

Tema II: “Reforma del Código Penal. Proyectos en la República Argentina y en los países del Mercosur. Simetrías y Asimetrías en la legislación y proyectos de reforma”

Título de la ponencia: “Estado de la legislación contra la delincuencia informática en el MERCOSUR”

Autor: **Marcelo** **Alfredo** **Riquert**

Profesor de Derecho Penal 1, Parte General, Universidad Nacional de Mar del Plata y de Derecho Penal 2, Parte Especial, Universidad Atlántida Argentina

Domicilio: Diagonal Pueyrredón 2938, piso 7, Mar del Plata
Teléfono: 0223 4931407
E-mail: riquertm@hotmail.com

Sumario: 1. Introducción. 2. Modelos legislativos comparados para el tratamiento de la delincuencia informática. 3. Análisis comparativo entre los países miembros plenos del MERCOSUR. 4. Algunos problemas sin resolución clara. 5. El nuevo miembro pleno: Venezuela. 6. La cuestión en los países unidos por compromiso democrático al MERCOSUR. 7. Conclusiones.

1. Introducción

En ocasión de celebrarse el Iº Encuentro Argentino de Profesores de Derecho Penal (Santa Fe, 2001), convocados para reflexionar sobre “*El sistema penal ante las exigencias del presente*”, tuvimos la posibilidad de presentar una ponencia acerca de la necesidad de una actualización legislativa en el marco del análisis de las relaciones entre la informática y el delito^[1]. Sin perjuicio de adelantar que, cinco años después, los avances en el ámbito local han sido escasos, es decir que, de hecho, varias de las “deudas” indicadas en aquel trabajo están vigentes, este Encuentro es una oportunidad de volver sobre la cuestión desde una perspectiva más amplia: la necesidad de armonización legal en la región.

En función del acotado espacio que puede ocuparse ahora para ello, se evitarán reiteraciones de conceptos generales vertidos en la anterior, a la que remitimos. Sin perjuicio de ello, es insoslayable recordar que, habida cuenta de las posibilidades que brindan las nuevas tecnologías de la comunicación y la aparición en escena de un nuevo espacio, el virtual o ciberespacio, en materia de delincuencia, facilitando la afectación de bienes jurídicos a una distancia y con una velocidad hasta no hace tanto impensadas, resulta un lugar común la afirmación de estar en presencia de una problemática frente a la que el proceso de homogeneización legislativa y de cooperación en los ámbitos

sustantivos y adjetivos, es una necesidad ineludible si se quiere evitar la existencia de “paraísos” de impunidad.

Es importante destacar que, lejos de la pretensión de fomentar aún más el fenómeno de inflación legislativa penal (rasgo ciertamente negativo propio del llamado “derecho penal de la modernidad”, paradójica designación para lo que, más que avance, pudiera ser un lamentable retroceso, una regresión a los momentos menos pensantes de la historia del derecho penal), entendemos media una necesidad legítima de completar la tarea de actualización legislativa. Como afirma Möhrenschrager, algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales, pero el Derecho Penal tradicional presenta, al menos parcialmente, relevantes dificultades para aprehenderlos derivadas en buena medida de la prohibición jurídico-penal de analogía y, en ocasiones, son insuperables por vía jurisprudencial, por lo que urge adoptar medidas legislativas^[li].

Natural derivación de un medio globalizado, estas observaciones se reproducen en el derecho comparado cuando se enfocan momentos de desarrollo legislativo similares. En concreto, el diferente estado de la cuestión en los países que conforman el bloque regional en forma plena o asociada, permitiría que el aprovechamiento de la experiencia de unos y otros aportara para optimizar la tarea de armonización.

Sin perder de vista las dificultades adicionales del singular proceso de integración que importa el Mercado Común del Sur, frente al que pueden hallarse visiones diametralmente opuestas, es posible avanzar desde lo local hacia esta equiparación que, luego, deberá ser integrada con los otros bloques regionales. En cuanto al propio, en palabras del constitucionalista brasileño Paulo Napoleão Nogueira da Silva, el Mercosur es una realidad que propone ser mucho más que una simple área de libre comercio, intenta ser una unión aduanera, una verdadera confederación económica que incluye la posibilidad de llegar a adoptar una moneda única^[liii]. En perspectiva crítica, indica Gabriela Wurcel que, más allá del nombre oficial, se está lejos de ser un verdadero mercado común o una unión aduanera perfecta^[liv].

Como recuerda Oscar Hermida Uriarte, el Mercosur tiene origen en el Tratado de Asunción, celebrado el 26 de marzo de 1991 entre Argentina, Brasil, Paraguay y Uruguay, regulándose un período de transición o de construcción de una zona de libre comercio entre los cuatro países y de un arancel externo común en las relaciones del bloque con el resto del mundo. En la actualidad, se ha incorporado un quinto país como miembro pleno, a partir del Protocolo de adhesión de la República Bolivariana de Venezuela, que fuera signado en Caracas, el 4 de julio de 2006. Por el Protocolo de Ouro Preto del 17 de diciembre de 1994, se estableció su estructura institucional definitiva, constituyendo el Mercosur en una “zona de libre comercio”^[lv] a su interior con un arancel interregional del 0 %, salvo excepciones, y una “unión aduanera”^[lvi] hacia terceros países con un arancel externo común diferencial que oscila del 0 al 20 %, con excepciones^[lvii]. Según la citada Wurcel, la crisis que atravesó el bloque regional a fin del milenio pasado, llevó incluso a hablar de la conveniencia de poner todo el esfuerzo en la consolidación de, al menos, la zona de libre comercio, dejando un tanto de lado el perfeccionamiento de la unión aduanera^[lviii].

Adriana Dreyzin de Klor apunta que al optar los gobernantes del bloque por un mercado común, la estructura intergubernamental sobre la que se construye repercute

operativamente en todos los campos, no sólo el jurídico-estructural, siendo la mayor crítica la carencia de órganos legisferantes con competencia legítima para elaborar el Derecho que rige su destino, junto a la falta de una Corte de Justicia Permanente. La verificación de numerosos disensos entre los miembros ha ido instalando como idea con consenso el efectuar un viraje institucional que dote al esquema de una legitimidad democrática de la que carece^[ix]. El actual conflicto entre Argentina y Uruguay por el tema de las papeleras frente la provincia de Entre Ríos, es una muestra cabal de los problemas aludidos.

Desde el año 1992, con un plan inicial de cuatro encuentros, que comenzó cuando se realizó en Asunción, Paraguay, entre el 1 y el 4 de julio, el 1º Seminario Internacional sobre “*Regionalización del Derecho Penal en el Mercosur*”, con la participación de delegaciones de los cuatro países signatarios, conformadas por reconocidos profesores de la materia, se vienen realizando distintas actividades sobre el punto. En aquel encuentro los temas abordados fueron: 1) organización judicial; 2) los movimientos de reforma procesal penal y la protección de los Derechos Humanos; 3) procedimientos de cooperación en materia penal. El 2º Seminario fue en Maldonado, Uruguay, entre el 10 y el 13 de noviembre de 1993, mientras que el 3º se desarrolló en Porto Alegre, Brasil, del 27 al 29 de octubre de 1994, volviéndose a tratar cuestiones relacionadas a la cooperación internacional y temas relativos al Derecho Penal Económico. El 4º Seminario fue en Santa Fe, Argentina, del 26 al 29 de junio de 1996, donde se profundizaron temas vinculados a la delincuencia económica, como la protección penal de la competencia, el régimen penal de marcas, patentes y diseños industriales y el análisis comparativo de sistemas judiciales y de garantías procesales en el área^[x].

En agosto de 2004 fue inaugurado en Asunción el Tribunal Permanente del MERCOSUR, órgano encargado de dirimir los conflictos referentes a disputas comerciales entre los países miembros, integrado por cinco juristas, se trata de un cuerpo arbitral permanente nacido a propuesta de Argentina (febrero de 2002) que plasmara en el Protocolo de Olivos. Puede actuar como tribunal de única instancia entre los Estados parte o en doble instancia (una “ad-hoc” y otra como Tribunal Permanente de Revisión, en causas referentes a problemas de índole comercial)^[xi].

En cuanto a la estructura del MERCOSUR, es la siguiente:

I. Órganos decisorios:

a. Consejo del Mercado Común: órgano supremo, tiene la conducción política y la toma de decisiones. Lo conforman los 4 presidentes de los países miembro, más los 4 ministros de Relaciones Exteriores, los 4 ministros de Economía y los 4 presidentes de los Bancos Centrales.

b. Grupo Mercado Común: órgano ejecutivo. Lo integran 4 miembros titulares y 4 alternos por cada país.

c. Comisión de Comercio del MERCOSUR: vela por la aplicación de los instrumentos de política comercial. Lo integran 4 miembros titulares y 4 alternos por cada país.

II. Órganos de representación parlamentaria:

* Comisión Parlamentaria Conjunta: representa a los Parlamentos de los Estados-parte en MERCOSUR, procura la armonización de las legislaciones conforme requiera el proceso de integración.

III. Órganos consultivos:

* Foro Consultivo Económico-Social: hace recomendaciones al Grupo Mercado Común

IV. Órganos de apoyo:

* Secretaría del MERCOSUR (sede permanente en Montevideo): órgano de apoyo operativo, se ocupa de la prestación de servicios a los demás órganos del MERCOSUR.

Para ir cerrando esta sintética noticia, debe tenerse presente que hay un compromiso democrático entre MERCOSUR y las Repúblicas de Bolivia y Chile, plasmado en el Protocolo de Ushuaia del 24/7/98, que tuvo por antecedente directo la “Declaración Presidencial” y el “Protocolo de adhesión” firmados en San Luis, el 25/6/96. Asimismo hay un “Acuerdo sobre extradición entre los estados partes del MERCOSUR y la República de Bolivia y la República de Chile”. Existe, asimismo, un “Protocolo de asistencia jurídica mutua en asuntos penales del MERCOSUR”, un “Acuerdo sobre extradición entre los estados partes del MERCOSUR”^[xiii] y se ha avanzado a la fijación de un régimen de jubilación unificado^[xiiii].

2. Modelos legislativos comparados para el tratamiento de la delincuencia informática

En el plano del derecho comparado pueden observarse diversas formas de acercarse a la tipificación de las conductas disvaliosas vinculadas a las nuevas tecnologías de la información. Al momento de analizar la situación en la perspectiva del MERCOSUR, se verifica que todos los modelos referidos han encontrado eco aún cuando el universo de países que lo componen es pequeño, incluyendo uno que prácticamente no ha generado modificaciones legales (Uruguay). Puede hacerse esta sintética categorización de modelos:

1. Dictado de **Ley Especial**: Venezuela y Chile (fuera de MERCOSUR: Estados Unidos, Alemania)

2. Modificación del Código Penal:

2.1. Difuminada: Paraguay (fuera: España)

2.2. Concentrada en un capítulo especial: Bolivia (ídem.: Francia)

3. **Mixto** (anárquico, combina 1 y 2): Argentina y Brasil (ambos, además, tienen al momento de redactarse este trabajo proyectos de ley especial con media sanción de la Cámara de Diputados y, en el primer caso, un proyecto de Código Penal en discusión que llevaría la situación al rubro 2.1.)

No se trata aquí del planteo de las ventajas y desventajas que cada uno de estos modelos posee, sino simplemente de objetivar la disímil técnica utilizada y pasar en lo que sigue a exponer los contenidos normativos de interés vigentes en los distintos países, con algunas acotadas notas de análisis dogmático.

3. Análisis comparativo entre los países miembros plenos de MERCOSUR

Más que nada por una cuestión de familiaridad con el propio derecho, a partir de la enunciación de los tipos penales vigentes en Argentina se irá haciendo mención de las normas que guardan alguna correspondencia (no necesariamente identidad) de los restantes países ya citados.

3.1. La primera norma considerando las nuevas tecnologías de la información fue la Ley N° 24.766 (1997) de *“Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos”*. Introdujo la protección del secreto de las informaciones de personas físicas o jurídicas almacenadas en medios informáticos (bases de datos), penándose su ilegítima divulgación conforme las penalidades del Código Penal para el delito de violación de secretos (art. 156: multa de \$ 1.500 a \$ 90.000 e inhabilitación especial de seis meses a tres años). El art. 2° dice: *“La presente ley se aplicará a la información que conste en documentos, medios electrónicos o magnéticos, discos, ópticos, microfilmes, películas u otros elementos similares”*. La protección es sólo de la información contenida en bases de datos no estatales. Estableció la protección de la información secreta, confidencial, de la empresa y personas físicas.-

Esta ley fue sancionada para cumplir con el art. 39 del Acuerdo sobre los Derechos de la Propiedad Intelectual, suscripto por nuestro país y aprobado por Ley 24.425^[xiv]. Su art. 12 dice *“Quien incurriera en la infracción de lo dispuesto en la presente ley en materia de confidencialidad, quedará sujeto a la responsabilidad que correspondiera conforme con el Código Penal, y otras normas penales concordantes para la violación de secretos, sin perjuicio de la responsabilidad penal en que se incurra por la naturaleza del delito”*. Básicamente, las acciones típicas son: a) usar la información confidencial sin causa justificada o sin consentimiento de la persona que la guarda o de su usuario autorizado; b) revelar la información confidencial sin causa

justificada o sin consentimiento de la persona que la guarda o de su usuario autorizado^[xvi]. La pena prevista es de multa de \$ 1500 a \$ 90000 e inhabilitación especial de 6 meses a 3 años (cf. art. 156 CP).

El secreto de empresa en Paraguay tiene protección penal expresa, conforme el Código Penal de 1997 (entró en vigencia a fines de 1998), en el Cap. VII, “Hechos punibles contra el ámbito de la vida y la intimidad de la persona”, en el artículo 147 “Revelación de un secreto de carácter privado”, cuya parte pertinente reza: “1° *El que revelara un secreto ajeno: 1. llegado a su conocimiento en su actuación como, a) médico, dentista o farmacéutico; b) abogado, notario o escribano público, defensor en causas penales, auditor o asesor de Hacienda; c) ayudante profesional de los mencionados anteriormente o persona formándose con ellos en la profesión; o 2. respecto del cual le incumbe por ley o en base a una ley una obligación de guardar silencio, será castigado con pena privativa de libertad de hasta un año o con multa. ...3° Cuando el secreto sea de carácter industrial o empresarial, la pena privativa de libertad podrá ser aumentada hasta tres años. Será castigada también la tentativa*”.

3.2. En el orden cronológico argentino sigue la “*alteración dolosa de registros fiscales*” que también en 1997 introdujera la vigente Ley Penal Tributaria y Previsional Nro. 24.769 (art. 12). En dicha figura se hace concreta referencia al *registro o soporte informático* como objeto de protección en paridad con el tradicional registro o soporte documental, en este caso, cuando sea del fisco nacional^[xvii]. Dice: “*Será reprimido con prisión de dos a seis años, el que de cualquier modo sustrajere, suprimiere, ocultare, adulterare, modificare o inutilizare los registros o soportes documentales o informáticos del fisco nacional, relativos a las obligaciones tributarias o de recursos de la seguridad social, con el propósito de disimular la real situación fiscal de un obligado*”.

El bien jurídico protegido genérico del régimen es la hacienda pública nacional y los recursos de la seguridad social, manifestado en concreto en esta figura por vía de la intangibilidad de los registros o soportes informáticos del Fisco nacional que se encuentren ligados con obligaciones de aquella naturaleza (tributaria o de seguridad social). Es delito común, cualquiera puede ser su autor, aunque naturalmente es una conducta cuyo desarrollo es más fácil efectuar puertas adentro de la AFIP, por el empleado infiel (un “*insider*”^[xviii]).

Por su parte, con anterioridad Brasil se había ocupado de un tema vinculado, cual es el del programa para fraude fiscal. Por Ley 8137 (27/12/90), sobre “Crímenes contra el orden económico y las relaciones de consumo”, se define una nueva forma de uso ilícito del ordenador, que sería la acción de utilizar o divulgar programas de procesamiento de datos que permita al contribuyente poseer información contable diversa que es, por ley, proporcionada a la Hacienda Pública. Al decir de Rodrigues da Costa, es un programa de ordenador destinado a permitir un fraude fiscal^[xviii]. Tiene pena de detención de 6 meses a 2 años y multa.

3.3. La Ley N° 25.036 (1998) modificó la Ley de Propiedad Intelectual N° 11.723, brindando protección penal al *software*. Ello a partir de la inclusión de los programas de computación en sus arts. 1, 4, 9, 55 bis y 57, ampliando así los objetos de protección de las conductas que ya se tipificaban en los términos de los arts. 71, 72 y ss. de esta última, los que no fueron a su vez adecuados en consonancia con aquellos^[xix]. Vale la pena recordar la amplitud del primero, que dice: “*Será reprimido con la pena establecida por el art. 172 del Código Penal el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta ley*”. La escala penal conminada en abstracto, por integración, es de un mes a seis años de prisión.

Se puso así fin al debate jurisprudencial que culminó con el fallo de nuestro máximo tribunal en causa “Autodesk”^[xx]. Se otorgó con la reforma la debida certeza jurídica en la materia, permitiendo actuar en modo más adecuado la función preventivo general del derecho penal.

En la reciente ley 25.922 (2004), se define al “*software*” como “*la expresión organizada de un conjunto de órdenes o instrucciones en cualquier lenguaje de alto nivel, de nivel intermedio, de ensamblaje o de máquina, organizadas en estructuras de diversas secuencias y combinaciones, almacenadas en medio magnético, óptico, eléctrico, discos, chips, circuitos o cualquier otro que resulte apropiado o que se desarrolle en el futuro, previsto para que una computadora o cualquier máquina con capacidad de procesamiento de información ejecute una función específica, disponiendo o no de datos, directa o indirectamente*” (art. 5°). Ello fijaría al presente el alcance del concepto normativo referido.

La tasa de piratería en Argentina el año anterior a la reforma (1997) fue del 65 %, mientras que en los índices del año 2000, había bajado al 58 %, lo que significó pérdidas para el sector del orden de los 114 millones de dólares^[xxi]. A esa fecha, el índice en Brasil era del 56 %, con pérdidas estimadas en 325 millones de dólares. La tasa promedio de piratería mundial en el año 2003 fue del 36 %, lo que habría importado una pérdida para la industria de 29.000 millones de dólares, según informa B.S.A. en su reporte de junio de 2004^[xxii]. La piratería en general para toda Latinoamérica en el año 2001 fue del 57%, pero en ese período en Argentina creció 4%, llegando al 62%. En estos porcentuales se incluyen bajo la denominación “piratería” los siguientes supuestos: copia o robo dentro de empresas y/o entre usuarios, falsificación de productos, preinstalación en discos rígidos de copias ilegales y alquiler de software. Aún cuando se observa entonces este retroceso (que entiendo puede en gran parte atribuirse a las graves dificultades económicas verificadas en el período considerado), no debe soslayarse que la reforma legal, aunque defectuosa (por ej., para aprehender la conducta de borrado de programas), ha servido de útil plataforma al sector particularmente interesado para obtener una disminución en la actividad ilícita aludida (al momento de verificarse una intensa polémica jurisprudencial en torno al problema de la protección penal del software, previo a su sanción, rondaba entre el 68 y el 70%).

El Estado ha tomado (en setiembre de 2004), medidas que pueden adquirir relevante trascendencia no sólo en forma directa en el impulso de la industria, reactivándola, sino que, por vía indirecta, pueden tenerla también en el ámbito que ahora se comenta, ya que el desarrollo de un fuerte polo tecnológico en materia de software de factura local incidiría sustancialmente en la posibilidad de adquirir productos locales a un precio razonable, desalentando de esa forma la piratería. La más

trascendente de las iniciativas es la sanción de la ya citada “*Ley de Promoción de la Industria del Software*” bajo el N° 25.922.

Pasando ahora a Brasil, la Ley 7646 (del 18/12/87), considera al software un derecho autoral. Se consagra un tipo delictivo específico, el art. 35: *Violar derechos de autor de programas de ordenador*: Pena: Detención, 6 (seis) meses a 2 (dos) años y multa. Hay otra norma, el art. 37 (*Importar, exportar, mantener en depósito, para fines de comercialización, programas de ordenador de origen extranjero no registrados*: Pena: Detención, de 1 (un) año a 4 (cuatro) años y multa), que consagró el delito de “contrabando de software no registrado”, pero es actualmente inoperativo según informa Rodrigues da Costa, ya que se dejó sin efecto la obligación de registración ante el Ministerio de Industria y Comercio^[xxiii].

En cuanto a Uruguay, en materia de protección penal del software, el proceso parece haber estado teñido por las mismas pinceladas del argentino, partiendo de una inicial aplicación en la primera instancia judicial de una interpretación extensiva de los tipos de la vieja ley de propiedad intelectual. En efecto, por sentencia de primer grado N° 65, fechada en Montevideo el 20 de noviembre de 1997, el Juez Peduzzi Duhau, en causa individualizada “*G. M., H. D. - Edición, Venta y/o Reproducción Ilícita de una obra literaria (Art. 46 Ley 9.739 del 17.12.37*”, ficha S 070/94, condenó a H.D.G.M. como autor responsable del delito de reproducción ilícita de una obra literaria a la pena de ocho meses de prisión^[xxiv].

Al comentarla, María José Vega sostiene que la importancia de esta sentencia radica en ser la primera en su país en materia penal por piratería de software, la cual fue dictada en un expediente que se inició en 1992 y en el cual se había dictado el primer procesamiento con prisión por violación al art. 46 de la ley 9.739. Al analizar los aspectos jurídicos de la cuestión, recuerda que el derecho de autor está reconocido por la Constitución uruguaya, cuyo art. 33 dice que el trabajo intelectual, el derecho del autor, del investigador o del artista deben ser reconocidos y amparados por la ley. Y ese artículo se ha cumplido con la sanción de la ley de propiedad intelectual, literaria y artística N° 9739 del año 1937. Algunos autores y, concretamente, el fallo indicado consideran al software incluido dentro de la protección de esta ley, que si bien enumera extensamente las obras que pueden ser alcanzadas, al final incluye a “*toda producción del dominio de la inteligencia*” (art. 5 inc. final). Si se entiende que el software es una producción del dominio de la inteligencia, estaría incluido en este artículo de la ley^[xxv].

Vega se aparta, creemos que con razón, de esta conclusión en la inteligencia que puede ser admitida en derecho civil pero no ocurre lo mismo en derecho penal donde priman los principios de legalidad y seguridad jurídica, por lo que concluye diciendo: “*Creo que la aplicación de la ley 9.739 implica una clara violación al principio de legalidad, que estamos haciendo una interpretación analógica, y la analogía en materia penal está absolutamente prohibida, salvo que sea a favor del justiciable, es decir, que beneficie al individuo (analogía in bonam parte)*”.

Resaltando la similitud de situaciones referida, expone la citada, debe tenerse en cuenta que el art. 46 de la ley 9.739 uruguaya es casi idéntico al art. 72 de la ley 11.723 argentina, respondiendo ambos textos a un mismo momento histórico (mediados de la década del '30)^[xxvi] y que, además, en Uruguay se pretendió incluir al software dentro del Derecho de Autor a través del decreto 154/89 que permite su inscripción en el

Registro de la Biblioteca Nacional, al igual que en Argentina se lo intentó por el decreto 165/94. Respecto de esto último, mientras el Juez uruguayo cita como fundamento de la sentencia la ley 9729 y sus modificativas, la C.N.Cas.Penal argentina en causa “Autodesk” dijo que es inadmisibles entender que el decreto viniera a definir conductas que antes se hallaban penalmente reprimidas y que el Poder Ejecutivo no puede, por vía reglamentaria, conferir protección penal a obras no incluidas en el texto de la ley 11.723.

Finalmente, en Paraguay rige el art. 184 del C.P. (1997), en función de la Ley 1328/1998 “De Derecho de Autor y Derechos Conexos”^[xxviii], cuyo texto dice: “*Artículo 184.- Violación del derecho de autor o inventor. 1º El que sin autorización del titular: 1. divulgara, promocionara, reprodujera o públicamente representara una obra de literatura, ciencia o arte, protegida por el derecho de autor; o 2. exhibiera públicamente el original o una copia de una obra de las artes plásticas o visuales, protegida por el derecho de autor, será castigado con pena privativa de libertad de hasta tres años o con multa.- 2º A las obras señaladas en el inciso anterior se equipararán los arreglos y otras adaptaciones protegidas por el derecho de autor.- 3º Con la misma pena será castigado el que falsificara, imitara o, sin autorización del titular: 1. promocionara una marca, un dibujo o un modelo industrial o un modelo de utilidad, protegidos; o 2. utilizara una invención protegida por patente.- 4º La persecución penal del hecho dependerá de la instancia de la víctima.- 5º En caso de condena a una pena se aplicará, a petición de la víctima o del ministerio público, lo dispuesto en el artículo 60”.*

3.4. La Ley N° 25.286 (2000) de Protección de Datos Personales (reglamentaria del proceso constitucional de Hábeas Data, art. 43 C.N.), incorporó al Código Penal de dos nuevos tipos, el 117bis dentro del Título II correspondiente a los “*Delitos contra el Honor*” y el art. 157bis en el capítulo III de la “*Violación de secretos*” del Título V “*Delitos contra la Libertad*”. En el Anteproyecto de Código Penal actualmente sometido a discusión, ambos tipos se funden en el art. 146, respecto del que podrían entonces reproducirse virtudes y defectos de las figuras que analizaremos por separado conforme derecho vigente.

3.4.1. Falsedad en archivos de datos personales y suministro de información falsa.

El art. 117bis dice: “*1º. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales. 2º. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales. 3º. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona. 4º. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena”.*

Ha recibido fundada crítica a raíz de que conforme su ubicación (delitos contra el honor) y descripción típica se pena el insertar o hacer insertar datos falsos aún cuando

nadie se perjudique (ya que el inc. 3º considera a esta situación como agravante, lo que importaría que el inc. 1º resultara una figura de peligro abstracto^[xxviii]) y, además, de cara al bien jurídico protegido (honor, en su vertiente objetiva) podría darse el caso que el dato falso no lo lesione ni lo ponga en peligro, incluso lo contrario, es decir, el dato falso mejore su crédito o fama. Bien señala Bertoni que si tomamos el bien jurídico protegido del título en su sentido tradicional la nueva figura se ha de limitar sólo a la inserción de datos falsos que disminuyan el honor o, caso contrario, habrá que reelaborar la interpretación del título por dejar de ser el honor el único bien jurídico tutelado por el ingreso de otros vinculados con el derecho a la información^[xxix]. En este contexto reductor de los alcances de la tipicidad, el primer párrafo resulta una figura de peligro concreto, ya que el insertar o hacer insertar el dato falso en un archivo de datos personales en forma que disminuya el honor del titular del registro falseado, torna cierta la posibilidad de afectar el bien jurídico tutelado por cualquiera que consulte el archivo.

En esta dirección, recuerda Villada que conforme el art. 1º de la Ley 25.326, sus disposiciones pretenden garantizar: a) *el derecho al honor e intimidad de las personas*, tutela de carácter “*subjetivo*” dirigida a la persona humana cuyos datos están integrados en archivos o bancos de datos, sean públicos o privados; b) *el acceso a la información correcta que sobre las mismas se registre*, protección “*objetiva*”, ya que está encaminada a proteger a los terceros y su confianza en la información que se les proporciona cuando requieren datos, pero que también tiene carácter “*subjetivo*” si se la enfoca desde el punto de vista de los sujetos que extraen la información y respecto a la persona de quien se requieren los datos para que la falsedad no le resulte perjudicial.

Con acierto indica el nombrado que este *falseamiento de datos* genéricamente afecta la fe pública (porque consta en los registros públicos o privados de una persona), ya que los datos están destinados a darse cuando son requeridos debidamente. Más que la intimidad y la honra de la persona, se protegen sus intereses, que pueden verse perjudicados con la provisión de un dato falso, que ha sido maliciosamente insertado en los archivos^[xxx].

La conducta descrita en el segundo párrafo, cuyo alcance debe guiarse por los cartabones de racionalidad que impone la crítica ya efectuada con relación al primero, puede cometerse tanto por medios informatizados como por cualquier otro medio. Como el verbo típico es proporcionar, se trata de un delito de acción. Conuerdo con Villada en que, en principio, no exige como resultado que el tercero sepa, lea, se entere o utilice el dato falso o crea en él, pudiendo además la falsa información referirse a cualquier aspecto de la persona titular del archivo de datos^[xxxi], pero insisto no puede soslayarse las limitaciones que, al igual que el supuesto anterior, imponen los principios de lesividad, racionalidad y mínima intervención.

Por su parte, concluye Ledesma con relación al 1º párrafo que el delito es formal o de pura actividad, puesto que se consuma con el solo hecho de insertar o hacer insertar, sin necesidad de la divulgación de los datos ni de que se cause perjuicio, real o potencial, siendo que el perjuicio efectivo está contemplado como agravante en el inc. 3º. Sostiene que, no obstante su carácter formal, es posible la tentativa y también cualquier forma de participación^[xxxii].

Pasando a Brasil, con mayor amplitud, se ha legislado un tipo de inserción de datos falsos y modificación o alteración no autorizada de sistemas informáticos. Ello

así, por Ley 9983 (del 14/07/00), que modificó los arts. 313 A y B del Código Penal. En la redacción vigente, según el art. 313-A: *“Inserción de datos falsos en sistema informático”*, se prevé pena de reclusión de 2 a 12 años y multa, para el funcionario público que inserte datos falsos en sistemas informáticos, mientras que el art. 313-B *“Modificación o alteración no autorizada de sistema informático”*, conmina con pena de detención de 3 meses a 2 años y multa, para el que modifica o altera un sistema de información o programa informático sin autorización o solicitud de autoridad competente; prevé como calificante la producción de daño a la administración pública o a un administrado, incremento de pena de un tercio a la mitad.

A su vez, en Paraguay, el Código Penal de 1997, con previsiones más cercanas a las de Brasil (a las que preceden) que a las argentinas, al regular los delitos patrimoniales incorporó un tipo de alteración de datos (art. 174) y otro de sabotaje de computadoras (art. 175). Su texto es el siguiente: *“Artículo 174.- Alteración de datos. 1º El que lesionando el derecho de disposición de otro sobre datos los borrara, suprimiera, inutilizara o cambiara, será castigado con pena privativa de libertad de hasta dos años o con multa. 2º En estos casos, será castigada también la tentativa. 3º Como datos, en el sentido del inciso 1º, se entenderán sólo aquellos que sean almacenados o se transmitan electrónicamente o magnéticamente, o en otra forma no inmediatamente visible”*; y *“Artículo 175.- Sabotaje de computadoras. 1º El que obstaculizara un procesamiento de datos de importancia vital para una empresa o establecimiento ajenos, o una entidad de la administración pública mediante: 1. un hecho punible según el artículo 174, inciso 1º; o 2. la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra parte accesorias vital, será castigado con pena privativa de libertad de hasta 5 años o con multa. 2º En estos casos, será castigada también la tentativa”*. En la “Exposición de Motivos” del propio Código, al referirse a la inclusión de los tipos transcritos se señala que: *“Dada la creciente importancia que tienen la transmisión de datos y las computadoras en la vida cotidiana y en los negocios que se llevan a cabo en la sociedad, y tomando en cuenta el valor patrimonial que actualmente tiene toda información, es menester que el nuevo código penal posea entre sus previsiones, las herramientas eficaces que permitan la sanción de quienes alteraren datos o sabotearan computadoras, ya sea alterando o borrando la información, así como la destrucción de unidades de almacenamiento (discos duros, diskettes, cd rom), o partes accesorias vitales (tarjetas u otro componente del hardware) que imposibiliten el procesamiento de estas informaciones”*.

3.4.2. Acceso ilegítimo a banco de datos personales y revelación de información registrada secreta.

El art. 157 bis dice: *“Será reprimido con la pena de prisión de un mes a dos años el que: 1º. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos accediere, de cualquier forma, a un banco de datos personales; 2º. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviera obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años”*

En este caso no se observan en principio objeciones en cuanto a su ubicación sistemática, ya que las conductas tipificadas en la nueva figura se relacionan directamente con la violación de secretos en general. Como enseñaba el maestro Núñez, el bien jurídico protegido en este capítulo del Código Penal es la incolumidad de: a) la intimidad de la correspondencia y de los papeles privados y, b) los secretos y la libre comunicación entre las personas^[xxxiii]. Ahora se incluye: c) la información que se hallare registrada en un banco de datos personales, que se conecta con el primer aspecto (intimidad) en el inciso 1º del art. 157 bis y el segundo (secreto) en el inc. 2º^[xxxiv], tratándose desde el punto de vista del autor de un delito común que prevé como agravante la autoría por funcionario público. Con relación al inciso primero, la acción típica de acceder puede concretarse por cualquier medio ya que no se especifica modalidad de ingreso alguna, aunque el contexto de la reforma es claro en cuanto a que el legislador quiso referirse a los medios informáticos^[xxxv]. La señalización de ilegitimidad del acceso importa la falta de consentimiento, lógicamente, de contar con este no estaríamos frente a una conducta punible. El inciso segundo exige que el autor sea alguien obligado a preservar la información. En ambos casos son conductas independientes dolosas^[xxxvi]. La lesión al bien jurídico protegido se concreta con el mero acceso y la simple revelación, respectivamente^[xxxvii]. Resulta admisible la tentativa.

Ledesma, al referirse a la acción penal, entiende que al no haberse modificado el art. 73 del digesto sustantivo incluyendo al art. 157 bis entre las excepciones que contiene, debe entenderse que la acción para perseguir este delito es privada^[xxxviii], punto en el que le asistiría razón ya que la exclusión se refiere taxativamente a los arts. 154 y 157.

Finalmente, debe agregarse que la protección de datos personales ha venido a ser complementada en la órbita contravencional por medio de la disposición 1/2003^[xxxix] de la Dirección Nacional de Protección de Datos Personales (autoridad de contralor de la ley de Habeas Data).

Por su parte, en Brasil, mediante la ya citada Ley 9983 del año 2000, se introdujo un tipo de violación de secretos calificado por vía de la modificación de los arts. 153 y 325 del CPB. En efecto, el art. 153, parág. 1º, letra “A”, “Violación de secreto”, prevé pena de detención de 1 a 4 años y multa para el que divulgue, sin justa causa, informaciones secretas o reservadas, así definidas por ley, contenidas en sistemas informáticos o bancos de datos de la Administración Pública; mientras que el art. 325, parágs. I y 2, “Violación de secreto funcional”, prevé pena de detención de 6 meses a 2 años o multa, para el que permite o facilita, mediante atribución, provisión y préstamo de clave o cualquier otra forma, el acceso de persona no autorizada a sistemas informáticos o banco de datos de la Administración Pública; o se utilizare, indebidamente, de acceso restringido. Califica por daño a la Administración Pública o a otro, con pena de reclusión de 2 a 6 años y multa.

3.5. La Ley N° 25.506 de Firma Digital (2001)^[xli], además de fijar su propio régimen de sanciones (contravencional) en los arts. 40/46, ha incorporado un nuevo artículo al cierre de la Parte General del código sustantivo argentino, realizando así la equiparación de sus conceptos centrales a los fines del derecho penal. Este es el artículo

78 bis (cf. art. 51 de la Ley citada), que dice: “Los términos *firma* y *suscripción* comprenden la *firma digital*, la *creación de una firma digital* o *firmar digitalmente*. Los términos *documento*, *instrumento privado* y *certificado* comprenden el *documento digital firmado digitalmente*”.

Debe valorarse positivamente la reforma porque se despeja cualquier duda sobre el particular ya que, como destaca Orts Berenguer, es claro que las técnicas informáticas pueden ser un instrumento idóneo para cometer falsedades documentales, facilitando su modificación en alguna de sus partes o creando uno nuevo, para hacerlos discurrir por el tráfico jurídico^[xiii]. El decreto reglamentario 2628/2002, aunque incurriendo en alguna superposición con el articulado de la ley, incorpora un glosario de utilidad con conceptos un poco más sintéticos que los detallados en aquella, los que resultan imprescindibles para fijar la extensión de aquellas referencias.

Así, por “*firma electrónica*” se entiende el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para poder ser considerada “*firma digital*” (art. 5, Ley 25.506), mientras que esta a su vez es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control, susceptible de verificación para identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma (art. 2, Ley 25.506). De tal suerte, cuando un tipo penal integra en su tipo objetivo como elemento normativo “*firma*” —como los arts. 173 inc. 4º (delitos contra la propiedad: abuso de firma en blanco) y 289 del CP (delitos contra la fé pública), y 135 de la Ley 24.241 (delitos contra la libertad de elección de AFJP)—, o la acción de suscribir (“*suscripción*”) —art. 168 inc. 2º del CP (delitos contra la propiedad: suscripción de documento mediante violencia, intimidación o simulación de autoridad)—, queda claro que firma digital y firma electrónica no resultan ser sinónimos y que sólo la primera habrá de ser considerada a los fines de la tipicidad penal.

En cuanto a las otras voces de interés, el “*documento digital*” es la representación digital de actos o de hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo (art. 6, Ley 25.506, donde se indica que satisface el requerimiento de escritura), el “*certificado digital*” es un documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (art. 13, Ley 25.506), mientras que el “*certificador licenciado*” es la persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello otorgada por el ente licenciante (art. 17, Ley 25.506). La “*Autoridad de Aplicación*” es la Jefatura de Gabinete de Ministros (art. 29, Ley 25.506). Deben tenerse en cuenta, además, las limitaciones al campo de aplicación de la firma digital fijadas por el propio art. 4º de la Ley 25.506.

Como refiere Alejandro D. Frascetti, tanto la firma ológrafa como la digital tienen dos funciones fundamentales: servir como medio de expresión de la voluntad y determinar la autoría de quien realiza un determinado acto jurídico, buscando además la última garantizar la inalterabilidad del documento suscripto. Según se ha visto, por la ley 25.506 se estableció la posibilidad de utilizar la firma digital cuando el ordenamiento jurídico exige la ológrafa, fijando algunas excepciones, e indicando como

presunciones “iuris tantum” de su uso la autoría y la integridad del mensaje. Al respecto, indica el nombrado que la prueba en contrario de la presunción de autoría puede estar vinculada con la real autoría del mensaje, es decir, con la voluntad real del titular, aún cuando todos los datos del certificado digital sean verdaderos^[xliii].

En Uruguay, la falsificación de documento electrónico se introdujo por vía del art. 697 de la Ley 16.736 del 5/1/96 (Ley de Presupuesto). El inc. 2º de dicha norma reza: “*El que voluntariamente transmitiera un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos en los arts. 236 a 239 del Código Penal, según corresponda*”. Montano, luego de señalar los beneficios de esta ley en cuanto a cerrar la situación de vacío normativo, opina que la remisión de esta disposición a los artículos 236 a 239 del C.P. ubica a este documento informático dentro de la categoría de documento público porque los tres tipos penales refieren al documento público^[xliv]. A su vez, el decreto 65/998 sobre procedimiento administrativo electrónico introduce en su capítulo III los conceptos de firma electrónica (art. 18) y firma digital (art. 19), con una serie de penalidades en el cap. IV con remisión a los tipos penales antes citados^[xlv].

Por su lado, Paraguay ha dedicado en su reciente Código Penal dos artículos a los hechos punibles contra la prueba documental. Se trata de los artículos 248 y 249. Su texto es el siguiente: “*Artículo 248.- Alteración de datos relevantes para la prueba. 1º El que con la intención de inducir al error en las relaciones jurídicas, almacenara o adulterara datos en los términos del artículo 174, inciso 3º, relevantes para la prueba de tal manera que, en caso de percibirlos se presenten como un documento no auténtico, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2º En estos casos será castigada también la tentativa. 3º En lo pertinente se aplicará también lo dispuesto en el artículo 246, inciso 4º*” y “*Artículo 249.- Equiparación para el procesamiento de datos. La manipulación que perturbe un procesamiento de datos conforme al artículo 174, inciso 3º, será equiparada a la inducción al error en las relaciones jurídicas*”.

3.6. Por Ley 25.930^[xlvi] se incorporó como inciso del art. 173 del Código Penal, el siguiente: “*15) El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciese por medio de una operación automática*”. Se advierte de inicio el apartamiento a la propuesta que sobre la figura del “fraude informático” había elaborado el proyecto de ley de delitos informáticos que se elaborara en el ámbito de la Secretaría de Comunicaciones de la Nación (res. 476/01)^[xlvii].

La nueva previsión legal viene a dar respuesta, al menos parcial, a algunos de los casos que habitualmente fueran denunciados como de patente inseguridad jurídica (por su discutible encuadre típico entre diversas figuras) o de lisa y llana atipicidad. Así, señalamos oportunamente que en los casos de maniobras ilegales con cajeros automatizados, atendiendo a la falta de previsión expresa en la normativa punitiva argentina, podía decirse que seguíamos en la discusión sobre si configuraban el delito de estafa (art. 172 CP) o el de hurto (art. 162 CP), situación en otros países ya superada. Por ej., el C.P. español de 1995, que en el pto. 2 de su art. 248 considera reos de estafa

los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero. Es claro que no es exactamente lo mismo que ahora se ha incorporado a nuestro digesto punitivo, ya que la norma española parece ser de mayor amplitud (como el proyecto local antes mencionado), pero debe resaltarse que las maniobras urdidas mediante el uso de tarjetas de compra, crédito o débito, sean originales a las que se accediera en forma permanente o transitoria o copias gemelas por el doblado de la banda magnética, así como usando datos de ellas en forma no autorizada, son cada vez más frecuentes y la nueva norma viene a dar una respuesta satisfactoria a esta problemática^[xlvii].

El fenómeno del robo de identidad se ha ido expandiendo como una plaga asociada al crecimiento de la tecnología digital, indicando noticias periodísticas que según estadísticas de la Comisión Federal de Comercio de USA, sólo en ese país en los últimos cinco años los delitos con datos robados de cuentas bancarias y tarjetas de crédito afectaron a 27 millones de personas. Dicha Comisión sostiene que casi el 5 % de los adultos norteamericanos ha sido afectado cada año por este tipo de delitos, que ocupan el primer lugar en la lista de los que afectan a los consumidores, calculándose que el perjuicio a las empresas ronda los 50.000 millones de dólares y un 10 % de esa cifra a los consumidores. Gran repercusión se dio en junio de 2005 el descubrimiento de que el mes anterior un hacker había logrado ingresar en los sistemas de seguridad de las empresas Mastercard Internacional, Visa Internacional y American Express, apoderándose de los datos de 40 millones de clientes de esas tarjetas en el país citado^[xlviii]. El diario Washington Post proclamó que 2005 es el año de la filtración de datos, en el que por hechos como el referido podría llegar a 50 millones las víctimas de robo de datos. A su vez, el New York Times informó que los usuarios de tarjetas de crédito de Australia, Japón, China y otros países asiáticos fueron alertados de que sus cuentas corrían peligro si las usaban en transacciones con Estados Unidos o con empresas norteamericanas^[xlxi].

Este orden de situaciones viene impactando fuertemente en los costos empresarios, sólo en Argentina el negocio de protección de redes ha registrado un fuerte aumento en su demanda y se calcula que facturará un 15 % más durante 2005. El Centro de Investigación en Seguridad Informática (CISI), realizó un estudio según el cual el 43 % de las empresas ha reconocido haber tenido algún “incidente” en sus sistemas, lo que llevó a que el 63 % de las consultadas señalara que prevé una mayor inversión en la seguridad de sus sistemas de computación y almacenamiento de datos. Otro aspecto relevante es que alrededor del 15 % de las firmas encuestadas directamente no sabían si sus sistemas habían o no sido accedidos^[l].

En Paraguay, el nuevo Código Penal, en su capítulo dedicado a los delitos contra el patrimonio, ha introducido dos tipos específicos vinculados, uno de operaciones fraudulentas por computadora (art. 188) y otro de aprovechamiento clandestino de una prestación (art. 189). Su texto es el siguiente: “*Artículo 188.- Operaciones fraudulentas por computadora. 1º El que con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante: 1. programación falsa; 2. utilización de datos falsos o incompletos; 3. utilización indebida de datos; o 4. otras influencias indebidas sobre el procesamiento, y con ello, perjudicara el patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2º En estos casos, se aplicará también lo*

dispuesto en el artículo 187, incisos 2° al 4°”; y “Artículo 189.- Aprovechamiento clandestino de una prestación. 1° El que con la intención de evitar el pago de la prestación, clandestinamente: 1. se aprovechara del servicio de un aparato automático, de una red de telecomunicaciones destinada al público, o de un medio de transporte; o 2. accediera a un evento o a una instalación, será castigado con pena privativa de libertad de hasta un año o con multa, siempre que no estén previstas penas mayores en otro artículo. 2° En estos casos, será castigada también la tentativa. 3° En lo pertinente se aplicará lo dispuesto en los arts. 171 y 172”.

3.7. Normas vinculadas a la punición de la ciberpornografía infantil. El problema de la extensión del tráfico de material y producción de contenidos de pornografía vinculada a los menores se ha visto facilitado por las nuevas tecnologías de la información y reflejado, en los últimos tiempos, en el incremento de procedimientos judiciales internacionales sobre los que periódicamente dan cuenta diversos medios periodísticos. Es una actividad gravemente disvaliosa en la que la nota de globalización se ha acentuado justamente por la aparición de herramientas que permiten la configuración de verdaderas “redes” delictivas. Al igual que en los casos anteriores, a nivel regional el estado de la legislación vigente no es parejo.

Brasil cuenta con previsiones expresas (al igual que Venezuela, país que trataremos aparte). En efecto, la conducta está tipificada por Ley 10.764 (del 12/11/03), que modificó el art. 241 del Estatuto del Menor y del Adolescente (ECA, Estatuto da Criança e Adolescente, Ley 8069/90), ampliando el crimen de “*pornografía infantil*”. Pune la divulgación y publicación de fotos o imágenes con escenas de sexo explícito que involucren a menores o adolescentes, por Internet. Tiene pena de reclusión de 2 a 6 años y multa. No son alcanzadas las “simulaciones” de pornografía infantil (“*virtual*”, al decir de Erick Iriarte^[iii]).

En Argentina, si bien no hay norma específica, puede señalarse que el 128 del CP (cf. Ley 25087/99) pune al que “*producere o publicare imágenes pornográficas en que se exhibieran menores*” o “*organizare espectáculos en vivo con escenas pornográficas en que participaren menores*” de 18 años. También al que “*distribuyere imágenes pornográficas cuyas características externas hiciere manifiesto que en ellas se ha grabado o fotografiado la exhibición de menores*” de 18 años “al momento de la creación de la imagen”, y al que “*facilitare el acceso a espectáculos pornográficos o suministrar material pornográfico a menores*” de 14 años. Entendemos que la amplitud de las conductas descriptas permite aprehender sin mayor problema los casos en el que el medio utilizado fuere Internet, aún cuando no sea mencionado en forma expresa pues ningún otro lo ha sido^[iii]. Por otra parte, el alcance jurídico del concepto de pornografía infantil viene delineado por la Ley 25763^[iiii], cuyo art. 1° aprueba el “*Protocolo facultativo de la Convención sobre los derechos del niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía*” (Asamblea General de Naciones Unidas, sesión plenaria del 25 de mayo de 2000). El art. 2° inc. c) dice que “*por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales*”. Adviértase la inclusión expresa de las simulaciones de acto sexual explícito de un

menor en función de los problemas que pudiera generar conforme anterior explicación en nota al pie^[liv].

La CSJN, en la causa “*Embajada Alemana s/corrupción de menores de 13 años*”, fallo del 27/12/05^[lv], en una cuestión de competencia negativa donde se investigaba precisamente una presunta infracción al art. 128 del C.P., hechos a los que se llegó a partir de información proporcionada por dicha representación diplomática, privilegió para asignarla a la justicia nacional y no a la bonaerense, el avanzado estado de la investigación realizada por la División Informática de la Policía Federal, que había detectado comunidades cerradas de usuarios de Internet en las que se intercambiaba, distribuía o divulgaba imágenes de pornografía infantil.

En el caso de Uruguay, no tiene norma específica y el viejo art. 278 del C.P. pena la pornografía en general^[lvii]. Finalmente, Paraguay no tiene norma específica ni similar a las anteriores^[lviii]. A mediados de diciembre de 2005, luego de su aprobación parlamentaria, estaba a la espera de promulgación por el poder ejecutivo la ley de “Penalización de la utilización de niños y adolescentes en pornografía”, iniciativa que terminaba con la criticada laguna de derecho apuntada^[lviiii].

4. Algunos problemas sin resolución clara

Puede afirmarse, luego de haber realizado una rápida visión del estado normativo de la cuestión en la región, que sigue presentándose un núcleo polémico que asienta tal característica, básicamente, en la falta de previsiones que más allá de toda discusión aclaren y perfeccionen los alcances de distintas figuras típicas tradicionales, cuyo texto ofrece márgenes de duda al momento de analizar la tipicidad de algunas de las conductas que se concretan mediante el uso de estas nuevas tecnologías, están vinculadas a ellas o recaen sobre intangibles.

En Argentina, ejemplo de ello es la polémica alrededor del tipo de daño^[lix]. En efecto, algunos autores estiman que el art. 183 del C.P. al tipificar el daño a una cosa mueble, podría comprender algunas de las nuevas realidades. En este sentido, debe recordarse que nuestros tribunales consideran “*cosa*” a la electricidad, los pulsos telefónicos y las señales de televisión o de cable (arg. cf. art. 3211 C.C.). De allí derivaría una posibilidad de aprehender típicamente algunas de las actividades que desarrollan los llamados *crackers* y *cyberpunks* (vándalos). A efectos de superar naturales objeciones de analogía prohibida, se ha propuesto de lege ferenda como alternativas: a) La reforma de dicho artículo agregando *intangible* a la lista de elementos pasivos de daño (“...cosa mueble o inmueble o un animal o *intangible*...”), precisando a su vez en el art. 77 del mismo Código Penal que con este término se hace referencia a datos manejados en sistema informático e incluyendo en el listado de agravantes cuando el daño en el equipo influya decisivamente en lesiones o muerte a una persona (así, Pablo O. Palazzi y Fabián García^[lx]); b) dictar una nueva ley especial al respecto.

Jurisprudencialmente, en caso “*Pinamonti*”^[lxi], se concluyó: 1) el software es una obra intelectual en los términos de la Ley 11.723 (tema superado cf. L. 25.036); 2)

dicha ley no contempla como acción típica el borrado o destrucción de programas de computación dentro de su elenco de figuras penales (arts. 71/72, que no fueron modificados por la L. 25.036); 3) tal conducta tampoco es aprehendida por el delito de daño (183 C.P.), pues el concepto de cosa es aplicable al soporte (diskette o disco rígido) y no a su contenido (programas o datos almacenados en ellos).

En síntesis, el caso de quien se ve perjudicado por el borrado total o parcial de un programa contenido en diskettes (por ej., por la aproximación adrede de un potente imán), al carecer de previsión expresa, sigue brindando abiertas dos posibles respuestas al interrogante sobre si el art. 183 CP incluye a los programas de computación y datos almacenados en un soporte magnético: a) negativa, porque no existían al sancionarse el Código (1921); b) afirmativa, interpretando ampliamente el término “cosa”, como se hizo con la energía eléctrica, el pulso telefónico y la señal televisiva.

La última ofrece la ventaja de solucionar la “laguna de punibilidad” que denuncia el fallo citado, pero afirma un sector de la doctrina que vulnera la prohibición de analogía (Salt, Saez Capel). La Cámara distinguió el continente (soporte) como “cosa” en los términos del art. 183 del C.P., del contenido (software o datos almacenados) y como el primero no fue afectado, consideró la conducta atípica. En términos de valores la distinción es inversa: el software es lo principal y el soporte lo accesorio, tanto desde el punto de vista del interés y utilidad del usuario como en la estricta relación económica de costo de uno y de otro.-

Entiendo que hay otra posibilidad: no ya analizar el objeto sobre el cual recae la acción típica, sino considerar la afectación de la función de la cosa destruida como también la de su valor económico. Si la acción realizada afecta la función que cumple el objeto o su valor económico, se está produciendo un daño efectivo alcanzado por el 183 C.P. No es otra cosa que el criterio de *utilidad* para describir la acción típica de daño que brinda Creus^[lxiii]. La jurisprudencia ha sostenido que el delito de daño no exige que la cosa mueble o inmueble quede totalmente destruida o inutilizada, sino que basta que la restitución del bien a su estado anterior demande algún gasto, esfuerzo o trabajo^[lxiiii]. En este caso, el esfuerzo o gasto podría consistir en recuperar la información borrada, ya sea por vía de la previsión de haber realizado previamente un *backup*, volver a instalar los originales o tener que adquirir otros, respectivamente.-

El anteproyecto de Ley de Reforma y Actualización integral del Código Penal presentado públicamente en el mes de mayo pasado^[lxiv] y cuya discusión es uno de los temas que se aborda en este Encuentro, se ha ocupado de este problema en los arts. 187 y 188. El primero dice: “*Será reprimido con prisión de quince (15) días a un (1) año, el que por cualquier medio destruya en todo o en parte, borre, altere en forma temporal o permanente, o de cualquier manera impida la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo o durante un proceso de transmisión de datos. La misma pena se aplicará a quien venda, distribuya, o de cualquier manera haga circular o introduzca en un sistema informático, cualquier programa destinado a causar daños de los prescriptos en el párrafo anterior, en los datos o programas contenidos en una computadora, una base de datos o en cualquier tipo de sistema informático*”, mientras que el segundo califica la conducta “...f) *Cuando el daño se ejecute en sistemas informáticos o bases de datos públicos, o relacionados con la prestación de un servicio público*”.

Similar situación a la argentina se presenta en Brasil, donde la discusión gira alrededor del art. 163 del código penal de 1940. Tulio Vianna se cuenta entre los autores que propician una interpretación extensiva del tipo, considerando “cosa” a los “datos informáticos”^[lxvi]. El proyecto de ley N° 84 de 1999 del diputado Luiz Piauhyllino, aprobado en la Cámara de origen y con trámite en el Senado bajo N° 89/033, prevé la modificación de dicho tipo penal, incorporando la difusión de virus electrónico como daño electrónico^[lxvii].

En Paraguay, según ya se ha visto, el tipo del art. 174 “alteración de datos” parece sortear el problema y aprehender los casos sobre los que aquí se polemiza.

A modo de simple enunciación de otros problemas, en el ámbito local siguen abiertas a interpretaciones divergentes cuestiones como la protección o desprotección penal del correo electrónico, de la tipificación o no del registro impropio de nombres de dominio (ciberocupación) o del spamming (correo basura o publicidad no solicitada^[lxviii]).

En lo local, superando discusiones doctrinarias y jurisprudenciales, a la vez que dando a la “privacidad” como bien jurídico protegido una mayor protección, el tema de la protección penal del correo electrónico es también contemplado en el proyecto de Código Penal presentado en el año en curso (además de tener varios proyectos legislativos independientes en consideración). Los arts. 138, 139, 142 y 143 lo han incluido en su redacción del siguiente modo: art. 138 (figura básica), “...*el que abriere indebidamente una carta, un pliego cerrado o un despacho telegráfico, telefónico, mensaje de correo electrónico o de otra naturaleza que no le esté dirigido; o se apoderare indebidamente de una carta, de un pliego, de un mensaje de correo electrónico, de un despacho o de otro papel privado, aunque no esté cerrado; o suprimiere o desviare de su destino una correspondencia o mensaje de correo electrónico que le esté dirigida...*”, calificando la conducta “...*si el culpable comunicare a otro o publicare el contenido de la carta, escrito, mensaje de correo electrónico o despacho*”; a su vez, el art. 139 califica la acción para “...*el que por su oficio o profesión se apoderare de una carta, de un pliego, de un telegrama o de otra pieza de correspondencia o de un mensaje de correo electrónico.- También si se impusiere de su contenido, la entregare o comunicare a otro que sea el destinatario, la suprimiere, la ocultare o cambiare su texto...*”.

El citado art. 142 del proyecto dice: “...*el que indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro tipo de envío de objetos o trans-misión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuviesen dirigidos...*”, agravando si el autor fuere funcionario público o integrante de las fuerzas armadas o de seguridad; y el art. 143 pune “...*el que, hallándose en posesión de una correspondencia o mensaje de correo electrónico no destinado a la publicidad, lo hiciera publicar indebidamente, aunque haya sido dirigido a él, si el hecho causare o pudiere causar perjuicios a terceros*”.

Aunque no vinculado en forma estricta con la cuestión del correo electrónico, también lucen de interés en la temática que nos viene ocupando, algunas precisiones que formula el proyecto en materia de entorpecimiento de las comunicaciones. Así, pueden

destacarse los arts. 228 a 230. El primero dice lo siguiente: “...*el que interrumpiere o entorpeciere toda comunicación transmitida por cualquier medio alámbrico o inalámbrico, o resistiere violentamente el restablecimiento de la comunicación interrumpida*”. El art. 229: “...*el que alterar, reemplazar, duplicar o de cualquier modo modificar un número de línea, o de serie electrónico o mecánico de un equipo terminal o de un Módulo de Identificación Removible del usuario, de modo que resulte perjuicio al titular, usuario o terceros*”. El último contempla la punición para “...*el que alterar, reemplazar, duplicar o de cualquier modo modificar algún componente de alguna tarjeta de telefonía o acceder por cualquier medio a los códigos informáticos de habilitación de créditos de dicho servicio, a efectos de aprovecharse ilegítimamente del crédito emanado por un licenciario de Servicios de Comunicaciones Móviles*”.

Finalmente, con relación al mero intrusismo, puede decirse que tanto en Argentina, como en Brasil^[lxviii] y en Paraguay, aparece como una conducta atípica. En este último país, sería eventualmente discutible el ingreso de la conducta en el campo de punición como tentativa de infracción al art. 174 del C.P. Autores como Palazzi, critican que en el Anteproyecto de Código Penal en discusión en Argentina, el art. 146 mantiene la tipificación del acceso ilegítimo a un banco de datos (introducida por Ley 25.326), pero no a la conducta más amplia de acceso a un sistema informático, apuntando que en el año 2005 cerca de 50 países legislaron como delito el acceso no autorizado a sistemas informáticos^[lxix].

En Uruguay, si bien no hay un tipo específico^[lxx], se ha verificado una condena por esta conducta, que se subsumió bajo la figura del art. 300 del C.P.^[lxxi], que pena el “conocimiento fraudulento de secretos”. El hecho consistió en el ingreso no autorizado al sistema informático del Laboratorio Tecnológico del Uruguay (LATU)^[lxxii]. Hay un proyecto de ley presentado por el Dr. Pacheco Klein, en el que se tipifica tanto el acceso doloso (art. 1), como el acceso culposo (art. 2), es decir, tanto aquel cuya intención se ajusta al resultado de interceptar, interferir, recibir, usar, alterar, dañar o destruir el sistema, como aquel que lo concreta por no prever el resultado previsible, debido a su negligencia, imprudencia, impericia o por desobediencia a las leyes o reglamentos^[lxxiii]. En el ámbito de las propuestas, estima Figoli que por tratarse el intrusismo de una conducta que atenta contra la intimidad, debería darse un papel preponderante a la víctima, recordando que el Código español de 1995 prevé el perdón del intruso por parte del damnificado. Entiende que esto posibilitaría que el hacker pueda negociar una salida venturosa, reparando el daño ocasionado.

5. El nuevo miembro pleno: Venezuela

Según se adelantó, el nuevo integrante del bloque regional cuenta con una “Ley Especial Contra los Delitos Informáticos”, del 6 de noviembre de 2001. Si bien posee un articulado más extenso que el habitualmente observado en casos análogos, incluyendo su propia parte general, donde se adoptan o corrigen principios e institutos habitualmente regulados en el Código Penal, se le han realizado críticas por olvidos o exclusiones, además de las generales de “descodificación”, “repetición de delitos ya existentes” (aunque su último artículo declara la derogación de cualquier norma que

colide con su texto) o de “alterar principios de la parte general del C.P.”. Entre las primeras estaría la de no tipificar delito alguno relativo a la seguridad e integridad de la firma electrónica y su registro^[Lxxiv]. La estructura está dada en cuatro títulos, cuyas notas principales son las siguientes:

El Título I “Disposiciones Generales”, indica como objeto de la ley la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley (art. 1). Se incluye un glosario de definiciones (art. 2). En su art. 3 regula la extraterritorialidad, diciendo que cuando el delito se cometa fuera del territorio, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros. Hay un catálogo de sanciones principales y accesorias (art. 4) y en el art. 5 adopta expresamente la responsabilidad de las personas jurídicas.

El Título II “De los delitos”, se divide en cinco capítulos, el primero “De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información”, consagra estas figuras típicas: acceso indebido; sabotaje o daño a sistemas; sabotaje o daño culposos; acceso indebido o sabotaje a sistemas protegidos; posesión de equipos o prestación de servicios de sabotaje; espionaje informático y falsificación de documentos. El capítulo II “De los Delitos Contra la Propiedad”, las de hurto; fraude; obtención indebida de bienes o servicios; manejo fraudulento de tarjetas inteligentes o instrumentos análogos; apropiación de tarjetas inteligentes o instrumentos análogos; provisión indebida de bienes o servicios y la posesión de equipo para falsificaciones. El capítulo III “De los delitos contra la privacidad de las personas y de las comunicaciones”, contempla los delitos de violación de la privacidad de la data o información de carácter personal; violación de la privacidad de las comunicaciones y la revelación indebida de data o información de carácter personal. El capítulo IV “De los delitos contra niños, niñas o adolescentes”, pune la difusión o exhibición de material pornográfico y la exhibición pornográfica de niños o adolescentes. Finalmente, el capítulo V “De los delitos contra el orden económico”, prevé las figuras de apropiación de propiedad intelectual y oferta engañosa.

Los últimos dos títulos se dedican a las disposiciones comunes y disposiciones finales. Como se advierte de esta apretada síntesis de su contenido es un instrumento legal de considerable extensión del que, no obstante, Fernández predica que llena sólo parcialmente el vacío legislativo, en la inteligencia que será mejor una nueva tipificación sistemática y exhaustiva en el marco de un nuevo código penal^[Lxxv].

6. La cuestión en los países unidos por compromiso democrático al MERCOSUR

Cerrando el trabajo comparativo, se recuerda brevemente las disposiciones pertinentes de los países que se encuentran unidos por compromiso democrático con el bloque regional sudamericano: Chile y Bolivia.

En el caso chileno, debe destacarse que fue el primer país de la región que dictó una ley especial en la materia, la N° 19223 del 7 de junio de 1993. Se consagraron en ella cuatro tipos penales: 1) sabotaje informático: *“El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento”*, contemplando agravante *“Si como consecuencia de estas conductas se afectaren datos contenidos en un sistema”*; 2) espionaje informático: *“El que con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema tratamiento de la misma, lo intercepte, interfiera o acceda a él”*; 3) alteración de datos: *“El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información”*; y 4) revelación de datos: *“El que maliciosamente revele o difunda los datos contenidos en un sistema de información”*, con agravamiento *“Si quien incurre en estas conductas es el responsable del sistema de información”*. Como se ve, en cuanto al mero intrusismo, mencionado al final del acápite 4, no aparece como expresamente tipificado.

En el caso de Bolivia, su Código Penal del año 1997 incluyó en Título dedicado a los “Delitos contra la Propiedad”, el Cap. XI “Delitos Informáticos”. El art. 363bis, “Manipulación informática”, dice: *“El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero. Sanción: reclusión de 1 a 5 años y multa de 60 a 200 días”*; mientras que el art. 363ter, “Alteración, acceso y uso indebido de datos informáticos”, reza: *“El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando un perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa de hasta doscientos días”*.

7. Conclusiones

Más allá de la obligada limitación que impone la extensión de una ponencia, que impone la necesidad de pasar rápidamente en forma superficial sobre muchos aspectos en una temática ciertamente variada y compleja, se podrían formular las siguientes observaciones:

a) La protección penal respecto de la delincuencia informática en el ámbito del MERCOSUR presenta una serie de asimetrías entre los estados miembros con carácter pleno y, además, con aquéllos a los que hallan unidos por el compromiso institucional democrático.

b) Esto se visualiza desde lo formal, en el distinto modo en que se aproximaran a las necesarias actualizaciones legislativas y, desde lo material, en la diferente consideración de algunos problemas o la directa ignorancia de estos por algunos de los miembros. Desde ambas perspectivas, en función de lo apuntado, el proceso de armonización se presenta como una necesidad ineludible.

c) Tratándose de una experiencia de integración regional con aún pretensiones y objetivos limitados, estructuralmente se ve favorecida tal falta de armonía, no encontrándose previstas vías institucionales por el momento para canalizar el proceso de superación del problema, aspecto en el que comparativamente la Unión Europea presenta ventajas notables, sin que ello quite complejidad al asunto.

d) El presentado a discusión Proyecto de Código Penal Argentino en el año en curso, aporta en su articulado la solución a algunas de las lagunas de punibilidad en su oportunidad denunciadas en el derecho interno, significando a la vez un avance hacia la armonización legislativa en el materia con otros países del bloque regional que se han ocupado de esta problemática en un modo más integral.

Notas

al

pie:

^[i] Bajo el título “*Informática y delito: necesidad de una actualización legislativa*”, pub. en el libro del Iº Encuentro, “*El sistema penal ante las exigencias del presente*”, Rubinzal-Culzoni Editores/UNL, 2004, págs. 175/190.

^[ii] Manfred E. Möhrenschrager, “*Tendencias de política jurídica en la lucha contra la delincuencia relacionada con la informática*”, pub. en AAVV “*Delincuencia informática*”, S. Mir Puig compilador, PPU, Barcelona, 1992, pág. 47.

^[iii] Así lo afirma en su trabajo “*Ajuste jurídico do Mercosul*”, pub. en “*Revista de Derecho del Mercosur*”, ed. La Ley, Bs.As., Año 1, N° 2, setiembre de 1997, págs. 186.

^[iv] Comienza con esta afirmación su trabajo “*La política aduanera de la Unión Europea*”, pub. en “*Revista de Derecho del Mercosur*”, ed. La Ley, Bs.As., Año 4, N° 1, febrero de 2000, pág. 17.

^[v] Según recuerda Wurcel, cuando se crea una zona de libre comercio, los países quieren poner en común sus economías pero no integrarlas ni convertirlas en una única, su finalidad es la eliminación total o parcial de los derechos aduaneros y las restricciones al comercio entre ellos, pero como cada miembro de la zona mantiene en vigor su propio arancel aduanero y su política comercial, es necesario establecer normas para determinar qué mercaderías pueden circular libremente de un país a otro dentro de la zona, por lo que los procedimientos aduaneros deben mantenerse en las fronteras internas para comprobar el cumplimiento de esas reglas (ob.cit., pág. 17).

^[vi] A diferencia del caso anterior, la unión aduanera tiende a la integración económica eliminando las restricciones fronterizas internas. En ella, los miembros aplican un arancel aduanero y una política comercial común frente a las mercaderías de terceros países, así, no son necesarias normas para determinar qué mercaderías pueden circular libremente dentro de esa unión, ni tampoco normas de origen, por lo que son

innecesarias las fronteras a efectos aduaneros o de comercio exterior (cf. Wurcel, ya citada, pág. 17).

^[viii] Cf. su artículo titulado “*Institucionalidad Laboral del Mercosur*”, pub. en “Revista de Derecho del Mercosur”, ed. La Ley, Bs.As., Año 1, N° 2, setiembre de 1997, pág. 41.

^[viiii] Ya citada, pág. 17.

^[lix] En su trabajo “*El Parlamento para el Mercosur: parte de una reforma integral*”, pub. en “Revista de Derecho Privado y Comunitario”, Tomo 2004-3 “Asociaciones y fundaciones”, Rubinzal-Culzoni Editores, Santa Fe/Bs.As., pág. 582.

^[lx] Cf. João Marcello de Araujo Junior, en su trabajo “*A regionalização do direito penal no Mercosul (Contribuição para história jurídica do Mercosul)*”, pub. en “Revista de Derecho del Mercosur”, ed. La Ley, Bs.As., Año 1, N° 1, mayo de 1997, págs. 85/89.

^[lxi] Fuente: noticia del día 12 de agosto de 2004 en el medio virtual “DiarioJudicial.com”.

^[lxii] Un detalle mayor sobre la normativa de interés penal en el ámbito del MERCOSUR puede consultarse en la ponencia presentada por la Dra. Mónica L. Cuñarro, titulada “Armonización de la legislación penal en las leyes de emergencia: Narcotráfico y Crimen Organizado”, cuyo texto gentilmente me permitiera conocer antes de la realización del Encuentro.

^[lxiii] Esto último, más allá de la existencia previa de convenios bilaterales con Brasil y Uruguay. En síntesis, se considerarán en forma proporcional los aportes realizados en los distintos países y se hará efectiva la jubilación en el país de residencia del trabajador, incluyendo los restantes beneficios de seguridad social. Ello así en función del Acuerdo Multilateral de Seguridad Social del MERCOSUR, en vigencia desde el 1/6/05.

^[lxiv] Cf. señala Palazzi en su obra “*Delitos Informáticos*”, Ed. Ad-Hoc, Bs. As., 2000, p. 162.

^[lxv] Cf. Palazzi, “*Delitos...*”, p. 166.

^[lxvi] Al respecto, he analizado en extenso de este tipo penal en mi trabajo “*Cuestiones de Derecho Penal y Procesal Penal Tributario*”, EDIAR, Bs.As., 2° edición, 2004, págs. 139 y ss.

^[lxvii] La problemática de los *insiders* es común a toda estructura institucional o empresaria significativa. Se trata de quienes trabajan o se han desempeñado dentro de ellas y aprovechan el conocimiento que poseen sobre programas, claves, organización o, sencillamente, la facilidad de acceso irrestricto a la información de los sistemas (ccte.: Cristián Varela, “*Algunas aproximaciones a la conducta informática disvaliosa, el delito informático y la respuesta estatal*”, ponencia presentada en las “1as. Jornadas Latinoamericanas de Derecho Informático”, organizadas por la OMDI (Organización Mundial de Derecho e Informática), Mar del Plata, 06 al 08 de setiembre de 2001).

^[xviii] Marco Aurélio Rodrigues da Costa, “*El derecho penal informático vigente en Brasil*”, pub. en REDI “Revista Electrónica de Derecho Informático”, N° 13, Agosto de 1999, disponible en el portal jurídico “vLex.com”.

^[xix] Me he ocupado del tema en el capítulo VII de mi monografía “*Informática y Derecho Penal Argentino*”, Ad-Hoc, Bs.As., 1999.

^[xx] CSJN, fallo del 23/12/97. Puede consultarse en la obra citada en la nota anterior, págs. 178/183, así como el pronunciamiento recurrido de la Sala 1 de la CNCasPenal, del 19/7/95, págs. 162/175.

^[xxi] Fuente: Diario Judicial, 22/5/01, sección Noticias del día.

^[xxii] Fuente: página web de la asociación civil “*Software Legal*” (www.softwarelegal.org.ar), que indica que la campaña llevada adelante durante el año 2000 en nuestro país ofreciendo una tregua en las acciones judiciales, llevó a que más de 6.000 empresas regularizaran sus instalaciones de software, motivo determinante de la reducción de la tasa de piratería verificada.

^[xxiii] Trabajo ya citado. En opinión del nombrado, el art. 35 retrata con claridad la intención del legislador de proteger el derecho de autor, sin caracterizarlo como un delito informático.

^[xxiv] El fallo íntegro se encuentra publicado en el medio virtual “ALFA-REDI”, en la sección “Delitos Informáticos”, con comentario de María José Vega, bajo el título “Uruguay: La piratería de software ¿Es un delito?. Análisis de las respuestas dictadas en fallos de Uruguay y Argentina”. En el primer considerando se afirmó “*Que el ilícito de autos encuadra en la figura delictiva tipificada en el art. 56 del Código Penal y art. 46 de la ley 9.739 en la redacción dada por el art. 23 de la ley 15.913 (UN DELITO CONTINUADO DE REPRODUCCION ILICITA DE UNA OBRA LITERARIA). En efecto la conducta antijurídica del sujeto activo consistió con unidad de resolución criminal en un lapso que se sitúa entre enero y julio de 1992 en reproducir o hacer reproducir programas de computación, sin autorización escrita de sus titulares*”.

^[xxv] Vega, op.cit., punto 3.1. A favor de esta tesis, cita la opinión de Cairoli, quien descarta que se trate de una aplicación analógica, señalando que es simplemente una interpretación “extensiva”, que tiende a evitar que se caiga en lecturas de las palabras de la ley ilógicas o anacrónicas.

^[xxvi] El art. 72 de la Ley 11.723 dice: “*Incurrir en el comportamiento punible el que edite, venda o reproduzca por cualquier medio o instrumento una obra inédita o publicada sin autorización de su autor o derechohabiente*”. El art. 46 de la Ley 9.739 establece: “*El que edite, venda o reproduzca o hiciere reproducir por cualquier medio o instrumento, total o parcialmente, una obra inédita o publicada, sin autorización escrita de su autor o causahabiente, o de su adquirente a cualquier título*”.

^[xxvii] Cf. informa Rosa Elena Di Martino Ortiz en su trabajo “Protección jurídica del software en la Legislación Paraguaya”, pub. en REDI, N° 60, julio 2003.

^[lxxviii] Ccte.: Villada, Jorge Luis, en su obra “*Reformas al Código Penal Argentino*”, Nova Tesis Editorial Jurídica, Rosario, Santa Fe, 2001, pág. 279.

^[lxxix] Eduardo Andrés Bertoni, “*El bien jurídico tutelado en los delitos contra el honor: ¿sigue siendo el mismo aún después de la sanción de la Ley de “Habeas Data”?*”, pub. en L.L., Suplemento de Jurisprudencia Penal, 23/3/01, págs. 12/17. Cctes.: Villada, ya citado, pág. 277, donde señala que si la disposición hubiese dicho “*el que insertare o hiciere insertar a sabiendas, datos falsos injuriosos o calumniosos, en un archivo de datos personales*”, se entendería la inclusión en este título y capítulo, “*pero tal como está redactado, pueden anticiparse dolores de cabeza a jueces que apliquen el art. 117 bis y a la doctrina sería que lo comente*”; Ledesma, ya citado, pág. 191, donde califica la radicación de “*francamente desafortunada*”.

^[lxxx] Villada, ob.cit., pág. 276. Apunta el nombrado que se trata de falseamientos que pueden provocar perjuicios, tipo de delitos que se estudian en el título XII del CP, especialmente el art. 293, por lo que bastaba al legislador agregar en dicho tipo “*insertar o hacer insertar declaraciones falsas en un archivo de datos personales público o privado...*”, para economizarse esta nueva disposición (pág. 277).

^[lxxxii] Villada, pág. 280, donde afirma que el tipo, legislando seriamente, debió expresar: “*el que insertare un dato falso sobre las condiciones personales o patrimoniales o personales de una persona, de modo que pueda resultar algún perjuicio*”.

^[lxxxiii] Ob.cit., pág. 193.

^[lxxxiiii] Ricardo C. Nuñez, “*Manual de Derecho Penal. Parte Especial*”, Marcos Lerner Editora Córdoba, 2º edición actualizada por Víctor F. Reinaldi, 1999, pág. 175.

^[lxxxv] Por su parte, Villada (op.cit., pág. 283) entiende que bien jurídico protegido es indudablemente desde el punto de vista “*subjetivo*” la intimidad de una persona física (en el inc. 1º) y desde el punto de vista “*objetivo*”, la confidencialidad y seguridad de datos personales reservados que existan en cualquier clase de archivo o banco de datos (inc. 2º).

^[lxxxvi] Ccte.: Donna, “*Derecho Penal. Parte Especial*”, Rubinzal-Culzoni Editores, Santa Fe, 2001, pág. 380. Allí relaciona la figura con la del art. 197.2 del CPE, con cita a Polaino Navarrete en el sentido que todo acceso cognitivo no autorizado al banco de datos reservados implica una lesión del bien jurídico intimidad, garantizado al titular de aquellos.

^[lxxxvii] Respecto del inciso 2º puntualiza Donna la posibilidad de realización del tipo con dolo eventual (ob.cit., pág. 381).

^[lxxxviii] Rectifico así anterior posición en la que había considerado al tipo como de peligro. Ccte.: Ledesma, quien refiriéndose al art. 157 bis 1º párrafo, entiende que es un delito formal o de pura actividad, que se consuma con el solo hecho de acceder, sin necesidad de la divulgación de datos ni de que se cause perjuicio, real o potencial (ob.cit., pág. 383). En cuanto al 2º párrafo de la misma norma, señala que el sujeto pasivo es el titular de los datos revelados que es, según el art. 2º de la ley 25.326, toda persona física o

jurídica con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere al propia ley (ob.cit., pág. 385).

^[xxxviii] Ob.cit., pág. 384 (inc. 1º) y 385 (inc. 2º).

^[xxxix] Pub. en el B.O. del 30/6/03. Fuente: Diario Judicial, sección Noticia del Día, correspondiente al 30 de junio de 2003 (www.diariojudicial.com.ar). Mediante ella se aprobó la “*clasificación de infracciones*” y “*la graduación de sanciones*” a aplicar frente a las infracciones que atenten contra la LPDP. Entre los objetivos perseguidos con ello, las autoridades han señalado que la disposición obedece a razones de seguridad jurídica, ello en un marco de acciones que tienen como norte la prevención, la difusión y educación de los ciudadanos sobre la protección de los datos personales. La normativa dictada dispone una clasificación de infracciones con sus pertinentes escalas sancionatorias. Las categoriza en leves (desde \$ 1000 a \$ 30.000), graves (\$ 3.000 a \$ 50.000) y muy graves (\$ 50.000 a \$ 100.000).

^[xl] Sancionada el 14/11/01, promulgada el 12/11/01 y publicada en el Boletín Oficial del 14/12/01. Puede consultarse además en “Anales de Legislación Argentina”, La Ley, Boletín Informativo N° 34, Año 2001, pág. 1 y ss. Ha sido reglamentada por Decreto 2628/2002, del 19/12/02. Puede ampliarse lo concerniente a este acápite con lo expuesto oportunamente en nuestra colaboración en la obra “Derecho Penal de los Negocios”, antes citada.

^[xli] En su obra conjunta con Roig Torres, “*Delitos informáticos y delitos comunes cometidos a través de la informática*”, Tirant lo blanch, Colección “Los delitos”, N° 41, Valencia, 2001, p. 147.

^[xlii] Frascchetti, “*La Ley de Firma Digital y las presunciones de autoría e integridad*”, pub. en J.A., revista del 25/2/04, pág. 45.

^[xliii] Cf. Pedro J. Montano, en su artículo “*Responsabilidad Penal e Informática*”, pub. en la siguiente dirección <http://unifr.ch/derechopenal/articulos/pdf/Montano1.pdf>.

^[xliv] Según informa Montano (trabajo citado), desde marzo de 2004 hay en tratamiento un proyecto de ley sobre firma digital y prestadores de servicio de certificación. En sus arts. 16 y 17 establece el régimen de sanciones administrativas y delitos de falsificación documentaria, respectivamente. El texto es el siguiente: “*Artículo 16.- Infracciones y sanciones administrativas.- Se considera infracción administrativa todo acto u omisión verificado por el prestador de servicios de certificación en contravención a las normas dispuestas en la presente Ley.- En tal caso, la URSEC podrá imponer a dichos prestadores, según la naturaleza y gravedad de la falta así como con arreglo a las normas del debido procedimiento, las siguientes sanciones: a. Amonestación; b. Multas de entre 2.500 U.l. y 250.000 U.l.; c. Suspensión de todas o algunas de las actividades del prestador de servicios de certificación de firma digital; d. Prohibición de la prestación directa o indirecta de la totalidad de los servicios hasta por el término de cinco años*” y “*Artículo 17.- Delitos de falsificación documentaria.- 1. El particular que proporcione un dato falso al prestador de servicios de certificación, o al tercero endargado de recoger la información, incurrirá en el delito previsto en el artículo 239 de Código Penal. 2. El que a sabiendas utilizara o se valiera de la firma digital o electrónica de un tercero, sin el consentimiento de éste, será castigado con la pena*

prevista en el artículo 240 del Código Penal. 3. Aquel que a sabiendas confeccionare una firma electrónica o una firma digital falsas, o adulterare una verdadera, o se valiera de la firma electrónica o digital de un tercero sin consentimiento de éste, o utilizare a sabiendas un certificado digital falso, incurrirá en el delito previsto en el artículo 239 del Código Penal. 4. A los efectos de las figuras delictivas previstas en el presente”.

[xlvi] Pub. en el B.O. del 21/9/04.

[xlvii] En efecto, allí se lo definía en su art. 4º en los siguientes términos: *“Será reprimido con prisión de un mes a seis años, el que con ánimo de lucro, para sí o para un tercero, mediante cualquier manipulación o artificio tecnológico semejante de un sistema o dato informático, procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. En el caso del párrafo anterior, si el perjuicio recae en alguna Administración pública, o entidad financiera, la pena será de dos a ocho años de prisión”.*

[xlviii] Toda la discusión previa a esta norma la he largamente expuesto en la citada obra *“Derecho Penal de los Negocios”* (parág. 120 *“Transferencia no consentida de activo patrimonial en perjuicio de tercero mediante manipulación informática”*, pág. 334 y ss), a la que remito por razones de brevedad. En concordancia, dice Alejandro O. Tazza que *“Los más destacable de esta reforma es que resuelve... el tan cuestionado supuesto que dividía a la doctrina y la jurisprudencia acerca del tipo penal aplicable cuando se obtenía un beneficio económico mediante la realización de una operación automática o mecánica en la que no existía un sujeto pasivo personal que por error provocaba el desplazamiento patrimonial propio de esta figura”* (en su trabajo *“Estafas con tarjetas de crédito y falsificación de moneda extranjera y otros papeles”*, pub. en L.L., diario del 5/5/05, pág. 2).

[xlviii] Fuente: diario *“Clarín”*, ejemplar del 19 de junio de 2005, págs. 48/49, nota titulada *“Un hacker robó datos de 40 millones de tarjetas de crédito”*.

[lix] Fuente: diario *“Clarín”*, ejemplar del 27 de junio de 2005, pág. 29, nota titulada *“Temor por el robo de datos en Internet”*.

[li] Fuente: diario *“Clarín”*, nota de tapa del *“Suplemento Económico”* del día 26 de junio de 2005, firmada por Damián Kantor y titulada *“La inseguridad informática preocupa a las empresas”*, págs. 3/4.

[lii] En su trabajo *“Brazil: o crime de divulgação de pornografia infantil pela Internet. Breves comentários á Lei 10.764/03”*, pub. en la revista virtual ALFA-REDI, sección *“Delitos Informáticos”*. Allí informa que la inclusión de la pornografía infantil virtual formó parte de la discusión parlamentaria, concretamente por intermedio del diputado Carlos Biscaia, con resultado negativo según se vio. Ello trae para Iriarte dos consecuencias: 1) se evita una eventual inconstitucionalidad por conflicto con el principio de libertad de expresión (cita al respecto el devenir de la Child Pornography Prevention Act estadounidense de 1996, reputada tal por la Corte Suprema); 2) la exclusión puede dificultar la persecución criminal en casos de efectivo delito de diseminación de material pedófilo, ya que podría eventualmente por los autores de las imágenes alegarse que se no se usaron menores reales para su elaboración.

^[liii] Este parece haber sido el criterio del Anteproyecto de Código Penal, pues no ha cambiado la redacción del actual art. 128, que allí pasa a ser el art. 161. Pablo Palazzi se ha pronunciado requiriendo una incorporación expresa, señalando que estaba contemplado en el anteproyecto de ley especial de la Comisión Interministerial (Ministerios de Justicia y Relaciones Exteriores) de 2004 y que la punición de la ciberpornografía está prevista por la Convención de Cibercriminación elaborada por el Consejo Europeo del año 2001, lo que resulta una nota de interés en orden al proceso de armonización (cf. su trabajo “*Breve comentario a los proyectos legislativos sobre delitos informáticos*”, pub. en la “*Revista de Derecho Penal y Procesal Penal*”, LexisNexis, Bs.As., 2006, fasc. 8, págs.1529/1530).

^[liiii] Pub. en el B.O. del 25 de agosto de 2003.

^[liv] Vinculado, puede recordarse con Muñoz Conde la modificación del art. 189 del CPE, que en su nuevo párrafo 7 penaliza la producción o difusión de material pornográfico “en el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada”. Es decir, se tipifica la utilización de imágenes virtuales sin ninguna base real, lo que lleva al reconocido profesor a preguntarse si no estamos frente a un nuevo derecho penal de autor, donde lo punible es la tendencia pederasta como tal, aún cuando se traduzca en actos que concretamente incidan directamente en un menor o incapaz (así, en su trabajo “*Las reformas...*”, ya citado).

^[lv] Pub. en el medio virtual www.elDial.com, sección el Dial Express, diario del 16/03/06.

^[lvi] El art. 278 (exhibición pornográfica) dice: “*Comete delito de exhibición pornográfica el que ofrece públicamente espectáculos teatrales o cinematográficos obscenos, el que transmite audiciones o efectúa publicaciones de idéntico carácter. Este delito se castiga con la pena de tres a veinticuatro meses de prisión*”.

^[lvii] Esta carencia era reconocida expresamente por la Secretaría Nacional de la Niñez y Adolescencia, en su informe “*Situación de la pornografía infantil en Internet en el Paraguay*” correspondiente al año 2004 (disponible en http://iin.oea.org/proy_trafico_ninos_internet/iintpi/pronog.paraguay.pdf).

^[lviii] La información consta en la siguiente dirección: http://scs/at.org/news/esp/noticias.php?_cod_208.

^[lix] En lo que sigue se sintetiza el análisis de la cuestión realizado en el artículo “*Algo más sobre el daño y sabotaje informáticos (en función del criterio de la Cámara Federal Criminal y Correccional)*”, pub. en la revista “*El Derecho Penal. Doctrina y Jurisprudencia*”, N° 1 enero de 2006, págs. 5/26. Allí se amplían las referencias bibliográficas que en lo sucesivo se hacen en el texto principal.-

^[lx] En su artículo “*Consideraciones para una reforma penal en materia de seguridad y virus informáticos*”, pub. en J.A., 1996-II-841.

^[lxi] Fallo de la Sala 6°, CNCyCorr., Cap. Fed., 30/4/93. Puede consultarse en “*Informática y D.P.A.*”, ya citado, págs. 154/155.

[lxii] Carlos Creus, “*Derecho Penal. Parte Especial*”, Tomo 1, 4º edición actualizada, Astrea, Bs.As., 1993, pág. 602, parág. 1380.

[lxiii] Así, CNCyCorrec., Sala IV, fallo del 13/2/90, pub. en ED 138-722, citado concordante por Edgardo A. Donna, en su “*Derecho Penal. Parte Especial*”, Tomo II-B, Rubinzal-Culzoni editores, 2001, pág. 760.

[lxiv] Entre sus múltiples publicaciones en el medio virtual pueden citarse la oficial en http://www.jus.gov.ar/guia/content_codigo_penal.htm y la de los sitios “Pensamiento Penal” (www.pensamientopenal.com.ar) y “Derecho Penal Online” (www.derechopenalonline.com.ar), que han elaborado sendos foros de discusión al respecto con amplia concurrencia e interesantes observaciones.

[lxv] Así, en su trabajo “*Brazil: do delito de dano e de sua aplicação ao Direito Penal Informático*”, pub. en el sitio www.informatica-juridica.com, disponible desde el 14/8/03. Allí concluye que el delito de daño del art. 163 CPB es “*perfectamente aplicable a la tutela de los datos informáticos, siendo completamente prescindible la creación de un nuevo tipo penal para tal fin. Se trata de la interpretación extensiva de la palabra “cosa”, elemento objetivo del tipo penal*” (traducción personal).

[lxvi] Cf. informa Omar Kaminski en su trabajo “*Brazil: os virus de computador e a legislação penal brasileira*”, disponible en el medio virtual ALFA-REDI, sección “Delitos informáticos”. En cuanto al estado del proyecto de ley sobre delitos tecnológicos en el Senado, uno de sus miembros, Marcelo Crivella, presentó una serie de enmiendas creando nuevas figuras delictivas, en particular, los tipos de falsedad informática (art. 154-C) y de sabotaje informático (art. 154-D), así como la obligación para todos los ISP de almacenar los registros de movimientos de sus usuarios por un plazo de tres años. Señala Democrito Reinaldo que, más allá de los beneficios que pudieran significar las nuevas figuras a la redacción original, sigue retrasándose el proyecto y este, en la redacción del diputado Piauhyino, era un estatuto básico de delitos informáticos que cubre bien ese papel. En su trabajo recuerda que las figuras contempladas en el proyecto originario eran: acceso indebido a medio electrónico, manipulación indebida de información electrónica, pornografía infantil, difusión de virus electrónico, falsificación de teléfono celular por medio de acceso a sistema informático, falsificación de tarjeta de crédito, daño electrónico, además de definir conceptos como “medio electrónico”, “sistema informático” y regular las modalidades de interceptación de comunicaciones telefónica, informática y telemática (cf. su artículo “*Brazil: o projeto de lei sobre crimes tecnológicos (PL 84/99). Notas ao parecer do Senador Marcello Crivella*”, pub. en el medio virtual www.informatica-juridica.com).

[lxvii] Sobre los proyectos legislativos al respecto he informado en el artículo antes citado pub. en EDP, enero de 2006, págs. 25/26.

[lxviii] Ccte.: Tulio Vianna, ya citado.

[lxix] Palazzi, “*Breve comentario...*”, ya citado, pág. 1531.

[lxx] Ccte.: Andrés Figoli, quien tras recordar que la protección de la vida privada tiene raíz constitucional implícitamente reconocida en el art. 7 de la C.N. uruguayana, en correlato con el art. 72 de la misma y normas internacionales como los arts. 12 de

DUDH, el 11.2 del Pacto de San José de Costa Rica y el 17 del PIDCyP de Naciones Unidas, señala que las figuras actuales de la legislación penal uruguaya no comprenderían este orden de situaciones (en su trabajo *“Uruguay: El acceso no autorizado a sistemas informáticos”*, pub. en el medio virtual ALFA-REDI, sección “Delitos Informáticos”).

^[lxxii] Dice: *“El que, por medios fraudulentos, se enterare del contenido de documentos públicos o privados que por su propia naturaleza debieran permanecer secretos, y que no constituyeran correspondencia, será castigado, siempre que del hecho resultaren perjuicios, con multa de 20 U.R. (veinte unidades reajustables) a 400 U.R.(cuatrocientas unidades reajustables)”*.

^[lxxiii] Sentencia de 1º instancia del Juzgado Letrado en lo Penal de 8º turno, Juez Pablo Eguren Casal, N° 311/96 del 27/2/98, confirmada en 2º instancia, según informa Figoli en el artículo ya citado.

^[lxxiiii] Ob.cit., punto 3.

^[lxxiv] Así, Fernando M. Fernández, en su trabajo *“Resumen de la ley de delitos informáticos en Venezuela”*, pub. en el portal jurídico “Delitos Informáticos” (www.delitosinformaticos.com), sección “Estafas”.

^[lxxv] En su trabajo ya citado.