónico en la conformación de lo que hoy se ha dado a conocer como las "sociedades de la información", en la que los miembros de las comunidades de la posmodernidad desarrollamos nuestras vidas, ha llevado en nuestro ámbito local, más puntualmente en la República Argentina, a preocuparse desde ya hace más de una década en formular planteos y reformulaciones conceptuales dentro del campo jurídico penal, a los fines de adaptar y actualizar nuestra legislación.

Es así que desde el año 1996 hasta nuestro días se han presentado un gran número de proyectos legislativos en el Congreso Nacional, destinados a permitir una incorporación armónica dentro de nuestra legislación penal de esta nueva tecnología, puntualmente, la tecnología informática, ya sea como medio o forma comisiva para la ejecución de diversos tipos penales ya contemplados en nuestra legislación ("criminalidad informática"), o bien, mediante su inserción normativa como un nuevo bien jurídico autónomo a tutelar, con la correspondiente y correlativa creación de nuevos tipos penales o de figuras delictivas que podrían haberse dado a conocer como "delitos informáticos".

A los fines de conocer cuales han sido los antecedentes históricos de la ley 26.388 es que efectuaremos un breve racconto histórico de los proyectos de ley presentados ante el Congreso Nacional durante el período 1996-2008.

El primer proyecto de ley sobre delitos informáticos, presentado a inicios del año 1996 por Leonor E. Tolomeo, preveía el tratamiento de la actividad informática como un medio comisivo para la realización o perpetración de las distintas figuras delictivas contempladas en nuestro Código Penal. El mismo no consistía en la incorporación de una ley complementaria al Código Penal, sino, por el contrario, se encontraba dirigido a una reforma de carácter integral del mismo en forma armónica y concordada, respetando la correlatividad de su articulado e introduciendo puntuales modificaciones a cada uno de los tipos penales, a los fines de permitir su comisión mediante medios informáticos. De esta manera, contemplaba la reforma de los siguientes tipos penales: 1) Incorporación de terminología y definiciones en el artículo 77 del C.P.N. 2) Violación de secreto (artículos 153, 154 y 157 del C.P.N), 3) Estafas y otras defraudaciones (artículos 173 y 175, inciso 2 del C.P.N.), 4) Daño (artículos 183, 184 y 185 del C.P.N.), 5) Interrupción de las comunicaciones (artículos 194 y 197 C.P.N.), 6) Delitos que comprometen la paz y la dignidad de la Nación (artículos 222 y 225 C.P.N.) y 7) Delitos contra la propiedad intelectual (artículo 72 ter de la Ley 11.723 C.P.N., Adla, 1920-1940, 443).

Como puede apreciarse el "Proyecto Tolomeo" era muy similar a la actual ley 26.388. En primer lugar, porque propuso una reforma integral, armónica y concordada al Código Penal, descartando la incorporación de una ley complementaria; en segundo término, porque previó a la criminalidad informática como forma comisiva para la realización de las figuras delictivas y, en tercer orden de ideas, porque modificaba prácticamente los mismos tipos penales que la ley 26.388, con excepción del delito de ofrecimiento y distribución de pornografía infantil y la destrucción de prueba.

Al poco tiempo, se presentó ante el Congreso Nacional el Proyecto de Ley de Carlos R. Alvarez, el que propuso la incorporación de una ley complementaria que contenía tres artículos relacionados con la comisión de los tipos penales de hurto y daño mediante medios informáticos.

En el mes de octubre de 1996 se presentó el Proyecto a cargo de José A. Romero Feris, que proponía a lo largo de sus cinco (5) artículos incorporar las figuras de hurto, estafa y daño a través de medios informáticos. Asimismo, agravaba estas conductas cuando fueran perpetradas por funcionarios públicos, sancionándolos con una pena accesoria de inhabilitación especial perpetua.

Al año siguiente, con fecha 22 de agosto de 1997, Antonio T. Berongaray presentó "El Proyecto de Ley dirigido a la "reglamentación de actividades vinculadas a computadoras, sistemas de computación o telecomunicaciones.", el que constaba de nueve capítulos, cuyos títulos eran los siguientes: Capítulo 1.- Glosario de Términos: Computadora, Sistema de computación, Datos, Programas de Computación, Función e Interceptar; Capítulo 2.- Del acceso no autorizado; Capítulo 3.- Daño a datos informáticos; Capítulo 4.- Violaciones a la propiedad intelectual en materia de programas de computación, no comprendidas en la legislación específica; Capítulo 5.- Fraude por medios informáticos; Capítulo 6.- Espionaje a través de la computación; Capítulo 7.- Entrega, distribución y venta de medios destinados a cometer delitos previstos en este capítulo; Capítulo 8.- Normas procesales y Capítulo 9.- Disposiciones transitorias y complementarias. Pese a la exhaustiva labor en el diseño de este proyecto de ley complementaria para regular la materia de criminalidad informática como delitos autónomos que podrían haberse conocido como la "Ley de Delitos Informáticos" o la "Ley de Reglamentación de Actividades Vinculadas a Computadoras, Sistemas de Computación o Telecomunicaciones", éste tampoco se materializó.

El 26 de noviembre de 2001 se presentó un "Anteproyecto de Ley", el que constaba de tres tipos delictivos básicos con sus respectivas figuras agravadas. De la lectura del apartado C de sus fundamentos surge que se optó por incluir los ilícitos proyectados dentro de una ley especial para no romper el equilibrio de la sistematización del Código Penal por tratarse de un bien jurídico novedoso que requería una especial protección jurídico-penal.

Los tres tipos básicos previstos eran: 1) "Acceso Ilegítimo Informático"; 2) "Daño Informático" y 3) "Fraude Informático". Sin embargo, este Anteproyecto tampoco se plasmó como ley complementaria.

Debieron transcurrir otros cuatro años para que, el 4 de marzo de 2005, se presentara el "Anteproyecto de Delitos Informáticos" que constaba de 16 artículos, entre los cuales se sugería regular como delitos autónomos, dentro de una ley complementaria, los siguientes tipos penales: 1) "Daño Informático"; 2) "Estafa Informática"; 3) "Delitos contra la Privacidad" y 4) "Ofrecimiento o difusión de Pornografía Infantil".

Durante el año 2006 se presentaron seis (6) proyectos de ley, a saber: 1) "Proyecto Delia Bisutti" (2032-D-06), a través del cual se proponía equiparar el correo electrónico a la correspondencia epistolar; 2) "Proyecto Canevarolo" (3001-D-06), similar al proyecto precedente; 3) "Proyecto Diana Conti y Agustín Rossi" (2291-D-06), en el cual proponían modificaciones al tipo penal de violación de secreto e introducía un nuevo bien jurídico, la privacidad, contemplando los siguientes dispositivos legales: artículos 153, 154, 154 bis, 155, 156, 157, 157 bis e incorporando los artículos 154 ter y 157 ter; 4) "Proyecto Silvia Martinez" (1798-D-05), el que expresamente punía el ofrecimiento y difusión de la pornografía infantil y prostitución infantil; 5) "Proyecto Marta Osario" (1225-D-05) que introducía modificaciones a los tipos penales de estafa y daño (artículos 173, inciso 15, 183 y 184) y 6) "Proyecto Andrés Sotos" (985-D-05), que como ley especial o complementaria que contenía cinco capítulos: Capítulo I.- Acceso Ilegítimo Informático; Capítulo II.- Violación al Correo Electrónico; Capítulo III.- Daño Informático; Capítulo IV.- Fraude Informático y Capítulo V.- Pornografía Infantil.

Es menester referir que durante el mismo año, una Comisión, de los más destacados Juristas nacionales, fue convocada por el Ministerio de Justicia y Derechos Humanos, bajo la coordinación de la Secretaría de Política Criminal y Asuntos Penitenciarios, a los efectos de elaborar una propuesta de Anteproyecto de Reforma Integral del Código Penal de la Nación. Así fue como se logró arribar al "Proyecto Ley de Reforma y Actualización Integral del Código Penal de la Nación" (Resoluciones M.J. y D.H. n° 303/04 y n° 136/05), a través del que se proponía actualizar tanto su parte general como su parte especial, permitiendo la supresión total de las leyes complementarias. Por otra parte, no preveía en forma alguna la introducción de la "Criminalidad Informática" como medio comisivo para la realización de los tipos penales ya contemplados por el Código Penal de la Nación o la incorporación de tipos penales autónomos conocidos como "Delitos Informáticos" mediante la creación de nuevos bienes jurídicos.

Ante la existencia de tantos proyectos de ley, la mayoría de los cuales coincidían en la temática, se creó una subcomisión especial integrada por asesores de las comisiones de Comunicaciones e Informática y de Legislación Penal, a la que fueron invitados los sectores interesados, tanto del ámbito público como privado. En ella participaron representantes de las empresas vinculadas con todos estos temas, cuyo aporte es por demás valorado y reconocido.

Fue bajo estas circunstancias, que surgió el expediente que dio origen al Proyecto de Ley (CD- 109/06; S- 1751-1875 y 4417/06), el cual fue producto del obrar conjunto de los diputados Nemirovsci, Romero, Bisutti, Irrazábal, Lovaglio Saravia, Osorio, Ritondo, Zottos, Canevarolo, Morini, Conti, Pinedo y Solanas.

El Proyecto de Ley (CD- 109/06; S- 1751-1875 y 4417/06 y Expediente 5.864-D.-2006), que da origen a la ley 26.388, ha surgido del tratamiento de un gran número de expedientes legislativos (1) y se presenta como una versión mejorada y refinada de todos los anteriores proyectos de ley desde 1996 hasta 2008.

También debe destacarse que el mismo encontró gran parte de su motivación e impulso para su dictado en la necesidad de adaptar nuestra legislación penal al "Convenio sobre Cibercriminalidad de Budapest del año 2001", al que han adherido más de 40 países (2). Fue así que a lo largo del año 2007 diversas comisiones del Senado examinaron y estudiaron el proyecto de diputados, hasta que finalmente el 28 de noviembre de 2007, el Senado aprobó con reformas el proyecto de ley en materia de criminalidad informática que había sido aprobado con media sanción el año anterior por la Cámara de Diputados. De esta forma en el Senado, las Comisiones de Justicia y Asuntos Penales y de Sistemas, Medios de Comunicación y Libertad de Expresión, luego de numerosas reuniones con expertos, emitieron un dictamen de comisiones (CD 109-06) que fue aprobado por el Senado en pleno.

Finalmente la ley 26.388 fue sancionada el 4 de junio de 2008, promulgada el 24 de junio de 2008 y publicada en el Boletín Oficial de la República Argentina el 25 de junio de 2008 (3).

Esta ley constituye una reforma integral y concordada al Código Penal y no configura de manera alguna una ley complementaria al mismo. Es como consecuencia de ello, que no se crean nuevos tipos penales, sino que se modifican ciertos aspectos de los ya existentes para receptar las nuevas tecnologías como medios comisivos para su ejecución. Contiene un total de 15 artículos, los cuales se analizarán en el acápite siguiente.

II. Análisis dogmático a los tipos penales previstos por la ley 26.388

A) Terminología

Artículo 1°- Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:

"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."

La sanción de la ley 26.388 incorpora una serie de definiciones al Código Penal, agregando para ello tres párrafos al final del artículo 77, derogando por otra parte el artículo 78 que ya establecía los conceptos de "firma

digital" y "documento digital firmado digitalmente" (ley de Firma Digital N° 25.506, Adla, LXII-A, 6).

Cabe que aclaremos que la ley 25.506, en su primer capítulo, nos da las definiciones de "Firma Digital" (artículo 2), "Firma electrónica" (artículo 5), "Documento Digital" (artículo 6).

A esto se debe sumar las definiciones que también establece la ley de Habeas Data N° 25.326 (Adla, LX-E, 5426) que en su Capítulo 1°, artículo 2° explica qué abarcan los términos de datos personales, sensibles, archivo, registro, base o banco de datos, tratamiento de datos, responsable de archivo, registro, base o banco de datos, datos informatizados, titular de los datos, usuario de datos y disociación de datos.

Los que nos situamos como profesores de Derecho Penal, conocemos cuales son los principios básicos de esa rama jurídica. Sin duda alguna, nadie en nuestro país ni en el exterior, incluido el país que más nos ha nutrido en lo que respecta a la dogmática (Alemania), desconocería los principios de subsidiaridad y última intervención.

La pregunta de un alumno perspicaz sería: Profesor si el derecho penal es subsidiario y se tiene que aplicar en última instancia y cuando ya más nada mejor se pueda hacer, ¿cómo se explica que una ley penal es aquella que modifica, desde el Código Penal, la extensión del término "documento" de la ley civil?

La respuesta es clara en razón de que dichos principios no se han respetado en este caso, toda vez que con la vigencia de este artículo se invierte la cuestión. Ya no vemos al penalista yendo a buscar definiciones al Código Civil, sino que veremos al civilista (jueces, abogados, etc.) hurgando en la ley penal para resolver un conflicto totalmente ajeno a esta, propio claro de un Estado que genera un expansionismo penal no sólo por la creación de tipos penales, sino por la legislación de distintas circunstancias y hechos generalísimos, a través de la ley penal.

Si le podríamos preguntar a Vélez Sarsfield cual es la definición de documentos, rápidamente nos diría que los documentos son papeles que dan cuenta de la existencia de algo, más precisamente son parte de las formas en que puede realizarse un acto jurídico (Arts. 973 y 978 del Código Civil), y una evolución de las solemnidades de los actos, ya que antes estas se daban a nivel oral (ver las explicaciones en nota al artículo 973 del citado cuerpo normativo).

También nos diría que los documentos en realidad adoptan dos modalidades: las de instrumentos públicos y privados, que justamente es la clasificación adoptada por Tejedor en la redacción del Código que a nivel penal hoy nos rige.

Es por ello que desde la ley civil para que exista un documento (instrumento) público o privado este debe ser escrito y firmado por las partes que intervienen en él (arts. 986, 987 y 1012 CC).

Entendemos que lo correcto hubiera sido una incorporación y/o modificación hermenéutica al Código Civil de las definiciones dadas por la ley de Firma Digital y la que ahora nos toca analizar. Aclarado el error, la problemática que plantea y nuestra opinión, pasemos ahora si a efectuar un somero análisis de los párrafos incorporados.

El primero explica que el término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

De la fórmula legal, se desprende una extensión de la característica de escritura que daba el Código Civil al documento, que llega ahora también a la escritura digital, es decir aquella asentada en medios de almacenamiento digital o electrónico.

Sin embargo, resulta necesario que un documento, para ser tal a nivel jurídico, ya sea en su faz privada o pública, esté firmado, y es aquí donde entra en juego el segundo párrafo agregado por la ley.

Este ordena los términos "firma" y "suscripción", que ya estaban en el ahora derogado artículo 78, ampliando la extensión de lo que ontológicamente conocíamos como firma y suscribir a sus reflejos a nivel electrónico, es decir la firma digital.

Con esta descripción, lógica atento a la evolución de los negocios que exige la modernización de la legislación para hacer valer como prueba documentos que antes no podían ser invocados como tales, la firma ahora también incluye la modalidad establecida en la ley 25.506, es decir aquella hecha por medios técnicos cuya explicación excederían los límites del presente trabajo, bastando decir que consiste en agregar a un documento digital un algoritmo matemático que se encuentra bajo control exclusivo del firmante y puede ser comprobado por terceros (llave pública -certificado- y llave privada).

El párrafo tercero nos obliga a efectuar un llamado de atención al aclarar que "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

Teniendo en cuenta los dos párrafos anteriores, parecería que el presente está simplemente demás pues el certificado no es otra cosa que la clave pública que ha almacenado una entidad certificante para que los terceros puedan comprobar la firma digital de un correo electrónico o un documento.

Sin embargo, y teniendo en cuenta que el término "documentos" debería abarcar a los instrumentos públicos y privados, con este párrafo se excluye a los efectos de la ley penal a los instrumentos públicos en su en su faz

digital.

En esa línea de ideas, no podemos dejar pasar por alto que las modificaciones introducidas, o por lo menos la contradicción entre los párrafos aludidos, llevan a una exclusión de la papelería pública digital en cuanto a falsificaciones y con ello a una alejamiento de los lineamientos que mundialmente se están materializando en cuento al Gobierno Electrónico y que en nuestro país ya tuvo el punta pie inicial en el decreto 378/2005.

La contradicción también genera una mezcla de conceptos vigentes y separados en distintos ordenamientos que merece ser recalcada a los efectos de evitar confusiones en los operadores jurídicos con respecto al artículo 6 de la ley de firma digital (4).

En síntesis y a poco que reflexionemos un poco, nos surgirá el siguiente problema. Si el Código Civil enumera en forma taxativa que instrumentos pueden ser considerados públicos, estableciendo entre uno de ellos a aquel confeccionado por un funcionario en el ejercicio de sus funciones (Art. 979 del Código Civil), mientras que el actual artículo 77 del Código Penal sólo extiende a su faz digital a los instrumentos privados; en aquel caso donde nos encontremos ante un elemento digital que reúna los requisitos de los primeros, no va a estar alcanzado por la ley civil en el referido artículo, pero tampoco va a poder ser considerado como un instrumento privado en razón de la característica "lex stricta" del principio de legalidad.

Con esto, la falsificación de una comunicación jurisdiccional que disponga un allanamiento (ver párrafo incorporado por la ley 25.760 (Adla, LXIII-D, 3827) al artículo 224 del CPPN), o el uso de la firmal digital por el Ministerio Público Fiscal que ya se encuentra implementado, así como también el posible uso de notificaciones vía correo electrónico, las comunicaciones entre representaciones consulares, o los actos de la administración, serán hechos atípicos.

B) Ofrecimiento y distribución de imágenes relacionadas con pornografía infantil

Artículo 2ª. Sustitúyase el artículo 128 del Código Penal, por el siguiente:

Art. 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, 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 finales 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 menores de catorce (14) años.

El aumento de casos de pornografía infantil por medio de la web hizo necesario la modificación del anterior artículo 128, no sólo introduciendo nuevas modalidades típicas, sino también incorporando los medios electrónicos como formas de comisión.

El nuevo texto del artículo 18 especifica como destinatario de la norma a los menores de 18 años en los párrafos 1° y 2°, mientras que en el párrafo 3° se refiere a las personas de 14 años, dejando de lado toda regulación sobre la exhibición de mayores de edad. Al igual que en la redacción anterior los legisladores omitieron otorgarle protección a los incapaces mentales, como si no fueran dignos de igual amparo que los menores de edad.

Dicho ello, corresponde señalar que lo ilícito no es la imagen que recibe el adulto, sino que lo se que pretende proteger es a los menores que se encuentran involucrados en las imágenes pornográficas o en el material que ellos reciben. Sintéticamente se advierte que el bien jurídico protegido es la protección del menor. De esta forma, podemos señalar que el objetivo primordial de este nuevo tipo penal reside en reprimir la explotación de niños en la producción de cualquier representación suya en actividades sexuales explícitas, puesto que expresamente pune todo ataque al normal desarrollo psíquico y sexual de menores de edad.

En su anterior redacción el artículo 128 penaba con prisión de seis meses a cuatro años a los que produjeren o publicaren imágenes pornográficas en que se exhibieran menores de 18 años, al que organizare espectáculos en vivos con escenas pornográficas en que participaren dichos menores y al que distribuyere imágenes pornográficas cuyas características externas hicieren manifiesto que en ellas se ha grabado o fotografiado la exhibición de menores de 18 años. Por último, preveía una pena menor —de un mes a tres años de prisión— a quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de 14 años.

La actual legislación sobre distribución u ofrecimiento de representaciones relacionadas con la pornografía infantil viene a cumplir con los compromisos internacionales adoptados a través de la aprobación del Protocolo relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía, complementario de la Convención de la Naciones Unidades sobre los Derechos del Niño de rango constitucional según el art. 75 inc. 22 CN (Adla, L-D, 3693).

La figura analizada se divide en tres párrafos, cada uno de los cuales prevé no sólo diferentes acciones típicas, sino también diversas penas.

El párrafo primero de la norma de mención establece una larga serie de verbos típicos como: a) producir, b) financiar, c) ofrecer, d) comercializar, e) publicar, f) facilitar, g) divulgar o h) distribuir, por cualquier medio, toda representación de menores de 18 años en actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales. La primera diferencia advertida con la legislación anterior se basa en la suma de nuevas conductas típicas. Nótese que anteriormente sólo resultaba punible la producción, publicación o distribución de imágenes pornográficas, incorporándose actualmente también el ofrecimiento, la comercialización, la financiación, la divulgación y la facilitación de estas imágenes. Resulta evidente que la intención de esta nueva legislación con la incorporación de nuevas figuras típicas encuentra su correlato en que la experiencia demuestra que en este tipo de situaciones generalmente participan un sinnúmero de personas, que en muchas ocasiones forman parte de una asociación destinada expresamente a la divulgación, facilitación u ofrecimiento de pornografía infantil.

En lo que interesa a este comentario podríamos definir qué se entiende por cada una de los verbos típicos expresados en el párrafo precedente. Así, conforme al Diccionario de la lengua española —vigésima segunda edición— y específicamente relacionado con la materia que aquí interesa la acción producir comprende el engendrar, procurar, originar, ocasionar, fabricar, elaborar o crear; por su parte financiar se encuentra definido como aportar el dinero necesario para una empresa o sufragar los gastos de una actividad, de una obra, etc. En cuanto al término ofrecer se advierte que tiene numerosas acepciones que podrían relacionarse con el tópico bajo análisis, entre las cuales encontramos 1) la acción de comprometerse a dar, hacer o decir algo, 2) el presentar y dar voluntariamente algo, 3) manifestar y poner patente algo para que todos lo vean, 4) presentar, manifestar, implicar y 5) mostrar determinado aspecto. Por su parte, la conducta de comercializar se encuentra definida como el dar a un producto condiciones y vías de distribución para su venta como así también el poner a la venta un producto.

Continuando con el análisis de los verbos típicos, específicamente la acción de publicar consiste en hacer notorio o patente, por televisión, radio, periódicos o por otros medios, algo, es decir, un escrito, una estampa, etc. En cuanto a facilitar se define como el hacer fácil o posible la ejecución de algo o la consecución de un fin, aunque también implica la acción de proporcionar o entregar algo.

Por último, se mencionan los términos divulgar —que podría definirse como el publicar, extender, poner al alcance del público algo— y el distribuir como dividir algo entre varias personas, designando lo que a cada una corresponde, según voluntad, conveniencia, regla o derecho, dar a algo su oportuna colocación o el destino conveniente o entregar una mercancía a los vendedores y consumidores.

Una de las primeras críticas que se evidencia en la nueva legislación resulta el hecho que en la mayoría de los casos algunos de los términos señalados como acciones típicas resultan ser sinónimos —a modo de ejemplo puede señalarse las acepciones de divulgar y publicar—. Sin embargo, tal circunstancia permite disipar cualquier situación que pueda presentarse en la práctica que conlleve a dudar a los operadores judiciales al momento de efectuar el correspondiente juicio de tipicidad en un caso concreto.

Continuando con el análisis de rigor, corresponde señalar que la nueva redacción del artículo 128 del Código Penal suple el término "imágenes pornográficas" como elemento del tipo penal por "cualquier representación de un menor de 18 años de edad dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales". Conforme al texto de la ley, tales representaciones deben contener fines predominantemente sexuales o representar explícitamente actividades sexuales en las cuales se encuentren involucrados menores de edad, excluyendo de esta forma las actividades simuladas.

Este ilícito, al igual que en su antigua redacción, prevé penas de prisión de seis meses a cuatro años, cuya investigación estará a cargo del Poder Judicial de la Ciudad de Buenos Aires en función de los "Convenios de Transferencia de Competencias Penales" celebrados entre la Nación y la Ciudad Autónoma de Buenos Aires (leyes 26.357 y 2257).

En lo que a este párrafo se refiere se evidencian una serie de cambios con la versión original remitida al Senado por la Cámara de Diputados. Así, en aquél proyecto el elemento del tipo penal eran las imágenes pornográficas y no toda representación de un menor de dieciocho años de edad dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, como finalmente se sustituyó en el dictamen del Senado. Tal acertada variación permite contemplar la correcta definición dada por el Protocolo relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía, que fuera mencionado en párrafos precedentes.

En cuanto al aspecto subjetivo, al igual que en su redacción anterior, este tipo penal se trata de una figura dolosa.

Merece destacarse que la nueva legislación incorporó la expresión "cualquier medio" para perpetrar las acciones típicas enumeradas, incorporándose, de esta forma, los medios electrónicos o informáticos como lugar

posible para perfeccionar este tipo de ilícitos penales. Esto lleva a suponer que los legisladores expresamente consideraron los datos reales que demuestran que la web resulta ser uno de los medios principales utilizados por los autores o partícipes del delito de ofrecimiento o distribución de imágenes relacionadas con la pornografía infantil.

Ahora bien, en cuanto a la segunda hipótesis delictiva prevista en el segundo párrafo del artículo 128 debemos señalar que se trata de un nuevo ilícito penal que no se encontraba previsto en la legislación anterior. El mismo tiene previstas penas de prisión de cuatro meses a dos años el que tuviere en su poder representación de las descriptas en el párrafo primero con fines inequívocos de distribución o comercialización.

Se trata expresamente de un tipo de tenencia, que mereció una clara modificación por parte de la Cámara de Senadores tanto en lo referente a la penalidad como así también a su finalidad. En primer lugar, la Cámara de Diputados había previsto para este ilícito la misma pena que en el caso del supuesto establecido en el primer párrafo del mismo artículo, situación que mereció una correcta sustitución puesto que no pareció conveniente que puedan ser pasibles de la misma escala penal las personas que distribuyan, publiquen, faciliten, comercialicen, financien cualquier imagen pornográfica de un menor, que aquel que las tenga, aún cuando también la finalidad de estos últimas sea la de distribuir. Sobre el punto, la Cámara de Senadores acertadamente expuso que al tratarse de ilícitos de diferente peligrosidad no resultaba posible que ambos contengan la misma penalidad. Por otra parte, el Senado incorporó el término "inequívoco" a la redacción de Diputados, de forma tal que en base a la nueva legislación para completar el tipo penal de mención se requiere que el autor en forma inequívoca tenga en su poder imágenes de pornografía infantil con fines de distribución o comercialización.

Más allá de las críticas que puedan efectuarse respecto al término elegido, lo cierto es que su incorporación vino a salvaguardar el principio de reserva contemplado en el art. 19 de la Constitución Nacional.

Este tipo penal, al igual que en el caso anterior, se trata de una figura dolosa, con lo cual se encuentran expresamente excluidos los casos de usuarios que posean imágenes de pornografía infantil sin conocimiento de dicha posesión. Por su parte, al exigirse como finalidad específica que el autor tenga las imágenes aludidas para distribuir o comercializar, si falta esa finalidad, la conducta se torna atípica.

A simple vista pareciera que este ilícito penal vino a despejar cualquier duda relacionada con los planteos que se efectuaban anteriormente respecto a si la conducta prevista en el anterior artículo 128 admitía la tentativa. Más allá de los problemas probatorios que se advertían en torno a esta materia, lo cierto es que la mayoría de la doctrina y la jurisprudencia admitía la posibilidad de que esta conducta podría quedar en grado de tentativa. Actualmente, en base a esta nueva disposición legal, pareciera que existen dos hipótesis, descartándose, en consecuencia, que la figura establecida en el primer párrafo pueda ser tentada. Si el autor ya distribuyó, publicó, divulgó, etc. será autor del primer párrafo del actual artículo 128 del Código Penal, mientras que si el mismo es sorprendido con este tipo de material y se comprueba el fin de distribuir o comercializar será considerado autor del tipo penal establecido en el segundo inciso del articulado bajo análisis.

Por último, en cuanto al tercer párrafo, consideramos que no merece mayor análisis puesto que no ha sido objeto de modificación.

C) Violación de secreto y privacidad

Artículo 3° - Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente: "Violación de Secretos y de la Privacidad"

En las últimas décadas se ha producido un desarrollo acelerado de las tecnologías de la información, siendo testigo la humanidad de una verdadera revolución en las formas comunicación a distancia, principalmente, mediante la utilización de computadoras conectadas e Internet y teléfonos celulares de múltiples funciones.

A raíz de estos avances técnicos y sus reflejos en la vida cotidiana, el derecho a la intimidad de las personas, caracterizado como la esfera de reserva o de autonomía personal exenta de la injerencia del Estado o de terceros, imprescindible en el desarrollo individual y válvula de contención del poder estatal, se ve constantemente amenazado por un sinnúmero conductas hasta hace algunos años impensadas, y por supuesto, inimaginables por el constituyente de 1853.

Entre estas podríamos traer a modo de ejemplo la utilización de sensores de calor que en otras legislaciones ha sido objeto de inclusión en los términos de la inviolabilidad del domicilio, y más relacionado con la presente modificación, se nos ocurren los programas de olfateo o captación informática ("sniffers") siendo sus mayores exponentes los sistemas "Echelon" y "Carnivore", el "spyware", las amenazas lógico informáticas y el hacking.

El derecho a la intimidad como materialización de las libertades ilustradas y garantía legal, ha sido objeto tanto de previsiones normativas como pronunciamientos jurisprudenciales con el fin de precisar su contenido y límites cuando medien razones de interés público superior. Su reconocimiento legal encuentra basamento en el respeto de la dignidad humana, como derecho personalísimo y estandarte fundamental del Estado de Derecho. Así, podemos citar la doctrina constitucional que surge, principalmente, del juego armónico de los artículos 18, 19 y 33 de nuestra Ley Suprema y, de los artículos 11 (incisos 2° y 3°) del Pacto de San José de Costa Rica (CADH) (Adla, XLIV-B, 1250), 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCH) (Adla,

XLVI-B, 1107), 12 de la Declaración Universal de Derechos Humanos y 10 de la Declaración Americana de los Derechos y Deberes del Hombre.

Al mismo tiempo, existen disposiciones específicas en el Código Civil (1071 bis), el Código Penal (Titulo V del Libro II), las Constituciones provinciales, los Códigos rituales y otras normas de naturaleza federal como la ley de Telecomunicaciones N° 19.978 (reformada por la ley N° 25.873) y la ley de Inteligencia Nacional N° 25.520 (Adla, XXXII-D, 5209; LXIV-A, 151; LXII-A, 22).

En el common law norteamericano esta garantía material, bajo el rótulo de "Right of Privacy", ha sido definida como el derecho que cada individuo tiene a permanecer aislado, sólo, dentro de una esfera de reserva o exclusión de la injerencia de otros individuos o del Estado; o sea, "como el derecho de vivir sin interferencias no deseadas por el público, sobre asuntos no que no están necesariamente relacionados con éste" (5).

Justamente, la ley N° 26.388, acogiéndose a la terminología anglosajona, agregó al epígrafe original del Capítulo III, del Título V, del Libro II del Código Penal, "Violación de Secretos" la mención del Bien Jurídico "Privacidad". Dicho cambio de rúbrica, creemos que, por un lado, es acertado pues, como enseñaba Molinario, las disposiciones de este capítulo del Código Penal no sólo protegen datos "secretos" porque correspondencia y papeles privados son cosas íntimas y no necesariamente secretas y, por otro lado, consideramos que si bien la terminología elegida puede entenderse como sinónimo de Intimidad, la interpretación más justa obliga a realizar la siguiente distinción: lo íntimo es necesariamente privado, pero lo privado puede no ser íntimo, de modo que, el resguardo de la intimidad de los individuos exige una protección más intensa que su vida privada (6). De esta manera, queda expuesto que la intención del legislador no ha sido la de acotar la intervención punitiva a los supuestos donde se afecte la intimidad, sino que ha extendido la protección penal a los ataques contra la privacidad del sujeto pasivo.

Considerando cual fue el hecho que detonó la sanción de esta ley (7), corresponde citar antigua doctrina constitucional según la cual "la vida privada del hombre público resulta inseparable de su vida pública, y cuanto más empinada sea la función que se ejerza, más recaerá la atención de los demás sobre sus actos privados" (8). El debilitamiento de la protección de la vida privada de los hombres que desempeñan una función pública, sin embargo, en nuestra opinión no justifica el intrusismo informático y la obtención de datos y pruebas en forma subrepticia e ilegal.

Por último, a modo de simple reflexión, debemos tener en cuenta que, en pleno desarrollo del "Siglo de la Información" (9), nuestra libertad de intimidad, dadas las debilidades técnicas de los sistemas informáticos y el mayor intervencionismo estatal (10), se encuentra materialmente socavada. Paradójicamente, cómo fuera en el pasado, en no pocas ocasiones las normas jurídicas, cualquiera sea su naturaleza, sólo podrán tener efectos simbólicos o meramente declamativos, siendo incapaces de resguardar el Bien Jurídico en términos reales. En este sentido, para Gabriel Baum, profesor de la Facultad de Informática de la Universidad Nacional de La Plata, "lo que ocurra con Internet en las próximas décadas, si la tendencia será hacia la concentración y el control (el "Gran Hermano") o hacia la libertad y la democratización (el oráculo al alcance de todos)… son decisiones que dependen más de la política que de la tecnología" (11). Nótese en este sentido lo antagónico que puede ser el uso de la tecnología informática ya que por un lado permite una ampliación de los derechos individuales, entre ellos la libertad de comunicación, el anonimato, etc., pero por el otro su abuso puede generar un monitoreo y seguimiento intolerable de los hábitos individuales, a través de los registros de los sitios visitados por los usuarios, o por otras tecnologías (ley de filmaciones en la ciudad de Buenos Aires), donde correctamente se hace un llamado de atención por lo extremadamente peligroso de que los gobiernos utilicen este tipo de técnicas para establecer conductas "anómalas" (12). A modo de ejemplo, y partiendo de la base el monopolio sobre la correspondencia establecido en nuestro país a través de la Ley de Correos N° 20216 (13), las situaciones son variadas pudiéndose citar como ejemplos claros a no imitar a Cuba, China y Estados Unidos.

Artículo 4° - Sustitúyese el artículo 153 del Código Penal, por el siguiente:

Artículo 153: "Será reprimido con prisión de quince (15) días a seis (6) 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.

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".

Desde aquel verano de 1971 cuando fue enviado, por el ingeniero Ray Tomlinson, el primer "e-mail", hasta nuestros días, la realidad social en torno al uso de métodos o herramientas de comunicación dista mucho de ser la misma. Algunos datos estadísticos servirán para ilustrar con claridad las progresivas y aún vigentes

transformaciones sociales en este sentido. Según la Comisión Nacional de Comunicaciones, entre los años 1995 y el 2004 el uso de la correspondencia epistolar decreció un 70%. Por su parte, entre diciembre de 2003 y el mismo mes de 2004 se produjo un aumento del número de cuentas de correos electrónicos de más del 40%; asimismo, actualmente existen en nuestro país aproximadamente ocho millones y medio de usuarios de Internet y 2.099.495 cuentas de "e-mail".

Sin embargo, como advertía Riquert, hasta la sanción de la 26.388, la apatía legislativa en materia de criminalidad informática poco aportaba a la seguridad jurídica y claridad que exige el proceso de subsunción de la ley penal (14). Por ello, durante muchos años convivieron en el foro, dos interpretaciones en torno a la tipicidad —o no— de la violación del correcto electrónico o "e-mail".

Algunos autores propusieron una interpretación extensiva, teleológica, progresiva o dinámica de las leyes por imperio histórico (15), mientras otro sector de la doctrina, rechazó esta exégesis de la ley, acusándola de constituir una forma solapada de extensión analógica del tipo penal, vedada al intérprete por imperio del principio de principio de legalidad, en su función de "lex stricta". Asimismo, al respecto, la jurisprudencia no era uniforme, habiéndose establecido, como habitualmente sucede, dos posturas claramente diferenciadas. Un sector, representado por la Sala VI de la Cámara Nacional en lo Criminal y Correccional —integrada por los Dres. Elbert, Escobar y González—, en el caso "Lanata, Jorge s/ desestimación", del 4/03/1999 (LA LEY, 1993-E, 70), sostuvo que "...Nada se opone para definir al medio de comunicación electrónico como un verdadero correo en versión actualizada. En tal sentido la correspondencia y todo lo que por su conducto pueda ser transmitido o receptado, goza de la misma protección que quiso darle el legislador al incluir los artículos 153 a 155 del C.P., en la época de su redacción, cuando aún no existían estos avances tecnológicos". En sentido contrario, el Juzgado Nacional en lo Correccional N° 9 de la Capital Federal, en la causa "Galvez, Esteban" del 11/04/2007, adoptó el criterio opuesto rechazando la asimilación del correo electrónico a la correspondencia privada, señalando, que: "...el principio de máxima taxatividad legal e interpretativa se manifiesta mediante la prohibición absoluta de la analogía 'in malam partem', lo que se verificaría si en la especie se intentara forzar la interpretación que inveteradamente se ha dado no sólo a lo concerniente al objeto de protección de la norma del Art. 153 del código sustantivo, sino a sus quehaceres típicos, por lo que resulta inaceptable dar cabida a la presente querella desde la norma escogida por la querella como la infringida por los intrusos, que accedieron a su correo del servidor Yahoo de Argentina S.R.L.".

Aclarada la situación precedente a la sanción de la "Ley de Delitos Informáticos", a continuación, realizaremos un breve análisis del tipo penal previsto en el artículo 153 del Catalogo Punitivo.

Núñez, definió a la correspondencia como "la comunicación por carta, pliego o despacho telegráfico, fonográfico o de otra naturaleza, enviada por un remitente a un destinatario [...] (siendo) necesario que el remitente sea un interlocutor del destinatario, vale decir, que aquél, mediante esa pieza, establezca un diálogo" (16). Por papeles privados se entiende cualquier expresión de ideas escrita comprendida dentro del ámbito de reserva de una persona. De la redacción típica del delito de "apoderamiento indebido de correspondencia u otro papel privado" parece asimilarse, en una relación de género a especie, los despachos, cualquiera sea su naturaleza —telegráfico, telefónico, etc.— al concepto amplio de papeles privados, siendo esencial, entonces, que el papel escrito "se encuentre dispuesto en forma tal que no baste su simple desdoblamiento para que el texto se ofrezca a la vista" y que su contenido revista el carácter de íntimo o personal, no siendo aptas para configurar el tipo, por ejemplo, una simple nota o publicidad comercial (17).

La ley 26.388 incluye dentro del concepto amplio de "correspondencia" a las comunicaciones electrónicas, solucionado por vía legislativa las controversias generadas en la doctrina y la jurisprudencia sobre la posibilidad de asimilar el correo electrónico ("e-mail") a la correspondencia tradicional. De todas formas, la solución legislativa, plantea algunas dudas, pues el vocablo "comunicación electrónica" parecería no sólo abarcar al correo electrónico sino que extenderse a otros medios de comunicación como los archivos multimedia, servicios de mensajería instantánea (SMS), sistemas de transferencia de datos vía Bluetooh, "chateo", etc. La ausencia de una definición precisa de este concepto, conllevará a su constante reformulación en virtud de los incesantes avances tecnológicos. Por ello, creemos que la jurisprudencia deberá precisar los alcances de este elemento normativo del tipo penal recurriendo a tal fin a la función reductora del bien jurídico. Por ejemplo, el acceso sin autorización del titular de la cuenta de correo electrónico de un mail basura o "spam" no podrá entenderse típico pues en modo alguno se lesiona la privacidad del sujeto pasivo.

Los verbos típicos consisten en abrir (remover los obstáculos que "cierran" la correspondencia -por ejemplo, un sobre lacrado- impidiendo a terceros imponerse de su contenido), acceder (entrar, ingresar, obtener), apoderarse (retener o apropiarse), suprimir (destruir u ocultar alterando la circulación) o desviar (darle un destino distinto al estipulado por el remitente sin alterar la circulación) la correspondencia, comunicación electrónica u otros papeles privados.

En la misma pena, incurre quien sin autorización intercepta (apoderarse, detener, u obstruir) o capta (percibe u obtiene) comunicaciones electrónicas o telecomunicaciones provenientes de un sistema de acceso privado o restringido. La ley 19.798 (Adla, XXXII-C, 3422) define el término "telecomunicación" como toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por

hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

La pena se agrava si el autor, además comunicare a otro el contenido de la correspondencia o papel privado, o lo publique, de modo tal que sea conocido por un número indeterminado de personas. Por último, si el hecho fuera cometido por un funcionario público abusando de sus funciones le corresponderá la pena conjunta de inhabilitación especial por el doble tiempo de la condena.

El Código prevé únicamente la modalidad dolosa de esta figura, extremo que ha merecido la crítica de una parte de la doctrina —a la cual no adherimos— para la cual debiera preverse al mismo tiempo, bajo una amenaza de pena menor, la figura culposa (18).

Artículo 5° - Incorpórase como artículo 153 bis del Código Penal, el siguiente:

Artículo 153 bis: "Será reprimido con prisión de quince (15) días a seis (6) 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 (1) mes a un (1) 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".

El artículo 153 bis reprime como figura de aplicación subsidiaria ("si no resultare un delito más severamente penado") el acceso ilegítimo a un sistema informático. La conducta típica consiste en acceder a sabiendas por cualquier medio e indebidamente (si autorización o excediendo la que se posea) a un sistema o dato informático de acceso restringido. La ley 25.326 de Hábeas Data define al dato informático como los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. Si tenemos en cuenta que el bien jurídico protegido por la norma es la privacidad, resulta razonable exigir que se trate de un dato de carácter personal, circunstancia que restringe lógicamente el ámbito de imputación penal. Por otro lado, es importante resaltar la naturaleza dolosa de este delito, por lo que resultarán atípicas aquellas conductas inocuas y hasta en ocasiones beneficiosas para el titular del sistema o dato informático, como es el denominado "hacking ético", es decir, aquella actividad que sólo persigue descubrir las vulnerabilidades de un sistema informático para mejorarlo sin afectar ni acceder a la información personal contenida en aquél (19). De lo contrario, resultarían punibles conductas que no lesionan el bien jurídico, transformándose al artículo 153 bis en un delito de pura actividad, en un acto preparatorio punible.

Artículo 6° - Sustitúyese el artículo 155 del Código Penal, por el siguiente:

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 otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

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

El tipo del artículo 155, presupone una correspondencia, comunicación electrónica, pliego cerrado o despacho de cualquier naturaleza, que se encuentra en poder del legítimo destinatario. El disvalor del injusto se fundamenta en el perjuicio ocasionado al hacer público —al publicar o hacer publicar— el contenido de la correspondencia o papel privado contra la voluntad del emisor.

La última parte exime de pena al sujeto activo si hubiera actuado con la intención inequívoca de proteger un interés público.

Artículo 7° - Sustitúyese el artículo 157 del Código Penal, por el siguiente:

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".

En este caso, la obligación de guardar el secreto es impuesta expresamente por la ley, en consecuencia, el funcionario, al quebrantarlo, no sólo vulnera un deber genérico de confianza y privacidad, sino, que su acción es antinormativa al contradecir una disposición legal que expresamente lo obliga a guardar silencio. La ley de "Delitos Informáticos" agregó a la fórmula legal la palabra "datos", ampliando el objeto de protección penal.

Artículo 8° - Sustitúyese el artículo 157 bis del Código Penal, por el siguiente:

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".

El artículo 157 bis, en su inciso 1°, reprime con prisión de un mes a dos años al que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales.

Es sujeto activo del delito quien accede a sabiendas (dolo directo) de cualquier forma a un banco de datos personales, enunciando la ley dos modalidades comisivas específicas: acceder "ilegítimamente" o "violando sistema de confidencialidad y seguridad de datos"; es decir, en ambos supuestos debe tratarse de un acceso sin autorización del titular o de la ley.

El objeto de protección penal son los archivos de datos personales, o sea, el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento electrónico o no, cualquiera fuere la modalidad de su formación, almacenamiento, organización o acceso (art. 2°, ley 25.326).

Técnicamente, un archivo, registro, base o banco de datos (data bank) es "un conjunto no redundante de datos organizados e interrelacionados de acuerdo con ciertos atributos comunes en función de los posibles requerimientos de distinta aplicación" (20). Paralelamente, conforme lo exige la Ley de Protección de Datos Personales los referidos bancos de datos deben reunir ciertas condiciones técnicas de inviolabilidad y seguridad; y asimismo, como sostienen Aboso-Zapata, estar destinados a dar informes (art. 1°, ley 25.326, Adla, LX-E, 5426) (21).

En el inciso 2°, el tipo penal sanciona con la misma pena al que 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.

Esta figura no presenta mayores novedades, pues estamos en presencia de una modalidad especial del convencional delito violación de secretos (arts. 156 y 157 C.P.), generada por los avances tecnológicos.

La ley de Hábeas Data (art. 10) coloca en cabeza del titular de una base de datos y de todas aquellas personas que intervengan en cualquier fase del tratamiento de datos personales, la obligación de guardar el secreto profesional, inclusive aún después de finalizada la relación laboral.

Por último, el obligado al secreto sólo podrá revelarlo, sin incurrir en delito, previa autorización judicial o ante la existencia de razones fundadas en motivos de seguridad pública, defensa nacional o salud pública.

El inciso 3°, castiga con la misma pena a quien insertare o hiciere insertar datos en un archivo de datos personales, sumando la pena de inhabilitación especial de uno a cuatro años cuando el autor sea funcionario.

Esta conducta, se encontraba prevista en el artículo 117 inciso 1° del Código Penal, dentro de los delitos que afectan el honor de las personas. Por esta razón, la figura derogada sancionaba la inserción de "datos falsos"; en cambio, la redacción actual, sólo requiere que el sujeto activo inserte o haga insertar "datos" en un archivo de datos personales. No obstante, creemos que la simple conducta de insertar cualquier dato no es suficiente para configurar el injusto penal, se requiere que éste tenga virtualidad suficiente para producir la lesión del bien jurídico.

En caso de que el autor sea funcionario público, sufrirá también la pena conjunta de inhabilitación especial de uno a cuatro años.

Párrafo aparte merece la circunstancia de que el delito bajo análisis, de conformidad con lo establecido por el artículo 73 inciso 2°, es de acción privada, y como consecuencia su persecución debe ser hecha por el damnificado, es decir quien se ve afectado en razón de los datos accedidos.

Así pues, la información privada contenida en las bases y bancos de datos privados bajo la órbita de organismos públicos, en cuanto a su acceso, copia y divulgación resultan abarcados por la naturaleza privada de la acción, resultando dicha situación algo inusual atento a la titularidad de la base de datos, y el sentido común que indicaría claramente la capacidad del Estado de iniciar de oficio la persecución penal.

Por nuestra parte, nos parece acertada la opción del legislador en este sentido. En primero lugar, debe tenerse encuentra el bien jurídico afectado que no es otro que el de la privacidad, que discutiblemente se vería afectado cuando los datos estén contenidos en servidores públicos atento a las limitaciones propias del estado de la capacidad de almacenamiento conforme la ley de Habeas Data (mal podrían ser catalogados como datos privados los nombres, estado civil, domicilio, número de teléfono, beneficio jubilatorio y documento nacional de identidad, entre otros), los cuales pueden ser recabados sin consentimiento.

Algunos problemas que se plantearían en este sentido estaría dada por algunas bases públicas (del Estado) cuyo contenido si debe ser estar reservado; por ejemplo, el Registro Nacional de Reincidencia y Estadística Criminal y las bases fiscales nacionales y provinciales; por lo que avizoramos una futura reforma en breve.

D) Estafa y otras defraudaciones.

Artículo 9° - Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente: Inciso 16. "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".

La ley 26.388, establece además, en su artículo 9° una incorporación al artículo 173. Y esa incorporación será la del inciso 16, como supuesto de defraudación informática o fraude informático.

Si bien es cierto que esta era un cuestión que se esperaba fuera tratada con especial énfasis, dadas las discusiones doctrinarias y jurisprudenciales que se venían presentando en torno a la significación jurídica de hechos que se debatían entre un supuesto defraudatorio o un simple hurto, creemos que la forma en que se ha legislado al respecto mediante esta incorporación no ha satisfecho las expectativas.

Sin embargo, el proyecto de la Cámara baja fue elevado con otros alcances que resultaran luego suprimidos y que serán merecedores de comentario.

Así, bajo el título de "Fraude" y registrado como artículo 11 de dicho proyecto de ley, el inciso 16 se había previsto de la siguiente manera: "El que defraudare a otro mediante cualquier técnica de manipulación y actuando sin la autorización del legítimo usuario del equipamiento, que altere el normal funcionamiento de un sistema informático, o la transmisión de los datos luego de su procesamiento".

Es interesante destacar que el proyecto de diputados incluía como elemento objetivo del tipo la no autorización del legítimo usuario para que se configure el fraude, como así también que la transmisión de datos se produzca luego de su procesamiento. A propósito de esta supresión el Senado supo explicar: "Se conservó la redacción de la sanción de Diputados con dos supresiones. "actuando sin autorización del legítimo usuario", porque se entendió que agrega un elemento al tipo que resulta confuso e innecesario, ya que la autorización no podría excluir la ilicitud de la conducta de defraudar; y "luego de su procesamiento", porque no se encontró el justificativo de fijar el momento técnico de una etapa de transmisión de datos. Por ello en el… presente dictamen no se discriminan esos momentos, dando al juzgador precisión normativa y evitando elementos típicos que lo pudieran hacer incurrir en confusión" (22).

Planteada así la cuestión, corresponde efectuar un análisis global del proyecto incluyendo en aquél las supresiones mencionadas y sus razones.

Así, debe decirse en primer término que la versión final del inciso 16 del artículo 173 del C.P., es poco explicativa y de modo muy forzado podrá decirse que se ajusta a la definición de una conducta defraudatoria. Antes bien, poca diferencia conceptual puede apreciarse respecto del tipo penal de hurto del que pretendía diferenciarse para poner fin a una discusión prolongada.

Por supuesto que el fin se pretende logrado porque la ley existe, lo que es dificultoso es que la misma pueda superar fuertes cuestionamientos de inconstitucionalidad desde que su apego al principio de estricta legalidad en materia penal (art. 18 C.N.) será difícil de defender.

Nótese que la norma elabora como verbo típico el acto de manipular lo que de por sí nada explica puesto que tiene sabor a actividad prolongada sobre un objeto para la obtención de algún provecho (el concepto de perjuicio patrimonial no se aprecia ni siquiera en la norma sino que debe derivarse de su calidad de defraudación especial y su ubicación sistemática en el código sustantivo en el capítulo de los delitos contra la propiedad).

Ahora bien, beneficiarse de la manipulación de algún elemento no es muy distinto al acto de apoderamiento ilegítimo de algo ajeno. Quizá sólo nos dé a pensar en alguna sofisticación o solapamiento a modo de tareas de inteligencia previa, como ya hemos sostenido en otras oportunidades, para intentar acercarnos a algo distinto y más complejo respecto del hurto. Pero lo cierto es que ello es sólo una sensación.

No se entiende por qué razón el legislador insiste en concebir como defraudatorio el acto de apoderarse de manera no evidente de algo ajeno. Quien se apodera de algo ajeno mediante una postura agazapada o expectante, o con la apariencia de realizar actividades inocuas alrededor de la propiedad ajena para hacerse de la misma ante alguna distracción de su titular, no realiza otra cosa que un hurto con independencia del sabor a manipulación o actividad subrepticia que ello pueda tener.

Teniendo presente que no nos hallamos ante una estafa propiamente dicha en los términos del artículo 172, cabe prescindir de la estricta trilogía típica de la figura básica (ardid, engaño, perjuicio patrimonial), tanto como ocurre en los casos de retención indebida o administración infiel (art. 173 incisos 2 y 7), por dar dos ejemplos, en los que el elemento de fraude surge a posteriori sin la estricta relación de determinación o causalidad de los componentes.

Ahora bien, lo que no cabe, existiendo una relación sistemática de figuras típicas respecto de la figura madre, es prescindir de todo concepto conector so pena de inventar un seudo fraude inexplicable como técnica legislativa (al respecto recordar las críticas a la llamada estafa impropia o fraude impropio de la legislación española y alemana que ya hemos formulado con anterioridad que sí hallaron voces que las defendieran como un supuesto de estafa) (23).

Es de toda evidencia que en esta fórmula se ha prescindido totalmente de la interacción del sujeto activo con el sujeto pasivo, aún cuando se diga "defraudare a otro" sin contenido a la intervención de ese "otro".

Interacción esa que resulta necesaria para cualquier supuesto de defraudación. Nótese que en todos los demás casos existe en la fundamentación de la prohibición, la frustración dolosa de expectativas del co-protagonista como definición del acto de defraudar.

Aquí en cambio, los protagonistas vuelven a ser el sujeto activo y la máquina o sistema informático "manipulado" para beneficio del primero, sin entrar jamás a escena la segunda voluntad humana defraudada en la relación contraída.

De modo que el sistema o dato informático pasa a ser medio, objeto y sujeto de la presunta defraudación. Tamaña unilateralidad en la realización del acto lesivo o disvalioso lo acerca más al apoderamiento como acto de sometimiento de uno a otro prescindiendo de la voluntad de ese otro, ya sea para hacerse de la cosa bajo engaño, o relacionarse lícitamente en un primer tramo para en un segundo defraudar su buena fe.

De modo que la técnica legislativa sigue sin ser satisfactoria teleológicamente, es decir, a nivel de la finalidad de la criminalización de la conducta en ese capítulo del digesto penal, no se han satisfecho tales pretensiones presentándose el caso como una caprichosa política criminal que pretende elevar a la categoría de defraudación lo que ontológicamente no difiere de la conducta ya criminalizada por el hurto.

Es decir, quien se vale de fallas de un sistema informático o lo "manosea" hasta hallarla o generarla, no defrauda con eso sólo sino que se apodera (por ejemplo si de esa manipulación se deriva la mutación de dinero contable pasado de una cuenta a la otra. Allí, cuando se extraiga el dinero, el mismo ya se encontrará en la cuenta B, con la maniobra perfeccionada y agotada como acto de apoderamiento ilegítimo de cosa ajena desde un concepto amplio de "cosa") (24).

Por su parte, debemos efectuar esta interpretación, en punto a que el legislador imagina una nueva conducta que en sí no difiere del hurto, ya que de legislar pensando en la contratación virtual desplazando patrimonio bajo engaño al recibir algún correo o ingresar a alguna página imitada o simulada, no haría más que reeditar los alcances del artículo 172 C.P. como figura base de manera innecesaria pues se mantendría la estructura de ardid-error-disposición patrimonial perjudicial y no se alcanzaría ningún ribete de defraudación específica del artículo 173 C.P.

Incluso se debe descartar como ejemplo, el supuesto de "phishing" (como captación de datos personales mediante correo o páginas web falsas) donde se hace ingeniería social obteniendo información pero sin que de por sí implique desplazamiento patrimonial alguno. Es decir, a lo sumo se captarán datos bajo engaño violando la privacidad como nuevo bien jurídico ya comentado con la víctima como instrumento a modo de autoría mediata, pero no se superará el mero acto preparatorio sin principio ejecutivo de estafa o maniobra fraudulenta alguna, pues el uso de esos datos será posterior y hasta allí, eventual.

Por lo cual, si se legisla bajo un nuevo inciso es porque se ha pensado en algo diferente y específico que no se ha definido con éxito, ya que de repensarse una estafa convencional pero en un contexto o con medios informáticos, sería innecesaria la ampliación del artículo 173 porque ya ingresaría en la esfera del artículo 172 C.P. (no pretendemos ver allí un hurto), y además iría en contra del espíritu global de la reforma que apunta a modificaciones necesarias de figuras ya existentes (valiéndose incluso de la ampliación terminológica inicial del art. 77) en lugar de la expansión punitiva.

Nótese de seguido, que la confusión e imprecisión no es solucionada por la supresión de la no autorización del usuario (recordar la supresión de senadores respecto de diputados) pues ello, si bien evita una casi identificación con la descripción de la figura de hurto que hubiera potenciado las críticas aquí (ello por cuanto la ilegitimidad del apoderamiento en el art. 162 C.P., como elemento normativo del tipo ya lleva implícita la ausencia de venia del titular), nos recuerda que el legislador ha prescindido de la interacción del co-protagonista perjudicado en la maniobra.

Esta ausencia, refuerza la crítica en punto a que ontológicamente la conducta prescinde del concepto de "defraudar" que recoge el artículo 172 y desparrama en la generalidad de las figuras específicas del artículo 173 C.P. A cambio de esa distorsión del significado de "defraudar" se hace hincapié en la malicia o maquinación (léase manipulación), como si ello lo resolviera todo y nos devolviera el componente de "fraude" distintivo de la figura.

Al respecto, es de toda procedencia reparar en el concepto de defraudar. Así, el diccionario de la real academia española dice: "defraudar: (Del lat. defraudare). 1. Privar a alguien, con abuso de su confianza o con infidelidad a las obligaciones propias, de lo que le toca de derecho. 2. Frustrar, desvanecer la confianza o la esperanza que se ponía en alguien o en algo. 3. Eludir o burlar el pago de los impuestos o contribuciones. 4. Turbar, quitar, entorpecer" (25).

Es de toda evidencia que la concepción legislativa que se aprecia como común denominador del acto de defraudar como verbo típico medular discurre por el abuso de la confianza depositada, la frustración de expectativas y buena fe o posturas elusivas ante reclamaciones de la contraparte.

Claramente, tal cual lo anticipáramos, el co-protagonista defraudado siempre está presente en la definición de estas defraudaciones específicas, ya sea cuando se defrauda en la calidad de las cosas al co-contratante,

cuando se retiene lo que debe devolverse y alguien reclama, cuando se desvía lo entregado en mandato, etc.

Siempre se presenta el sujeto activo defraudando las expectativas de buena fe depositadas por parte del sujeto pasivo en una relación bilateral definida claramente y que escapa a la estructura convencional de la figura básica al incorporar caracteres propios. Sea viciando su voluntad mediante ardid generador de error (versión base del art. 172) o surgiendo el contenido fraudulento en un segundo momento sin ese yerro como componente central. Pero siempre se defrauda a otro.

De todos modos, sea viciando su voluntad mediante ardid generador de error (versión base del art. 172) o surgiendo el contenido fraudulento en un segundo momento sin ese yerro como componente central, siempre se defrauda a otro. Esa definición no se aprecia con la armonía del caso, en el inciso 16.

En el mismo se hace foco en la actitud del infractor de manipular el sistema y anormalizarlo, lo cual no necesariamente reclama la coexistencia de otra figura defraudada.

Pues bien, pareciera que el legislador hizo base en un concepto de defraudar distinto, más acotado y cercano a su última acepción como turbación o quite de lo que es ajeno, lo cual nos acerca más a la voz "apoderarse" propia de la figura del hurto.

Es inadmisible concebir la defraudación en una misma línea en todas las figuras preexistentes y mutarla aquí para hacer hincapié sólo en el perjuicio derivado de manipular o traspasar datos (ergo apoderarse), pues ese cambio intempestivo reflejaría toda incoherencia lógica y sería de una hermenéutica inadmisible dentro de la interpretación sistemática que debe hacerse de las normas penales.

Tampoco cabría pretender legitimar la descripción como un caso de defraudación por desvío de lo que es confiado mediante adulteración del sistema informático, pues para ello ya existe la administración fraudulenta, de modo que esa interpretación no es posible pues implicaría admitir que estamos ante un legislador que haciendo casuística legisla dos veces lo mismo, como un caso de administración infiel informática. Ello es de toda improcedencia como argumento en defensa de la figura, ya que implicaría contradecir todo el espíritu de la reforma que se encarga de introducir conceptos generales para alcanzar nuevas tecnologías en la comisión de delitos ya existentes y no ampliarlos por el mero hecho de la utilización de "lo informático".

Si la intención era prever una administración fraudulenta informática se hubiera ampliado terminológicamente el artículo 173 inc. 7° (si es que resulta necesario) en lugar de introducir el inciso 16 como descripción de una nueva conducta típica con notas propias.

Ergo, el legislador cree estar frente a un nuevo formato de defraudación pero no lo define como tal y en la ausencia de claridad se pretende solucionar debates doctrinarios y jurisprudenciales cuando en verdad se están exacerbando con este tipo de legislación.

Por lo demás, la confusión generada por la temporalidad de la conducta ("luego de su procesamiento") permite entender acertada su supresión.

A su turno, la aclaración de que la manipulación debe ser informática, como agregado del senado al proyecto de diputados, explica demasiado poco dado que el componente de lo "informático" se satisface ya con el objeto de la manipulación que no es otra cosa que el sistema informático o sus datos transmitidos.

Por su parte, resta hacer pie en la consecuencia de la manipulación que el tipo requiere, es decir, la alteración del normal funcionamiento.

Al respecto cabe insistir en su vaguedad e imprecisión puesto que, si la manipulación debe derivar en la anormalidad funcional como único supuesto para que opere la norma, la laguna de atipicidad que pretendía llenarse seguirá intacta en los casos en que la manipulación consista en el usufructo de grietas o fallas del sistema preexistentes y no provocadas.

Si el verbo típico que pretende recoger el elemento distinto de defraudar con el que comienza el tipo es la manipulación, debiera ser indiferente que ella cause la alteración funcional para que la maniobra prospere o que ella preexista a la manipulación pero que con la misma se aproveche la falencia para derivar en el resulta lesivo.

No olvidemos que detrás de la norma se ubica la propiedad como bien jurídico protegido y no el normal funcionamiento del sistema en sí mismo. Esta es otra falencia a nivel gramatical o estructural que suma imprecisiones de entidad como para superar la constitucionalidad exigida por principio de legalidad en el marco de una política criminal liberal.

En esta falencia legislativa podríamos hallar otra razón para verificar que se ha partido de un debilitado y fungible concepto de defraudar, ya que si se pretende hacer base en la maquinación o malicia del manipulador, no habría razón para dejar fuera el que usufructúa la grieta o anormalidad preexistentes en el sistema. De todos modos, de receptarse ese supuesto entraríamos en la asimilación al delito de hurtar aprovechando un infortunio previo que es fundamento de un plus punitivo como figura agravada (art. 163 inc. 2 del C.P.).

A su turno, si se pretendiese sostener que no se toma el caso de valerse de la alteración del sistema porque la defraudación se halla en la alteración provocada, se estaría, nuevamente, distorsionando el concepto de defraudación ya que el dañar cosas para hacerse de un valor ajeno (de carácter económico claro está en este

caso), no modifica los alcances del concepto de apoderarse. Y el dañarlo con deseos de no ser descubierto tampoco, pues ello no difiere de la voluntad o sentir de todo infractor que pretende escapar a la detección de su maniobra.

En suma, debemos decir que esta norma distorsiona el concepto de defraudar recogido en todo el capítulo, toma quizá de manera solapada la última de las acepciones gramaticales que se asimila al acto de apoderarse propio del hurto (que es en definitiva lo que está legislando, esto es, un hurto sofisticado pero hurto al fin), y que aún con todo ello, de manera confusa y poco respetuosa del principio de estricta legalidad, fuerza un concepto para elevarlo punitivamente a la categoría de defraudación sin caracteres óntico-ontológicos a nivel de la conducta descripta que se diferencien del apoderamiento ilegítimo de lo ajeno ya contenido en el artículo 162 de la ley de fondo.

La felicidad con que parte de la doctrina ha recibido esta incorporación, sólo se explica a partir de la previa decisión inmodificable de inventar un caso de defraudación por el sabor a poco que, punitivamente, genera encuadrar esos casos en el delito de hurto.

Ahora bien, si esa es la razón político criminal para legislar de ese modo, y si el producto normativo nace con tamaños déficits, poco hay para festejar.

Afirmamos entonces que este inciso 16 resulta una de las piezas más débiles, o pasible de mayores objeciones de esta reforma, que en general hemos calificado de acertada.

E) Daño

Artículo 10. - Incorpórase como segundo párrafo del artículo 183 del Código Penal, 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".

Artículo 11. - Sustitúyese el artículo 184 del Código Penal, por el siguiente:

Artículo 184: "La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

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 delito en despoblado y en banda;

5. Ejecutarlo en archivos, registros, bibliotecas, museos o en 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; o en datos, documentos, programas o sistemas informáticos públicos;

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".

Las diversas posturas doctrinarias y jurisprudenciales planteadas al interrogante de si las nuevas realidades tecnológicas se encontraban contempladas y, por ende, protegidas en alguna de las figuras penales enunciadas precedentemente (es decir, art. 183 ó art. 184 del Código Penal) como así también si la información almacenada en el disco rígido, un diskette o la memoria de una computadora podía ser objeto del delito de daño se encuentran actualmente respondidas sin mayores inconvenientes ante las incorporaciones y sustituciones efectuadas por la ley 26.388.

Previo a efectuar un análisis exhaustivo sobre la normativa actual, entendemos prudente recordar que a criterio de los suscriptos, con anterioridad a la modificación bajo análisis, los llamados "daños informáticos" no se encontraban previstos en los casos señalados por los arts. 183 y 184 del Código Penal, puesto que expresamente el articulado mencionado en primer término se refería como objeto de delito a las cosas muebles, concepto normativo definido por el artículo 2311 del Código Civil que reza "Se llaman cosas en este Código, los objetos materiales susceptibles de tener un valor. Las disposiciones referenciadas a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de apropiación". Es decir, "cosa mueble" implica todo objeto detectable materialmente, transportable y susceptible de tener un valor, definición que impediría considerar a un archivo de computadora almacenado en un soporte informático como cosa mueble y, en consecuencia, como objeto del delito de daño. Sobre el punto se ha explayado la doctrina al señalar que "El contenido intelectual o la información almacenada, es decir la idea que transmite considerada como abstracción, no puede ser comprendida en el concepto de cosa mueble ... al destruir o borrar un archivo, esto es el disquete, no se daña, pues puede volver a utilizarse" (26).

Sin embargo, sobre el punto la doctrina no ha sido pacífica en lo que respecto a los elementos característicos de la cosa. Así, un sector doctrinario entendió que aquellos son su corporeidad y su valor patrimonial. Para

algunos autores —como Soler— la corporeidad exige la ocupación de un lugar en el espacio, mientras que para otros —por ejemplo, Núñez— bastaría que el objeto pueda ser detectado materialmente.

Oportunamente entendimos que, en base a tal legislación, se opte por uno o por otro concepto, lo cierto es que ningún archivo o página web podía asimilarse al concepto de cosa, por no tratarse de un objeto corpóreo ni pasible de ser detectado materialmente, extremo que necesariamente conducía a la atipicidad de aquellas conductas dirigidas a dañar, destruir o inutilizar archivos, contenidos intelectuales o información almacenada en un soporte, diskette, disco rígido, unidad de almacenamiento extraíble o pendrive u ordenador. Así, fue entendido jurisprudencialmente por la Sala VI de la Excelentísima Cámara Nacional de Apelaciones en lo Criminal y Correccional en el conocido caso "Piamonti", de cuyos considerandos se advierte que "el borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito de daño (art. 183 C.P.), puesto el concepto de cosa es aplicable al soporte y no a su contenido" (27).

Por último, postulamos que una interpretación extensiva y forzada del concepto de cosa comprendería una acepción que implicaría un claro menoscabo al principio de legalidad establecido en el artículo 18 de la Constitución Nacional y que la aplicación de una pena por el daño inmaterial (datos, programas, software) sería una analogía in malam partem.

Sin embargo, como fuera señalado en los párrafos que anteceden al comenzar el comentario de los artículos que aquí se analizan, la nueva redacción de los mismos conlleva necesariamente a despejar cualquier tipo de interrogante sobre la destrucción, alteración o inutilización de un dato, documento, programa o sistema informático.

Pasando a analizar la primera de las figuras —art. 183— se advierte que el proyecto final incorporar un nuevo párrafo a su redacción anterior. Así, indica que tendrán la misma pena – es decir, de 15 días a un año, el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos, a la vez que también pune a todo aquel que vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daño.

En cuanto a la primera parte de este artículo y específicamente en cuanto a sus acciones o verbos típicos, no se advierte mayores diferencias con el primer párrafo del artículo 183 anterior. Así, el artículo bajo estudio enumera —ejemplificativamente— las modalidades en que puede cometerse el ilícito, ya sea destruyendo la cosa (arruinando o alterando su esencia), inutilizándola (haciéndola inepta) o alterándola (modificando un archivo de datos o programa sin destruirlo completamente). Más allá que estos tres conceptos no se diferencian en demasía de aquellos previstos en el tipo penal original, lo cierto es que resulta acertada la sustitución del término desaparecer (que podría definirse como la acción de colocar la cosa fuera del alcance de su titular) por alterar. Sin perjuicio de lo expuesto, merece destacarse que tal enumeración es meramente enunciativa y no taxativa, de forma tal que cualquiera fuera la conducta perpetrada por el autor que conlleve un daño sobre el objeto del delito configuraría el tipo penal de referencia.

Ahora bien, hasta la sanción de esta nueva normativa penal eran objeto de delito las cosas muebles e inmuebles siempre que sean ajenas. Actualmente, se incorporan como objeto de protección penal los datos, documentos, programas o sistemas informáticos.

Además de ello, se incorporó como una nueva modalidad delictiva a la venta, distribución, circulación o introducción en un sistema informático de cualquier programa destinado a causar daño. Efectivamente debemos encontrarnos ante un programa cuyo principal objeto sea el causar un daño a un sistema informático, de forma tal que se pune a toda persona que encontrándose en poder de los mismos los venda, distribuya o coloque en circulación.

En ambos casos se tratan de figuras dolosas, que en su aspecto subjetivo expresamente requieren el conocimiento y voluntad de dañar un sistema, programa, documento o dato informático. Ante la falta de esa finalidad, la conducta se torna en atípica.

Como en el caso de los delitos de pornografía infantil, su investigación se encuentra a cargo del Poder Judicial de la Ciudad de Buenos Aires en función de los Convenios de transferencia de competencias penales celebrados entre la Nación y la Ciudad Autónoma de Buenos Aires (ley 26.357, Adla, XLI-A, 25 y 2257).

En lo que a este artículo se refiere se evidencian una serie de cambios con la versión original remitida al Senado por la Cámara de Diputados. Así, en aquél proyecto se preveía una escala penal mayor para ambos supuestos delictivos, puesto que la pena a imponer comprendía una escala de un mes a dos años de prisión. Por su parte, el proyecto sancionado por la Cámara de Diputados subdividía las nuevas modalidades delictivas en dos incisos, advirtiéndose modificaciones por parte de la Cámara de Senadores sólo en cuando al primero de ellos. De esta forma, de la lectura del artículo 12 de la versión original surge que se preveían como acciones típicas el destruir en todo o en parte, el borrar, el alterar en forma temporal o permanente o el impedir la utilización de datos, documentos o sistemas informáticos cualquier sea su soporte. La Cámara de Senadores solamente se limitó a sancionar los verbos típicos, sin especificar si la destrucción, alteración o inutilización debe ser total o parcial, sobreentendiéndose que será punible cualquiera sea la afectación del daño al objeto de delito -recuérdese que el bien jurídico protegido es la propiedad, con lo cual en nada importa si esta se ve

afectada total o parcialmente, siempre y cuando se vea afectada-; por otra parte también incorporó al catálogo de objetos a los programas informáticos y descartó la expresión "cualquier sea su soporte", por cuanto al encontrarse protegidos los datos, documentos, programas o sistemas informáticos se sobreentiende que esa expresión resulta sobreabundante y, en consecuencia, innecesaria.

Por último, en cuanto al artículo 11 de la ley 26.388, corresponde señalar que a través del mismo se sustituyó el inc. 5 del artículo 184 y se incorporó el inc. 6 en el mismo precepto penal. En este caso, se trata de un agravante del daño informático, que al igual que en la redacción actual tiene previstas penas de prisión de tres meses a cuatro años y que, por los mismos motivos expuestos para el caso anterior, también estos supuestos deben ser investigados por el Poder Judicial de la Ciudad Autónoma de Buenos Aires.

Expresamente en el caso del inciso 5 la agravante está relacionada con el objeto atacado, habiéndose incorporado en el catálogo anterior a los datos, documentos, programas o sistemas informáticos públicos. Por su parte, se incorporó el inciso 6, de cuya lectura también se evidencia que esta relacionado con el objeto del delito, puesto que si el daño recayere sobre sistemas informáticos destinados a la prestación de servicio de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público, con encontraríamos ante un daño agravado.

Sobre estas incorporaciones debemos recordar que al igual que en el caso del daño simple se trata de una figura penal dolosa y que la redacción final se corresponde íntegramente con la versión original remitida al Senado por la Cámara de Diputados.

Finalmente, como fuera expuesto en párrafos precedentes, esta modificación permite disipar las discrepancias advertidas en la práctica respecto a la tipicidad o no de los daños provocados en sistemas informáticos.

F) Interrupción de las comunicaciones

Artículo 12. - Sustitúyese el artículo 197 del Código Penal, por el siguiente:

Artículo 197: "Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida".

El artículo 12 de la ley que nos toca analizar ha venido también a dar tratamiento a una cuestión fundamental en esta época que nos toca vivir, que tiene como núcleo por un lado a la información digitalizada, y como lógica consecuencia a su trasmisión. Por el otro lado, y como segunda cuestión central nos encontramos con la utilización de las redes y de la Internet para permitir la intercomunicación local e internacional de las personas. Así pues, la transmisión de información (publicación y envió) y las conversaciones o diálogos montados en la red son formas de comunicación entre las personas, y es allí donde existía un vacío legal, el cual debía ser por aplicación de la lógica jurídica actualizado.

El artículo 197 del Código Penal, en su aspecto tradicional, no tuvo siempre la mirada complaciente del legislador siendo el mismo derogado en dos oportunidades retornando a su vigencia finalmente por la Ley de Defensa de la Democracia (23.077, Adla, XLIV-C, 2535).

La diferencia entre la fórmula tradicional y el nuevo y flamante artículo radica en el agregado de la frase "o de otra naturaleza".

La modificación aludida, sin perjuicio de su tratamiento en anteriores antecedentes no ha sido objeto de análisis en los fundamentos para el dictamen de sanción dirigido al Poder Ejecutivo Nacional (CD 109/06), y sólo incorpora a los efectos que aquí interesan para su comentario nuevos canales por los cuales hoy se puede materializar el bien jurídico, quedando vigente toda la discusión dogmática anterior relativa a los sujetos de delito, el momento consumativo, el aspecto subjetivo, ubicación sistemática (28), si nos encontramos ante un servicio público (29), etc.

Aclaremos que el bien jurídico protegido es entonces la comunicación, que en lo que respecta al tipo penal no necesita estar en curso de ejecución. Es decir, la intención del legislador es la de garantizar la posibilidad de comunicarse por parte de la ciudadanía (30).

La actualización, necesaria por cierto, se produce como dijimos sólo de los medios pero lamentablemente a través de un dispositivo cuya utilización nos parece desacertada. Con la frase "o de otra naturaleza", se abre un abanico de posibilidades tan amplia que resultarán abarcadas conductas totalmente extrañas al objetivo del tipo penal. Debemos preguntarnos si por comunicaciones de otra naturaleza no podrían entenderse a aquellas efectuadas por dos individuos en forma personal. En ese sentido, debe tener en cuenta la amplitud del término comunicación (31).

Por mucho, hubiera resultado saludable el agregado de comunicaciones telefónicas, telegráficas, "electrónicas o digitales", para abarcar toda la serie de gamas de las actuales comunicaciones modernas, sin poner en juego la posibilidad de que el tipo penal no cumpla con las características del principio de legalidad, teniendo en cuenta el reciente fallo "Kimel" de la Corte Interamericana de Derechos Humanos (32) que pone en tela de juicio dichas circunstancias respecto de los delitos de calumnia e injurias, y que son abarcativas de este

tipo de artilugios legislativos.

Dicho esto, entendemos que en lo atinente a la informática quedan abarcados ahora los casos que afecten las comunicaciones entabladas mediante los sistemas de mensajería instantánea, voz sobre ip, los protocolos sobre los cuales corren los servidores de correo, telefónica celular, mensajería de texto, radio unilateral y bilateral, las redes internas, así como las redes privadas virtuales, y cualquier otro sistema que de cualquier forma permita el diálogo o la trasmisión de información entre dos o más personas.

Así pues, el presente artículo pasa ahora a ser más abarcativo que la contravención establecida en el artículo 44 del Código Contravencional de la Ciudad de Buenos Aires, dándose así respuesta al interrogante de Marín Fraga (33).

G) Destrucción de prueba

Artículo 13. - Sustitúyese el artículo 255 del Código Penal, por el siguiente:

Artículo 255: "Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o 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 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)".

Como vemos, se mantiene la previsión de la versión dolosa y la versión culposa de la figura, se conservan los mismos verbos típicos a la hora de delimitar la conducta prohibida a excepción de la voz "alterare" que se incorpora, y se muta el concepto de culpable por el de autor.

Esto último, que no se incluyera en el proyecto de diputados dado que se mantenía el concepto de "culpable", no requiere mayores comentarios más allá de interpretarlo como un acierto a la hora de eliminar conceptos que van más allá de la imputación de conductas al nivel de tipicidad y ya conllevan la configuración de un delito por la determinación de la culpabilidad. Parece acertado prescindir de anticipaciones a la hora de describir la conducta prohibida.

Respecto de la incorporación del acto de alterar como propio del tipo penal, es de destacar que ello es armónico con otros tipos penales del mismo proyecto ya analizados y parece acertado dada su compatibilidad con el fundamento de la prohibición.

Es decir, si se protegen los instrumentos que adquieren calidad de medios de prueba, su mutación material o sustancial, ya ingresa en el ámbito de protección de la norma pues distorsiona ese valor probatorio adquirido, reconocido y protegido.

Para que esa afectación a la entidad probatoria se dé cómo justificante de la punición, no es necesaria, la eliminación del medio de prueba como se da al ser destruido o inutilizado, o su inaccesibilidad, como ocurre cuando se lo sustrae u oculta.

También se dará esa afectación a lo que resulta objeto de tutela, y de manera idónea, cuando el medio de prueba aparece actual y accesible pero modificado, alterado en su conformación.

Ello así, pues perderá el valor previamente conferido en tanto ya no se tratará del mismo documento u objeto a nivel de valor probatorio, más allá de que se lo pueda apreciar sensorialmente o hallar en el lugar dejado.

En definitiva, el alterar lo existente, es equivalente a su eliminación u ocultamiento para tornarlo inaccesible, pues será aprehensible pero sustancialmente diferente perdiendo las notas características que le daban valor.

Esto nos lleva a aclarar, que la alteración debe ser en un aspecto medular del documento, registro u objeto calificado como elemento de prueba o confiado en su custodia por razones de interés público, por lo que una mutación insignificante o significativa pero periférica (es decir, en un aspecto no esencial para que el elemento haya adquirido valor probatorio previamente), no llenará la norma y deberá quedar fuera de la prohibición por cuestiones de atipicidad.

Algo similar a lo que ocurre con la falsedad ideológica del artículo 293 del C.P., en tanto se entiende doctrinaria y jurisprudencialmente que la falsedad histórica introducida en un documento en sí auténtico, debe radicar en aquello que el documento debía probar como información central.

Lo dicho resulta de interés ya que la norma, como otra diferenciación respecto de la versión sustituida, incorpora la afectación al elemento de prueba "en todo o en parte", lo cual se aprecia adecuado pues su afectación parcial, antes no contemplada, podría tornar letra muerta la norma, ya que el infractor erradicaría lo importante y dejaría subsistente lo inútil.

Esto reafirma lo dicho en cuanto a que lo que se afecte debe ser relevante en términos de valor probatorio, y

no información secundaria, tal cual sostuviéramos al plantear la analogía con el delito de falsedad ideológica.

En cuanto al concepto de "documento", que en sí es lo que hace a la materia informática, es de hacer notar que la ley en su versión final suprimió la frase "cualquiera fuese el soporte en que estén contenidos" que traía el proyecto de diputados ya que resulta innecesario dada la previa definición terminológica en el nuevo artículo 77 que amplía los alcances del concepto de documento, aspecto en el que el proyecto de diputados era más acotado, como ya hemos analizado más arriba.

De modo que el contenido informático adquiere reconocimiento como objeto de protección por vía del nuevo artículo 255 en función del nuevo artículo 77 C.P., y nos invita a pensar en casos en los que los datos informáticos puedan revestir calidad probatoria a nivel judicial.

Desde ya que la protección es al contenido de valor probatorio entendido como la información, más allá del soporte físico.

Respecto del art. 77 C.P., estamos a lo ya dicho en su oportunidad en este trabajo, con la aclaración de que en definitiva, sea cual fuere la naturaleza del instrumento (público o privado), en tanto revista carácter de medio de prueba por afectación a un proceso judicial determinado, allí le será dada la calidad de público.

Finalmente en lo que hace a la versión culposa, no cabe ahondar demasiado pues no habrán de esgrimirse comentarios específicos en materia de criminalidad informática que es lo que nos convoca, más allá de hacer notar ciertas discrepancias que bien pueden hallarse en cualquier comentario en general de ésta o la anterior versión del artículo 225 de la ley de fondo.

Me refiero a lo cuestionable que resulta criminalizar cualquier daño de lo que se custodia pues implicaría un depósito perfecto ajeno a cualquier afectación no querida, lo cual coloca al depositario o custodio, sea o no funcionario público, en una obligación de resultados de difícil cumplimiento. Piénsese que hasta un magistrado podría ser sancionado si por algún descuido, casi propio de cualquier actividad diaria o doméstica, estropeara hasta lo ininteligible, un expediente del Tribunal a su cargo.

En lo atinente al material informático, simplemente podría agregarse que mantener inmaculado un dato, archivo o documento informático que pueda revestir carácter de medio de prueba, es más difícil aún en tiempos en los que abundan maniobras que ponen a prueba los niveles de seguridad en busca de nuevos umbrales de vulnerabilidad en el marco de un actividad, de momento elitista, en cuanto a que su dominio profesional o al nivel de expertos es de muy pocos, sin haber alcanzado ese dominio un nivel masivo.

De modo que criminalizar la pérdida negligente de un documento en tal soporte, parece peligroso en tiempos en los que nadie puede conocer a ciencia cierta con qué nivel de diligencia alcanza para escapar a la norma prohibitiva, pues nunca se sabe si estamos o no frente a otro que sabe más y más capacidad tiene para sortear la autoprotección.

Ello requerirá esfuerzos del juzgador para definir en el caso concreto cual era el cuidado esperable para evitar la vulnerabilidad y para ello necesitará de expertos (si los hay) que colaboren a nivel de administración de justicia.

Este tipo penal abierto, por la materia puntual que tratamos, compleja, explorada permanentemente y llena de imponderables aún no resueltos ni imaginados, será más abierto aún y exigirá mayores esfuerzos y prudencia de parte de los magistrados.

III. Consideraciones criminológicas a la ley 26.388

Desde una perspectiva criminológica la Ley 26.388 de reforma en materia de criminalidad informática al Código Penal, no exhibe una remisión terminológica y conceptual a la Escuela Positivista de la Criminología (34), no ha recurrido en tal sentido a una clasificación Biotipológica o en este caso puntual Cibertipológica de autores.

Es así que la Ley 26.388, lejos de recurrir a un derecho penal de autor, con su correlativa clasificación de autores de la criminalidad informática, se orienta claramente a un derecho penal de acto, dirigiéndose en forma directa a reglar las conductas o acciones pasivas de sanción penal.

En este sentido, la presente ley de reforma en materia de criminalidad informática al Código Penal de la Nación, en ningún de los tipos penales contemplados (Ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (Artículo 128 C.P.N), Violación de Secreto y Privacidad (Artículos 153, 153 bis, 155, 157, 157 bis C.P.N), Estafa y otras Defraudaciones (Artículo 173, inciso 16, C.P.N.), Daño (Artículo 183 y 184, C.P.N.), Interrupción de comunicaciones (Artículo 197 C.P.N.), Destrucción de prueba (Artículo 255 C.P.N.), ha recurrido al empleo de una Biotipología de autores de la Criminalidad Informática o Cibertipología como puede ser las designaciones de: 1) Hacker (35); 2) Cracker (36); 3) Preaker o Phreaker (37); 4) Phisher (38); 5) Sniffer (39); 6) Virucker (40); 7) Propagandista informático (41), 8) Pirata Informático (42), o 9) Cyberbullyng (43) o Ciber-Acosador.

Puede decirse en este sentido que la presente ley de reforma en materia de criminalidad informática al Código Penal, resulta por demás aséptica en el empleo de su terminología y definiciones conceptuales.

Ello puede contemplarse en haber introducido todos los preceptos, conceptos, definiciones y terminologías en el Artículo 77 del Código Penal de la Nación, empleando como cláusula genérica situada en la parte general del Código Penal y despojándola en absoluto y por completo de todo tinte criminológico no sólo positivista sino también sociológico, criminológico crítico o de un realismo de derecha o de izquierda.

IV. Conclusiones político-criminales de la ley 26.388

Incursionando en un análisis Político-Criminal de la Ley 26.388 de reforma en materia de criminalidad informática al Código Penal de la República Argentina, puede verificarse, en primer orden que, desde un perspectiva de la técnica legislativa empleada, el legislador ha acudido a la instrumentación de una ley de reforma integral y concordada al Código Penal y no ha recurrido al empleo de una ley complementaria.

Como consecuencia de la instrumentación de una ley de reforma integral, armónica y concordada con el Código Penal, no se crean nuevas figuras delictivas o tipos penales, sino que se modifican ciertos aspectos de los tipos penales ya contemplados, con el objeto de receptar y captar las nuevas tecnologías como medios comisivos para su ejecución.

En este orden de ideas el Modelo Político Criminal bajo el cual se ha enfocado este proyecto de reforma puede clasificarse como un Modelo Político Criminal Liberal (44), de corte reductor, no expansionista o Panpenalista (45), ya que ha alcanzado con su reforma un número muy limitado de tipos penales como lo son: 1) El Ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (artículo 128 C.P.), 2) Violación de Secreto y Privacidad (artículos 153, 153 bis, 155, 157, 157 bis C.P.), 3) Estafa y otras Defraudaciones (artículo 173, inciso 16, C.P.N.), 4) Daño (artículo 183 y 184, C.P.), 5) Interrupción de comunicaciones (artículo 197 C.P.), 6) Destrucción de prueba (artículo 255 C.P.).

En este sentido puede decirse que la Ley 26.388, posee como base el Proyecto de Ley de Leonor E. Tolomeo de 1996, que preveía una ley de reforma integral, armónica y concordada sobre el Código Penal de la Nación, y sobre esta plataforma normativa se ha perfeccionado su técnica legislativa con los aportes efectuados por los diversos proyectos presentados en los años subsiguientes como han sido los Proyectos de: 1) Carlos "Chacho" Alvarez (1996); 2) José A. Romero Feris (1996); 3) Antonio T. Berongaray (1997); 4) Anteproyecto de Ley de 2001; 5) Anteproyecto de Ley de 2005; 6) Proyectos de ley de Delia Bisutti (2032-D-06), 7) Canevarolo (3001-D-06), 8) Diana Conti y Agustín Rossi (2291-D-06), 8) Silvia Martinez (1798-D-05), 9) Marta Osario (1225-D-05) y 10) Andrés Sotos (985-D-05); hasta culminar en el Proyecto de Ley (CD- 109/06; S- 1751-1875 y 4417/06) y (Expediente 5.864-D.-2006), que dio origen a la presente ley.

Sin alejarnos de un Modelo Político Criminal Reductor del poder punitivo, y compartiendo que la reforma debía instrumentarse desde una ley integral, armónica y concordada en su articulado con el Código Penal, sin caer en la sanción de una Ley Complementaria de "Delitos Informáticos", es menester formular una crítica desde la óptica del Principio de Legalidad.

Entendiendo a la criminalidad informática como un medio comisivo para la realización de los tipos penales ya comprendidos y contemplados por el articulado del Código Penal, puede afirmarse y aseverarse que esta ley no ha previsto todos los tipos penales que pueden materializarse mediante el empleo de las nuevas tecnologías y puntualmente a través de la informática.

Así es que no ha contemplado y ni previsto los siguientes tipos penales que pueden instrumentarse y materializarse a través de la informática como medio comisivo: 1) Hurto (artículo 162 C.P.) (46); 2) Delitos contra la Propiedad Intelectual (artículo 72 ter Ley 11.723) (47); 3) Delitos que comprometen la Paz y la Dignidad de la Nación. (artículos 222 y 225 C.P.) (48); 4) Régimen Penal Cambiario (artículo 1, Ley 19.359 C.P.) (49); 5) Régimen Penal Tributario (Artículo 12, Ley 24.769 C.P.) (50); 6) Derecho Penal Aduanero (51); 7) Ilícitos Bancarios (52); 8) Lavado de Dinero; 9) Crimen Organizado (53); 10) Estrago; 11) Espionaje.

El hecho de no considerar la posible comisión de estos tipos penales puede traer aparejado, la atipicidad de estas conductas cuando fueran perpetradas bajo la modalidad de la criminalidad informática, ya que, por principio de especialidad, no podrían ser subsumidas bajo estos tipos penales.

Salvo por esta crítica en cuanto a la completitud y alcance limitado de esta reforma, puede decirse que la Ley 26.388 fue, en términos generales, cuidadosa en los conceptos y definiciones empleadas, con excepción de ciertos temas puntuales que han sido tratados expresamente al momento del análisis de los tipos penales en particular en la segunda etapa de estudio.

Por otra parte, la ley no presenta el empleo de tipos penales culposos a excepción del tipo penal de destrucción de prueba, con lo cual respeta la tradición jurídico-normativa de nuestra legislación en cuanto a mantener a los tipos culposos como "Numerus Clausus".

En el mismo orden de ideas, la Ley 26.388 de reforma en materia de criminalidad informática al Código Penal, no incorpora ningún tipo omisivo, ni doloso, ni culposo, lo cual debe destacarse en un Estado de Derecho y respetuoso del principio de reserva de los ciudadanos, ya que como es sabido, legislar mediante figuras omisivas acota y restringe en gran medida el ámbito de libertad de los habitantes, en particular porque desproveería de toda eficacia al principio de legalidad "Ningún habitante de la Nación, será obligado a hacer lo

que no manda la ley, ni privado de lo que ella no prohíbe".

(1) Los expedientes legislativos que se han considerado para la presente reforma son los siguientes: Los expedientes CD-109/06 - Proyecto de ley en revisión por el cual se incorporan las nuevas tecnologías como medios de comisión de distintos tipos previstos en el Código Penal; S-1751/06 - Proyecto de ley de los senadores Giustiniani e Ibarra, modificando diversos artículos del Código Penal en relación al uso privado del correo electrónico; S-1875/06 - Proyecto de ley del senador Saadi, incorporando a la legislación argentina la regulación del correo electrónico o e-mail y modificando las penas establecidas para la comisión de delitos tipificados en los artículos 153, 154, 155, 156, 157 y 157 bis del Código Penal; S-4417/06 - Proyecto de ley de la senadora Bortolozzi, estableciendo penas para los delitos electrónicos y tecnológicos; y teniendo a la vista los expedientes S-1281/06 - Proyecto de ley del senador Pichetto, modificando el art. 128 del Código Penal acerca de la protección de los niños en Internet; S -1628/06 - Proyecto de ley del senador Jenefes y otros senadores, sobre regulación y protección jurídica del correo electrónico; S-2127/06 - Proyecto de ley de la senadora Fellner, modificando el art.128 del Código Penal, respecto de establecer las penas pornografía infantil; S-2218/06 - Proyecto de ley del senador Jenefes, modificando el art. 128 del Código Penal, en lo que respecta a la pornografía infantil; S-3373/06 - Proyecto de ley del senador Saadi, sustituyendo el art. 128 del Código Penal a fin de establecer las penas por el delito de pornografía infantil; S-323/07 - Proyecto de ley del senador Basualdo y otros senadores, modificando el art. 128 del Código Penal, respecto a la pornografía infantil; S-465/07 – Proyecto de ley de la senadora Escudero, reproduciendo el proyecto de ley sobre modificación del art. 128 del Código Penal fijando las penas por la difusión de la pornografía infantil (Ref.: S-1610/05); S-520/07 -Proyecto de ley del senador Jenefes, modificando el Código Penal respecto a las penas por delitos informáticos; S-809/07 - Proyecto de ley de la senadora Giusti, modificando el Código Penal, respecto a las penas por pornografía infantil; S-823/07 - Proyecto de ley de la senadora Giusti, modificando el Código Penal respecto a las penas por violación de correo electrónico; S-2021/07 - Proyecto de ley de la senadora Bortolozzi, sobre tipificación de delitos cometidos por medios electrónicos e informáticos; S-2575/07 - Proyecto de ley de la senadora Viudes, modificando diversos aspectos del Código Penal, en relación a los delitos contra la privacidad. Conforme surge de la Orden del Día N° 959, de las Sesiones Ordinarias del día 16 de Noviembre de 2007, de la Cámara de Senadores del Congreso de la Nación de la República Argentina.

(2) Ver versión taquigráfica de la 5 ° Sesión Ordinaria de tablas, 13° reunión, Orden del Día N° 172, del Honorable Congreso de la Nación de la República Argentina, de fecha 4 de junio de 2008, a la hora 16:34, Pág 8.

(3) Ver Boletín Oficial de la República Argentina, Buenos Aires, miércoles 25 de junio de 2008, Año CXVI, Número 31.433. Ley 26.388, Código Penal de la Nación, Sancionada el 4 de junio de 2008, Promulgada el 24 de junio de 2008 y Publicada el 25 de junio de 2008.

(4) Artículo 6: "Documento digital. 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".

(5) Enciclopedia Jurídica Omeba (versión digital), voz "intimidad (derecho a la)", tema desarrollado por el Dr. Mateo Goudstein.

(6) En el mismo sentido: BADENI, Gregorio, "Tratado de Derecho Constitucional", Tomo I, La Ley, Pág 564.

(7) Según informaciones periodísticas, habría sido determinante en la sanción de la ley 26.388 (Adla Bol 17/2008, p. 4) el intrusismo informático sufrido por actores sociales de importancia, entre otros: Ricardo Lorenzetti, Rául Zaffaroni, Carmen Argibay (ministros de la CSJN), Héctor Magnetto, Daniel Hadad, Bartolomé Mitre, Jorge Fontevecchia (directivos de de empresas de multimedios), Daniel Scioli, Hilda Duhalde, Aníbal Ibarra (representantes políticos). Así, en "La Nación" del 15/06/08, p. 17.

(8) LINARES QUINTANA, "Tratado de la Ciencia del Derecho Constitucional", Tomo IV, Plus Ultra, Buenos Aires, 1978, Pág. 622.

(9) Así es tratada esta etapa de la evolución humana por CASTELLS, Manuel, en su obra "La Era de la Información. La Sociedad Red", Volúmen 1, 1996. Alianza.

(10) Como ejemplo de esta tendencia, puede citarse la ley N° 25.873 que en su artículo 2° establece como obligación de los prestadores de servicios de telecomunicaciones el registro y sistematización de datos filiatorios, domiciliarios, y de tráfico de comunicaciones de clientes y usuarios, por el plazo de 10 años. Posteriormente, mediante el dictado del Decreto 1563/2004 —actualmente suspendido por el Decreto 357/2005— se estableció como órgano receptor de esta información a la Secretaría de Inteligencia de la Nación (SIDE), ampliándose el objeto de la registración y el monitoreo al contenido de las comunicaciones, exigiéndose, además, el acceso a la información en tiempo real.

(11) La Nación Revista, nota titulada "¿Hacia donde evolucionamos?", 9 de diciembre de 2007, p. 84.

(12) CHIARIGLIONE, Leonardo, "Contenido electrónico", publicado en la Revista Derecho de Alta Tecnología (DAT), Año XI, número 100, junio de 1999, página 19.

(13) Publicada en el Boletín Oficial el 23 de marzo de 1973, a través de sus artículo 2° establecía el monopolio de la correspondencia que para aquel entonces era un medio básico y casi único de comunicación en nuestro país.

(14) RIQUERT, Marcelo Alfredo, "Protección penal de la intimidad en el espacio virtual", Ediar, Buenos Aires, 2003, p. 116.

(15) En este sentido: CREUS, Carlos, "El miedo a la analogía y la creación de vacíos de punibilidad en la legislación penal (intercepción de comunicaciones telefónicas y apropiaciones de "e-mail"), JA, 1999-IV-869.

(16) NUÑEZ, Ricardo C., "Manual de Derecho Penal. Parte especial", 2° Ed. actualizada por Víctor F. Reinaldi, Marcos Lerner, Córdoba, 1999, Pág. 175.

(17) OSSORIO Y FLORIT, Manuel, "Código Penal de la República Argentina. Comentarios. Jurisprudencia. Doctrina. Legislación complementaria", Universidad, Buenos Aires, 1979, Pág. 237.

(18) En este sentido: OSSORIO Y FLORIT, Manuel: ob. cit., p. 237.

(19) Sobre el alcance de los términos "hacker" y "hacking": ROSENDE, Eduardo E., "El intrusismo informático. Reflexiones sobre su inclusión en el Código Penal", Suplemento La Ley de Penal y Procesal Penal, Mayo 2008, p. 20.

(20) CESARIO, Roberto, "Habeas Data. Ley 25.326", Universidad, Buenos Aires, 2001, Pág. 27.

(21) ABOSO, Gustavo Eduardo – ZAPATA, María Florencia, "Cibercriminalidad y Derecho Penal", Bdef, Buenos Aires, 2006, Pág. 145.

(22) PALAZZI, PABLO A., "Análisis del proyecto de ley de delitos informáticos aprobado por el Senado de la Nación en el año 2007", próximo a publicarse en la Revista de Derecho Penal y Procesal Penal, Lexis Nexis, Buenos Aires, publicado electrónicamente en www.delitosinformaticos.com.ar/blog

(23) In extenso, FILLIA, Leonardo César, MONTELEONE, Romina, NAGER, Horacio S., SUEIRO Carlos Christian. "Análisis integrado de la criminalidad informática", Prólogo Carlos Alberto Elbert, Fabián Di Plácido Editor, Buenos Aires, 2007, Págs 40/48.

(24) Al respecto no habremos de explayarnos ya que no se ha incluido el hurto en este proyecto como para invitarnos a la reflexión, sin perjuicio de recordar la conveniencia de una amplia concepción de cosa en el art. 2311 del C.C.

(25) Según definición del Diccionario de la Real Academia española en su 22ª. edición en página web http://buscon.rae.es/draeI/ consultada el 6 de julio de 2008.

(26) CARO, Rodrigo F. "El archivo almacenado en soporte informático como objeto del delito de daño, artículo 183 del Código Penal" en La Ley 2004-A, 1436.

(27) BROND, Leonardo – BRIGNANI, Sebastián, "Delitos Informáticos – panorama deslindante y criterio de demarcación" La Ley, 2004-C, 1250.

(28) De esta forma se introducen al análisis del tipo penal ESTRELLA, Alberto Oscar y LEMOS GODOY, Roberto, "Código Penal. Parte Especial. De los delitos en particular", Editorial Hammurabi, 1° edición, Buenos Aires, 2000, página 107.

(29) CNCrim. y Corr., sala 7ª, 01/11/2002, - González, Adriana B.

(30) Cámara Nacional de Casación Penal, Sala IV, 18-03-05, M.G.G.

(31) Ver www.rae.es

(32) Puede ser obtenida una copia en http://www.corteidh.or.cr/

(33) MARIN FRAGA, Facundo J. "Internet y Derecho Penal. ¿Es relevante para el Derecho Penal la interrupción de las comunicaciones que se realizan a través de Internet?", Publicado en la La Ley 2001, Tomo F, página 1336.

(34) En relación a la Escuela Positivista se recomienda ver ANITUA, Gabriel Ignacio, "Historias de los pensamientos criminológicos", prólogo de Eugenio Raúl Zaffaroni, Editores del Puerto, Buenos Aires, 2005; BARATTA, Alessandro, "Criminología Crítica y Crítica del Derecho Penal" introducción a la sociología jurídico-penal, editorial Siglo XXI, Buenos Aires, 2002; BUJAN, Javier Alejandro, "Elementos de Criminología en la Realidad Social" Editorial, Depalma, Buenos Aires, 1998; ELBERT, Carlos Alberto, "Manual básico de criminología", 4ta Edición, Editorial Eudeba, Buenos Aires, 2007; PAVARINI, Massimo, "Control y Dominación, Teorías Criminológicas Burguesas y Proyecto Hegemónico" Editorial Siglo XXI, Buenos Aires, 2002; TAYLOR, Ian, Walton Paul y YOUNG, Jock, "La Nueva Criminología, Contribución a una Teoría Social de la Conducta Desviada", Editorial, Amorrortu, Buenos Aires, 2001; GARCIA - PABLOS DE MOLINA, Antonio. "Criminología. Una introducción a sus fundamentos teóricos", Presentación. Prólogo y Estudio

Preliminar para Latinoamérica y el Perú a cargo de Miguel Pérez Arroyo, Editorial, Instituto Peruano de Criminología y Ciencias Penales, Editores Iuris Consulti, Lima – Perú, 2006.

(35) Ver CHIARAVALLOTI, Alicia y LEVENE, Ricardo (h), "Delitos informáticos. Segunda Parte", La Ley 1998-F, 976; FILLIA,, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO Carlos Christian, "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 117.

(36) Ver CHIARAVALLOTI, Alicia y LEVENE, Ricardo (h), "Delitos informáticos. Segunda Parte", La Ley 1998-F, 976; FILLIA,, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO Carlos Christian. "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 118.

(37) Ver CHIARAVALLOTI, Alicia y LEVENE Ricardo (h), "Delitos informáticos. Segunda Parte", La Ley 1998-F, 976; FILLIA,, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO Carlos Christian. "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 118.

(38) FILLIA,, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO, Carlos Christian, "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 119.

(39) ROSENDE, Eduardo E., "El intrusismo informático. Reflexiones sobre su inclusión en el Código Penal". Publicado en el Suplemento La Ley Penal y Procesal Penal, Editorial La Ley, Buenos Aires, Martes 27 de mayo de 2008, Pág 21.

(40) RIQUERT Marcelo Alfredo, "Informática y Derecho Penal Argentino", Editorial Ad- Hoc, Buenos Aires, 1999, Pág 57; FILLIA, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO Carlos Christian, "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 120.

(41) RIQUERT, Marcelo Alfredo, "Informática y Derecho Penal Argentino", Editorial Ad- Hoc, Buenos Aires, 1999, Pág 57; FILLIA, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO Carlos Christian, "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 120.

(42) RIQUERT, Marcelo Alfredo, "Informática y Derecho Penal Argentino", Editorial Ad- Hoc, Buenos Aires, 1999, Pág 57

(43) Ver nota publicada en el diario La Nación (online) del domingo 6 de julio de 2008. "Cyberbullying: la nueva forma de agredir".

(44) Ver BINDER, Alberto M., "Política Criminal de la formulación a la praxis" Editorial, Ad-Hoc, Buenos Aires, 1997, Pág 38.

(45) Ver SILVA SÁNCHEZ, Jesús María, "La expansión del Derecho Penal – Aspectos de la Política Criminal en las sociedades postindustriales", segunda edición, Editorial BdeF, Montevideo-Buenos Aires, 2006.

(46) Conforme los Proyectos de Ley de Carlos "Chacho" Alvarez (1996) y José A. Romero Feris (1996).

(47) Conforme el Proyecto de Ley de Leonor E. Tolomeo (1996).

(48) Conforme el Proyecto de Ley de Leonor E. Tolomeo (1996).

(49) Ver MILLE, Antonio, "Aspectos legales de la transferencia electrónica de fondos" Publica por la editorial La Ley 1989-D, Pág 1142; FILLIA, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO Carlos Christian. "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 77

(50) Ver FILLIA, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO Carlos Christian. "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 7779/81.

(51) Ver FILLIA, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO Carlos Christian, "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 81/83.

(52) Ver FILLIA, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO, Carlos Christian. "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 83/84.

(53) Ver FILLIA, Leonardo César – MONTELEONE, Romina – NAGER, Horacio S. – SUEIRO Carlos Christian. "Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007, Pág 85.