
Revista
Enero 2012
29
tirant lo blanch

Revista Penal

Número 29

Sumario

Publicación semestral editada en colaboración con las Universidades de Huelva, Salamanca, Castilla-La Mancha, Pablo Olavide de Sevilla y la Cátedra de Derechos Humanos Manuel de Lardizábal.

www.revistapenal.com

EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email:tlb@tirant.com
http://www.tirant.com
Librería virtual: http://www.tirant.es
DEPÓSITO LEGAL:
ISSN.: 1138-9168
IMPRIME: Guada Impresores, S.L.
MAQUETA: PMc Media

La regulación de los delitos informáticos en el Código Penal argentino

Por Gustavo A. AROCENA*

"La computación ya no sólo tiene que ver con computadoras.
Tiene que ver con la vida"
(**Nicholas NEGROPONTE**, *Ser digital (being digital)*,
traducción de Dorotea Pläcking,
Atlántida, Buenos Aires, 1995, p. 14).

Revista Penal, n.º 29.— Enero 2012

***RESUMEN**: En el presente ensayo, el autor analiza la ley nacional argentina nº 26.388, de 2008, que modifica el Código Penal de ese país, incorporando distintas modalidades delictivas vinculadas con los sistemas informáticos. Previo a ello, el jurista propone su propia definición del delito informático, examina sus características definitorias y presenta las diversas opciones legislativas que se encuentran en el Derecho comparado a la hora de regular sobre esta materia. Por último, el penalista estudia en forma breve, aunque prolija, la mencionada reforma.*

***PALABRAS CLAVE:** delito informático, cibercriminalidad, hacking, fraude informático, cracking, Convenio sobre Cibercriminalidad de Budapest.*

***ABSTRACT:** In this essay, the author analyses argentinean law nº 26.338, of 2008, that modifies the criminal law of his country, incorporating different forms of the crime related to computer systems. Before that, the jurist proposes his own definition of the computer crime, examines its characteristics and presents the diverse legislative options that he finds in the compared law at the moment of regulating on this matter. Finally, the writer studies in brief form, though prolix, the mentioned reform.*

***KEY WORDS:** Cybercrime, cybercriminality, hacking, cyber fraud, cracking, Budapest Convention on Cybercrime.*

* Profesor de Derecho Penal (Parte Especial) y de Derecho Procesal Penal, en la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Córdoba (República Argentina). Co-director del Centro de Investigación Interdisciplinaria en Derecho Penal Económico (http://www.ciidpe.com.ar/). Ha publicado, en Argentina y en el extranjero, numerosos trabajos monográficos y artículos relacionados con sus principales materias de investigación: la Parte Especial del Derecho Penal, el Derecho Procesal Penal y el Derecho de Ejecución Penal.

SUMARIO*: *I. El Derecho penal y la informática. II. El principio de subsidiariedad del Derecho penal. III. El Código Penal argentino de 1921 y la delincuencia informática. IV. Concepto y principales características definitorias del delito informático. V. Regulación legal del delito informático: Derecho comparado, antecedentes legislativos argentinos y normativa vigente en nuestro país. VI. Reflexión final. Bibliografía.

I. El Derecho penal y la informática

En los tiempos que corren, las **nuevas tecnologías**, en general, y la **informática**, en particular, introducen incansablemente no sólo **nuevas formas de realizar tareas conocidas**, sino también **nuevas actividades**, muchas de las cuales se manifiestan como antisociales y reprobables, en razón de interferir en la pacífica convivencia de los ciudadanos.

Es que la informática no sólo importa una técnica destinada a hacer lo mismo, aunque mejor y más rápido, por medio de la ayuda electrónica y del soporte magnético. Por el contrario, ella supone también una fértil fuente de *nuevos estados de cosas*, que pueden colocar en jaque a los sistemas jurídicos, cuando los muestran impotentes para contemplar las nuevas realidades.

Si, como es fácil advertir, una nueva revolución tecnológica afecta hoy a la información jurídica, y la etapa a iniciar ha de cambiar nuestra vida y nuestro pensamiento al menos tanto como lo hicieron las técnicas del Derecho escrito y del Derecho impreso —que la técnica informática, superpuesta a ellas, viene a potenciar—, no puede el Derecho penal quedar ajeno a tamaña circunstancia.

Es algo enseñado y aceptado que con las conquistas técnicas se abre un campo del que parten los influjos más intensos sobre el desarrollo de la criminalidad.

Lo cierto es que, en el ámbito de la **delincuencia dolosa tradicional**, el progreso tecnológico da lugar a la adopción de nuevas técnicas como instrumento que le permite producir **resultados especialmente lesivos**, a la vez que posibilita el surgimiento de modalidades delictivas dolosas de nuevo cuño.

Pero también resultan relevantes, y quizás en mayor grado, los impactos tecnológicos en el ámbito de la **delincuencia no intencional** (infracciones cometidas con dolo eventual o infracciones imprudentes).

II. El principio de subsidiariedad del Derecho penal

1. Sentado esto, cabe afirmar que ante el surgimiento de nuevas conductas reprochables —como, por ejemplo, las relativas a la informática—, lo primero que debe tener presente el legislador son las implicancias del **principio de subsidiariedad del Derecho penal**.

Según este principio, el Derecho criminal deja de ser necesario para proteger a la sociedad cuando esto puede conseguirse por **otros medios**, que serán **preferibles en cuanto sean menos lesivos** para los derechos individuales[1].

De tal suerte, así como aparece irrefutable el impacto que, en moneda de nuevos efectos **disfuncionales** para la sociedad, tiene la alta tecnología informática, también lo es que el Derecho penal no resulta el *único* —ni, en muchos casos, el *mejor*— instrumento para hacerles frente.

En este sentido, existe una amplia coincidencia en el sentido de entender que sólo son legítimas las penas necesarias: el arraigo del principio de "intervención mínima" muestra, precisamente, que no hay discrepancias a la hora de proponer una reducción de los mecanismos punitivos del Estado al "mínimo necesario".

En lo que atañe a nuestro tema, podríamos decir que la tipificación penal de las conductas indeseadas que plantean las nuevas tecnologías sólo parecerá legitimada, en la medida en que contribuya a aportar una reducción de la *violencia social informal* imposible de lograr mediante otros instrumentos del sistema jurídico, como los que pueden propiciar el Derecho civil y el Derecho administrativo.

La medida de la necesidad de tutela penal, pues, podría resolverse sobre la base de la regla según la cual debe sancionarse **tanta legislación penal** para las conductas nocivas de la tecnología informática, **como incapaces para lograr su evitación sean otros medios** del sistema jurídico.

1 Sobre esta máxima, LUZÓN PEÑA asevera: "Según el principio de subsidiariedad —también denominado entre nosotros (...) «*principio de intervención mínima*»—, derivado directamente del de necesidad, el Derecho penal ha de ser la «*ultima ratio*», el último recurso al que hay que acudir a falta de otros menos lesivos, pues si la protección de la sociedad y los ciudadanos puede conseguirse en ciertos casos con medios menos lesivos y graves que los penales, no es preciso ni se debe utilizar éstos" (cfr. LUZÓN PEÑA, Diego-Manuel, *Curso de Derecho penal. Parte general*, 1ª edición, 1ª reimpresión, Universitas, Madrid, 1999, t. I, p. 82).

En otros términos, se justificará el recurso al Derecho penal, cuando la protección de los bienes jurídicos por parte de las otras ramas del ordenamiento legal resulte insuficiente para asegurar la defensa de aquéllos.

Pero, incluso, aun cuando se tenga por justificada la necesidad del Derecho penal para el tratamiento de las cuestiones problemáticas que trae aparejadas la alta tecnología informática, resulta indispensable determinar también si es imprescindible sancionar **nuevas reglas** del Derecho criminal enderezadas a dicha tarea.

Sólo si el ordenamiento jurídico penal fracasa en su función regulativa de las conductas humanas, pues no indica solución alguna, deberán promulgarse nuevas reglas penales. En suma, sólo si el sistema jurídico penal es *incompleto*.

Otro tanto podría afirmarse si la respuesta que brinda el ordenamiento criminal para cierta hipótesis es **inadecuada**.

Por ello, siempre debe analizarse si los tipos penales vigentes en determinado orden jurídico resultan o no ineptos para contemplar los fenómenos que plantean las modernas tecnologías, porque sólo en el último caso aparecerá justificada la creación de nuevas normas.

2. Todo cuanto acaba de afirmarse resulta relevante ante un fenómeno frecuente en la legislación penal de los últimos tiempos.

Es habitual que las diversas situaciones que derivan de los progresos tecnológicos tengan como contrapartida la rápida reacción de los responsables de crear las normas jurídicas, elaborando nuevas reglas sin realizar una profunda reflexión previa acerca de las **posibilidades del sistema jurídico para "*hacerse cargo*" de aquéllas eficazmente**.

No es difícil constatar la existencia de una tendencia claramente dominante en la legislación hacia la introducción de nuevos tipos penales y la agravación de los ya existentes, que puede enclavarse en el marco general de la restricción o la "reinterpretación" de las garantías clásicas del Derecho penal sustantivo y del Derecho penal procesal.

Así, se crean nuevos "bienes jurídico-penales", se amplían los espacios de riesgos jurídico-penalmente relevantes, se flexibilizan las reglas de imputación y se relativizan los principios político-criminales de garantía, en una tendencia general a la que podría designarse con la expresión "**expansión del Derecho penal**"[2].

Ante tal tendencia, acaso pueda pensarse como criterio corrector, un principio que propusiera que se legislaran **tantas nuevas reglas de Derecho penal** para las conductas nocivas que trae aparejada la tecnología informática, como inidóneas sean las reglas vigentes del ordenamiento jurídico penal para hacerles frente.

III. El Código Penal argentino de 1921 y la delincuencia informática

Es innegable que el legislador que elaboró el **Código Penal** promulgado por el Presidente Hipólito Yrigoyen el 29 de octubre de **1921** no podía prever los desarrollos tecnológicos que ocurrirían en los más de ochenta años posteriores, ni el impacto que ellos tendrían en los sistemas jurídicos.

Quizás esta circunstancia plantee un dato relevante a la hora de determinar la eventual *idoneidad* de los tipos penales vigentes para acoger la delincuencia informática.

No sólo la existencia de **hipótesis fácticas de imposible subsunción** en las figuras penales existentes provee casos a contemplar en eventuales nuevas tipificaciones legales.

Por el contrario, también justifica la construcción de nuevas figuras delictivas la constatación de que la posible subsunción de un supuesto fáctico novedoso en un tipo penal existente obtiene del sistema normativo una **respuesta impropia**.

Una **respuesta *impropia*** de los tipos penales sería una pena cuya naturaleza no corresponda al contenido de injusto del hecho atrapado en el tipo penal.

Es que el hecho de que entre pena y delito no exista ninguna relación natural no excluye que la primera deba ser *adecuada* al segundo en alguna medida.

Al contrario, el carácter convencional y legal del nexo retributivo que liga la sanción al ilícito penal exige que la elección de la calidad y de la cantidad del castigo se realice por el legislador y por el juez *en relación con* la naturaleza y gravedad de la infracción.

En razón de lo expuesto, resulta invariablemente necesario analizar los tipos penales vigentes en un lugar y tiempo determinado, para así dilucidar si tales descripciones, en los casos en que aportan un *molde* apto para captar ciertas hipótesis fácticas, lo hacen mediante una

2 Sobre esto, v. SILVA SÁNCHEZ, Jesús-María, *La expansión del Derecho penal —Aspectos de la política criminal en las sociedades postindustriales—*, 1ª edición, reimpresión, Madrid, 2001, pp. 15 y ss.; y CESANO, José Daniel, *La política criminal y la emergencia (Entre el simbolismo y el resurgimiento punitivo)*, Mediterránea, 2004, pp. 23 y ss.

respuesta punitiva **acorde con el contenido de injusto** de las "nuevas realidades".

IV. Concepto y principales características definitorias del delito informático

Llegados a este punto, conviene intentar delinear los contornos de un **concepto de delito informático** —ni el único ni el último—, que reúna, a la vez, las notas de justeza y diafanidad expresiva.

El **delito informático o ciberdelito** es el injusto determinado en sus elementos por el **tipo de la ley penal**, conminado con pena y por el que el autor merece un reproche de culpabilidad, que, utilizando a los **sistemas informáticos** como **medio comisivo** o teniendo a aquéllos, en parte o en todo, como su **objeto**, se vinculan con el **tratamiento automático de datos**.

No podemos ocuparnos en esta breve exposición del análisis de todas y cada una de las características definitorias que componen esta noción de delito informático.

Sin perjuicio de ello, debemos mencionar que el concepto de ciberdelito se construye en derredor de la noción de **"sistema informático",** pues, como se acaba de ver, es éste el que, en la clase de infracciones que analizamos, se constituye en el *instrumento del delito* o su *objeto de ataque*, o sea, el medio a través del cual el ilícito se comete, o en el objeto material sobre el cual recae la conducta típica.

Parece imprescindible, entonces, que se proponga una básica definición de este elemento.

El "**sistema informático**" es **todo dispositivo o grupo de elementos relacionados que realiza el tratamiento automatizado de datos, generando, enviando, recibiendo, procesando o almacenando información de cualquier forma y por cualquier medio**.

Este dispositivo o grupo de dispositivos ha de servir para el tratamiento automatizado de datos.

El tratamiento de la información es "**automatizada**" cuando se emplean para ello, no ya personas físicas, sino dispositivos mecánicos o electrónicos. Es claro que la computadora es operada por un ser humano, pero el tratamiento de los datos, *en sí mismo*, es llevado a cabo por tales dispositivos tecnológicos.

Lo que se maneja a través del sistema son "**datos informáticos**", o sea, representaciones de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.

Es sabido que, hoy por hoy, la **información** ha adquirido un valor altísimo desde el punto de vista económico, constituyéndose en un bien sustrato del tráfico jurídico, con relevancia jurídico-penal por ser posible objeto de conductas delictivas (acceso ilegítimo, sabotaje o daño informático, espionaje informático, etc.) y por ser instrumento de comisión, facilitación, aseguramiento y calificación de los ilícitos tradicionales.

Otro rasgo saliente de la infracción informática es su extraterritorialidad **y su** intemporalidad**.**

El "**derribo de las fronteras**" derivado de las características de la delincuencia moderna transnacional y el fenómeno de la "aldea global" surgido del uso de Internet por un operador situado en cualquier lugar del globo, valiéndose de una computadora, un teléfono, un módem y un proveedor del servicio hacen risibles los ejemplos tradicionales de "casos difíciles" sobre la determinación de la ley aplicable en el espacio[3] y nos colocan ante una fantástica serie de situaciones de colisión de derechos penales nacionales frente a un mismo supuesto de hecho.

En cuanto a esto, CÁRDENAS, refiriéndose específicamente a los delitos cometidos a través de Internet, asevera que, en ellos, "...lo corriente será que se trate de «delitos a distancia» en los que la conducta no se inicia o no tiene lugar en el mismo Estado que la consumación, o de «delitos de tránsito», donde tanto la conducta como la consumación tienen lugar en país extranjero, sirviendo el Estado de que se trate solamente de lugar de tránsito (por ejemplo, porque la información pasa por un servidor ubicado allí). En estas clases de delito [agrega la autora] resulta necesaria una elaboración teórica para determinar cuál o cuáles son los Estados facultados para ejercer su jurisdicción y aplicar su derecho penal sobre el caso"[4].

3 Recuérdese que, en nuestro derecho positivo vigente (artículo 1 CP), la regla, en orden a la validez espacial de la ley penal, es *la territorialidad de la ley penal argentina*, operando sólo en forma subsidiaria el denominado *principio real, de defensa o de protección del Estado*. Según el primer criterio, es válida la ley penal del lugar donde se comete el delito, sin interesar dónde deba producir sus efectos, ni la nacionalidad de su autor o del sujeto pasivo. Conforme el segundo, es válida la ley penal argentina para los delitos cuyos efectos deban producirse en el territorio de la Nación Argentina o en los lugares sometidos a su jurisdicción. De la vigencia, como regla, del "principio de territorialidad" se desprende claramente la *importancia* de determinar cuál es el lugar en que se considera cometido el delito informático.

4 V. CÁRDENAS, Claudia, "El lugar de comisión de los denominados ciberdelitos", en Política Criminal, nº 6, 2008, A2-6, p. 4, disponible en World Wide Web: http://www.politicacriminal.cl/n_06/a_2_6.pdf (accedido el 21 de octubre de 2010).

Por lo demás, el problema del lugar de comisión de esta clase de infracciones no parece que pueda ser resuelto por medio del reconocimiento de que tal lugar no es otro que el "**ciberespacio**"; es que, si así se admitiera, el fenómeno cultural del delito informático quedaría, por virtud de la vigencia general del criterio territorial en materia de validez espacial de la ley penal, fuera de la jurisdicción de cualquier Estado, lo que no parece una alternativa plausible[5].

Pero la disociación entre acción y resultado típico de los delitos informáticos no se verifica sólo espacial, sino también temporalmente.

Por existir en las computadoras un reloj interno que es alimentado por una batería, es posible tanto determinar la fecha en que se activará el programa o se ejecutará una determinada instrucción dañosa (p.ej., el virus informático *Jerusalén* estaba destinado a destruir todas las memorias militares y científicas de Israel el 13 de mayo de 1988), como obstaculizar la investigación de tales hechos (p.ej., mediante programas que al detectar un acceso eliminan determinada información o avisan del intento de acceso a alguien o al propio autor del delito, que de esa manera saben que lo están investigando).

La especial mención que hemos hecho de estos particulares caracteres tiene justificación.

Según nuestro entender, estos rasgos demuestran que la ilicitud informática —al igual que otras formas de delincuencia de las sociedades postindustriales, como el terrorismo, el narcotráfico, el tráfico de armas, etc.— imponen **repensar** no sólo las **categorías de la Parte Especial del Derecho penal**, sino también los estratos analíticos propios de su **Parte General**.

En cuanto a esto, cabe enfatizar que el Derecho penal de la globalización es, desde algún punto de vista, eminentemente práctico, pues trata de proporcionar una respuesta uniforme o, al menos, armónica a la delincuencia transnacional, que evite la conformación de "*paraísos jurídico-penales*".

La existencia de estos "*paraísos*" resulta especialmente disfuncional cuando se trata de combatir una modalidad de delincuencia como la cibercriminalidad, en la que —conforme acaba de destacarse— el lugar y el momento de la intervención de los principales responsables pueden resultar perfectamente disponibles.

La obtención de tal respuesta tendencialmente uniforme no es fácil.

De entrada, podría pensarse en una suficiencia de los procesos de armonización de legislaciones en los preceptos correspondientes.

Sin embargo, ello, con ser necesario e importante, no resulta suficiente.

Es preciso, además, homogeneizar las reglas legales de la Parte General que determinan esencialmente la aplicación que haya de darse a tales preceptos específicos.

Lo anterior, incluso, puede también resultar insuficiente si no se trabaja de modo simultáneo en una construcción supranacional relativamente homogénea del sistema del Derecho penal, de los conceptos y categorías de la teoría jurídica del delito, y de los principios y garantías político-criminales fundamentales.

V. Regulación legal del delito informático: Derecho comparado, antecedentes legislativos argentinos y normativa vigente en nuestro país

1. Ahora bien, determinada la eventual necesidad de una regulación legal específica del ciberdelito, existen dos opciones a la hora de pergeñar esta normativa particular.

Por un lado, puede sancionarse una **ley específica**, complementaria del Código Penal. Es la opción por la que se han inclinado, por ejemplo, **Venezuela** —que sancionó su "Ley Especial contra los Delitos Informáticos" el 30 de octubre de 2001—, **Chile** —que hizo lo propio mediante ley nº 19.223, del 28 de mayo de 1993— y **Alemania** —que el 15 de mayo de 1986 adoptó la "Segunda Ley contra la Criminalidad Económica", que se ocupa casi excluyentemente de la ciberdelincuencia, pero atrapa igualmente algunas figuras ajenas a ella, como, por caso, la utilización abusiva de cheques—.

5 Aunque no podemos detenernos aquí en este tema, parece conveniente señalar que las distintas opciones que pueden encontrarse a la hora de determinar el lugar de comisión del delito informático son: **a)** Aplicar la ley del Estado donde está *físicamente* presente la persona que ejecutó la acción (**teoría de la actividad**); **b)** Emplear la ley del Estado donde se produce el resultado típico que consuma el delito (**teoría del resultado**); y **c)** Tener en cuenta las leyes del Estado donde se lleva a cabo la conducta típica y la de aquel donde se produjo el resultado, es decir, tanto la jurisdicción de uno como la del otro Estado serían competentes (**teoría de la ubicuidad**). Cabe agregar, por otro lado, que las llamadas "teoría de la actividad" y "teoría del resultado", han dado lugar a interpretaciones extensivas sobre su sentido y alcance, cuando de ciberdelitos se trata. Tales intelecciones se apoyan en la divergente significación que se asigna a los conceptos de "acción" y "resultado" del delito informático. Sobre esto, v. CÁRDENAS, "El lugar de comisión", pp. 7 a 10.

Por el otro, puede preferirse una **reforma del Código Penal**, ora agregando un nuevo título que contemple las nuevas ilicitudes no tipificadas, ora ubicando éstas en los distintos títulos del digesto, conforme los diversos bienes jurídicos que pretendan tutelarse. Entre otros países, ha legislado sobre los delitos informáticos en su Código Penal, mediante la creación de un capítulo específicamente dedicados a ellos, **Bolivia**: en su Libro Segundo, el Título XII —destinado a los delitos contra la propiedad— incorpora el Capítulo XI, que tipifica los delitos informáticos. En cambio, ha preferido regular los ciberdelitos en su código penal, esparciendo las diversas figuras en distintos pasajes de su articulado, **Paraguay**, **España**[6] y **Francia**, por ejemplo.

En nuestro país, en el desarrollo histórico de la legislación penal más reciente, encontramos ejemplos de cada una de estas dos grandes alternativas, aunque la normativa vigente decide incluir la cibercriminalidad en su Código Penal en forma desconcentrada, esto es, incluyendo los distintos tipos legales en los diversos títulos del Libro Segundo del digesto, conforme los variados objetos jurídicos que se desea tutelar.

1.1. La **elaboración de una ley específica sobre ciberdelitos** fue la elección de, *verbi gratia*, la Secretaría de Comunicaciones del Ministerio de Infraestructura y Vivienda de la Nación, que —mediante **resolución nº 476/2001**[7]**—** preparó un **"Anteproyecto de Ley de Delitos Informáticos".**

En los Fundamentos de este Anteproyecto, la Secretaría de Comunicaciones explicaba que se optaba por incluir estos delitos en una ley especial, en lugar de apelar a la introducción de enmiendas al Código Penal, fundamentalmente para no romper el equilibrio de su sistemática y por tratarse de un bien jurídico novedoso que amerita una especial protección jurídico-penal. Además, se prefería esta alternativa porque tal esquema tiene la bondad de permitir la incorporación de nuevas figuras que hagan a la temática dentro de su mismo seno, sin volver a tener que discernir nuevamente con el problema de romper el equilibrio de nuestro Código Penal, que viene siendo objeto de sucesivas modificaciones.

Este "Anteproyecto de Ley de Delitos Informáticos" estructuraba distintos tipos delictivos, entre cuyos elementos se encontraban las nociones de "sistema informático" y "dato informático" o "información".

El mismo compendio normativo delimitaba el alcance de tales conceptos, mediante **definiciones estipulativas**[8] contenidas en su artículo 6°.

El **bien jurídico tutelado** en los delitos informáticos, se decía en los Fundamentos del Anteproyecto, es, precisamente, **la información, en todos sus aspectos** (v. gr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos), entendiéndose que su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnologías, etc.).

Sin embargo, se aclaraba, **la información**, como valor a proteger, **ha sido tenida en consideración por el Derecho penal en otras ocasiones**. Ello no obstante —enfatizaban los Fundamentos—, se lo ha hecho desde la óptica de la confidencialidad, **pero no como un nuevo bien jurídico tutelado abarcativo de varios intereses dignos de protección penal**.

Asimismo se buscaba —según la Secretaría—, de alguna manera, cubrir las lagunas legales que fueron quedando luego de la incorporación de cierta protección a determinados intangibles en nuestro derecho positivo nacional.

El Anteproyecto proponía la creación de **tres tipos de delitos básicos**, con sus correspondientes **agravantes**, a saber: el "***hacking***", el "***cracking***" y el "**fraude informático**".

En el "Anteproyecto" se decidía privilegiar el tratamiento de esas tres figuras delictivas, puesto que —ex-

6 Para un análisis de la regulación de los delitos informáticos en España, v. GONZÁLEZ RUS, Juan José, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", en Revista Electrónica de Ciencia Penal y Criminología (RECPC), num. 01 (1999), disponible en World Wide Web: http://criminet.ugr.es/recpc/recpc_01-14.html (accedido el 2 de noviembre de 2010).

7 BON 26/11/2001.

8 Es sabido que las **definiciones legales** son, precisamente, estipulaciones que introduce el legislador en un determinado conjunto normativo, como una forma de permitir la mejor identificación de las propias normas de dicho universo de reglas. Para un interesante estudio acerca de la función de las definiciones legales, puede verse ALCHOURRÓN, Carlos E./BULYGIN, Eugenio, "Definiciones y normas", en ALCHOURRÓN, Carlos E./BULYGIN, Eugenio, *Análisis lógico y derecho*, Centro de Estudios Constitucionales, Madrid, 1991, pp. 439 y ss.

presaban los fundamentos—, no una gran cantidad, sino la mayoría de las conductas que habitualmente se cometen o se buscan cometer dentro del ámbito informático, son alcanzadas por alguno de los tipos tratados.

1.2. La **reforma del Código Penal** para absorber las modalidades delictivas vinculadas con la informática es, en cambio, la alternativa a la que ha apelado la vigente **ley nacional nº 26.388**[9], sancionada el 4 de junio de 2008.

Lo ha hecho conforme el "**criterio desconcentrado**" que antes hemos presentado, o sea, difuminando las distintas figuras delictivas en los diversos títulos del Libro Segundo del digesto criminal, ubicándolos con arreglo al específico objeto jurídico que se desea tutelar mediante cada tipificación legal.

En razón de esto, *en principio*[10], **no puede predicarse ya la existencia de un único bien jurídico** amparado por los nuevos delitos informáticos; antes bien, lo resguardado mediante cada una de estas figuras será el común objeto jurídico designado por el título del código que alberga una u otra descripción típica.

No parece superfluo subrayar que, en buena medida, la ley se ha basado en el **Convenio sobre Cibercriminalidad de Budapest**, redactado en 2001 por el Consejo de Europa, junto a Estados Unidos, Canadá, Japón, Costa Rica, Méjico y Sudáfrica, y al que la República Argentina ha adherido durante el año 2010.

1.2.1. La **doctrina jurídica** argentina ha expresado su **opinión** sobre el nacimiento de este conjunto normativo.

Así, por ejemplo, apenas nacida la ley, GRANERO subrayaba: "Con su sanción el Estado ha considerado suficientemente grave privar de la libertad o sancionar económicamente a quien hoy transgrede los nuevos tipos legales. Ya no hay dudas, hoy la pornografía de menores en Internet, abrir un mail del cual no se es el destinatario, ingresar indebidamente a una base de datos, o le producir daños a sistemas informáticos u ocultar pruebas existentes en registros, ya es claramente delito. Y eso no es poco. El Estado les ha dado a estas situaciones un respeto acorde con las nuevas circunstancias y ha reconocido la influencia de la tecnología es este nuevo ordenamiento legal. Poco importa si existen falencias técnicas o mejoras que debieron haberse aprovechado al respecto. Será tarea de nuevas investigaciones y de avances doctrinarios y jurisprudenciales"[11].

Ya con algún tiempo de vigencia de la 26.388, RIQUERT ha señalado que ella, "...ha significado un sustancial avance sobre temas cuya consideración venía siendo reclamada desde mucho tiempo atrás, poniendo fin a antiguas discusiones jurisprudenciales y doctrinarias. A su vez, resulta un aporte hacia la armonización legislativa en la materia con otros países del bloque regional que se ocuparan antes de esta problemática en un modo más integral"[12]; la aseveración no le ha impedido al jurista advertir que la ley nacional nº 26.388, "... junto a las recientes nº 26.362 y 26.364, marcan el «reinicio» en estos últimos meses de la inadecuada práctica de «emparchar», reformar en modo parcial o, lisa y llanamente, descodificar mediante leyes especiales, en materia penal"[13].

Por fin, más recientemente, PILNIK ERRAMOUSPE sentenció: "Nuestro país ha dado un gran paso al sancionar la ley 26.388 y, con ella, ha armonizado nuestra legislación con la de varios de los miembros regionales del Mercosur. Con esta nueva ley [añade] se podrán perseguir y penar muchas conductas que, ante el vacío legal, quedaban impunes y generaban cuantiosas pérdidas económicas. Aún así [reconoce el autor], todavía resta regular la situación de todos los actores que aparecen involucrados en la interacción electrónica, ya que es a partir de una correcta distinción de qué roles cumplen cada uno, que se podrán delimitar responsabilidades"[14].

9 BON 25/06/2008.

10 Decimos "en principio" porque la introducción de algunas figuras penales ha traído como consecuencia la modificación o, aun, la ampliación del bien jurídico protegido en el título en el que aquéllas se incorporaron.

11 V. GRANERO, Horacio R., "Delitos informáticos: muchas gracias", disponible en "elDial.com", Suplemento de Derecho de la Alta Tecnología, editorial del 11/6/2008, disponible en World Wide Web: http://www.eldial.com.ar/publicador/comodin/comodin.asp?archivo-CC102A.html&pie-CC102A&titulo-Por%20Horacio%20R.%20Granero (accedido el 26 de octubre de 2010).

12 V. RIQUERT, Marcelo A., "Algo más sobre la legislación contra la delincuencia informática en Mercosur a propósito de la modificación al Código Penal Argentino por ley 26.388", p. 58, en Centro de Investigación Interdisciplinaria en Derecho Penal Económico (CIIDPE), disponible en World Wide Web: http://www.ciidpe.com.ar/area2/DELINCUENCIA%20INFORMATICA.RIQUERT.pdf (accedido el 25 de octubre de 2010).

13 Cfr. RIQUERT, "Algo más", p. 58.

14 Cfr. PILNIK ERRAMOUSPE, Franco D., "Delitos informáticos en la legislación argentina", en Actualidad Jurídica, Suplemento Penal, nº 154, octubre de 2010, p. 1234.

Expondremos sucintamente nuestra posición en las líneas finales de este texto; antes que eso, analicemos en forma breve la reforma.

1.2.2. En primer lugar, la ley modifica el **artículo 77 del Código** incorporando como últimos párrafos de esta norma los siguientes:

"El término «**documento**» comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

"Los términos «**firma**» y «suscripción» comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

"Los términos «**instrumento privado**» y «**certificado**» comprenden el documento digital firmado digitalmente".

Se trata, desde luego, de verdaderas **definiciones legales**[15], a las que el legislador recurre para precisar el alcance de los vocablos incluidos en las normas por él sancionadas.

1.2.3. Además, la ley **sustituye el artículo 128 del Código Penal**, por el siguiente:

"Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

"Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

"Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años".

La norma tipifica **tres figuras delictivas**.

Ellas se orientan a la **protección de la indemnidad sexual de los menores de dieciocho años de edad**, o sea, a la tutela del derecho de tales menores a un desarrollo de su sexualidad progresivo y libre de injerencias indebidas.

La promulgación de estos tipos legales se ve ampliamente justificada ante los cuantiosos casos de pornografía infantil que —tanto en el medio internacional como en el ámbito local— vienen teniendo lugar en los últimos tiempos, cuyas particulares modalidades comisivas demuestran que Internet se ha convertido en la vía primordial para que paidófilos intercambien imágenes y videos de niños, sin que las fronteras de los diferentes Estados nacionales les signifiquen obstáculo alguno para tal accionar.

De allí que el Código Penal deba contemplar esta nueva manifestación delictiva.

Pero, además, la inclusión de las figuras delictivas en dicho digesto posibilita que nuestro país cumpla con los compromisos adoptados por la Argentina al suscribir determinados acuerdos internacionales.

En este último sentido, conviene recordar que la **ley nacional nº 25.763** aprobó el **Protocolo Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía**, que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño —Nueva York, 1989— (de rango constitucional, según el artículo 75, inciso 22, CN).

El artículo 1 de dicho Protocolo prescribe: "Los Estados Parte prohibirán la venta de niños, la prostitución infantil y la *pornografía infantil*, de conformidad con lo dispuesto en el presente Protocolo".

Según su artículo 2, inciso c, por "pornografía infantil" se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales (artículo 2, inciso "c", del referido Protocolo).

Por último, el artículo 3 del Protocolo refiere: "Todo Estado Parte adoptará medidas para que, como mínimo, los actos y actividades que a continuación se enumeran queden íntegramente comprendidos en su legislación penal, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente: ...La producción, distribución, divulgación, importación, exportación, oferta, venta o posesión, con los fines antes señalados, de pornografía infantil, en el sentido en que se define en el artículo 2".

15 Es sabido que las **definiciones legales** son, precisamente, estipulaciones que introduce el legislador en un determinado conjunto normativo, como una forma de permitir la mejor identificación de las propias normas de dicho universo de reglas. Para un interesante estudio acerca de la función de las definiciones legales, puede verse ALCHOURRÓN/BULYGIN, "Definiciones y normas", pp. 439 y ss.

1.2.3.1. En el **primer párrafo, primera hipótesis, del artículo 128**, se consagra un delito de acción, de resultado e instantáneo, y de pluralidad de actos, mixto alternativo.

Las **conductas típicas** son las de producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir representaciones. Se advierte que la norma describe distintas *modalidades concretas de acción*, siendo indiferente que se realice una u otra, o todas ellas, por entender el legislador que no se añade mayor desvalor al injusto.

Desde que la ley establece que estos comportamientos pueden perpetrarse "por cualquier medio", sin lugar a dudas, ellos podrán ser llevados a cabo valiéndose el autor de sistemas informáticos, y a través de, por ejemplo, **correos electrónicos** o **Internet**.

Es claro, por otro lado, que la expresión "por cualquier medio" materializa a la descripción legal como tipo penal **resultativo**, en el sentido de que basta cualquier conducta que cause el resultado típico.

El **objeto material** del delito son representaciones, o sea, figuras o imágenes que se perciben con la vista, tales como los dibujos, las pinturas, las fotografías, los retratos, las películas cinematográficas, etcétera. Y esas representaciones pueden apoyarse en un soporte físico o, en lo que aquí interesa, uno *informático*. Recuérdese, en este sentido, que la ley que analizamos incorpora al artículo 77 del Código Penal una estipulación según la cual el término "documento" comprende toda representación de actos o de hechos, *con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión*.

Pero, además, la descripción típica reclama que se trate de representaciones de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas, o de sus partes genitales, con fines predominantemente sexuales.

Las figuras o imágenes, en consecuencia, deben exhibir a menores de dieciocho años, esto es, a personas que no han cumplido tal edad. Serán representaciones de menores de dieciocho años dedicados a actividades sexuales explícitas cuando en ellas se mostrare a dichos menores practicando clara y determinadamente actos de trato sexual, de deleite sexual. A su vez, consistirán en representaciones de las partes genitales de menores de dieciocho años, cuando exhiban los órganos sexuales externos (pene, testículos, vulva, clítoris, etcétera) de estos niños.

Ha de tratarse de representaciones en las que la mostración de los genitales responde a fines predominantemente sexuales, o sea, a propósitos preponderantemente relacionados con el trato sexual orientado a la obtención de placer venéreo.

La naturaleza del bien jurídico tutelado determina que la posibilidad de conocimiento de las imágenes por parte el público —publicidad— no constituya un presupuesto esencial de esta modalidad delictiva. Conviene recordar, a este respecto, que no se protege aquí el pudor público, sino el derecho de los menores de dieciocho años a un desarrollo de la sexualidad progresivo y libre de injerencias indebidas.

El **tipo subjetivo** es doloso. Admite el eventual. El autor debe tener conocimiento, o aún la mera representación, del contenido de las figuras o imágenes a producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir. También resulta suficiente la representación de la edad de los menores cuyas imágenes obtendrá.

El error, inevitable o evitable, relativo al contenido de las imágenes o la edad del sujeto pasivo elimina la tipicidad subjetiva dolosa del delito y, con ella, la punibilidad, atento la falta de previsión legal de la figura a título de imprudencia.

Sujeto activo puede ser cualquier persona.

Solo puede ser **sujeto pasivo**, en cambio, una persona de uno u otro sexo menor de dieciocho años.

El delito se **consuma** con la sola realización de las conductas típicas, esto es, con la producción, financiamiento, ofrecimiento, comercio, publicación, producción, facilitación, divulgación o distribución de representaciones de un menor de dieciocho años dedicado a actividades sexuales explícitas, o de sus partes genitales, con fines predominantemente sexuales.

Es admisible la **tentativa**.

1.2.3.2. El primer párrafo, segunda hipótesis, del artículo 128 castiga al que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren menores de dieciocho años.

Es una figura que no fue incorporada por la ley nacional nº 26.388, sino que lo preveía ya la nº 25.087, y no parece incluir elemento alguno que la vincule con la criminalidad informática.

1.2.3.3. El delito del **segundo párrafo del artículo 128** constituye un delito de tenencia que, en cuanto tal, es merecedor de fundados reproches dogmático-jurídicos por no satisfacer las exigencias elementales del principio de culpabilidad en orden a la necesidad de una acción o una omisión humana como presupuesto para la legítima imposición de una pena. Es que, en definitiva, la expresión "tener" no describe ninguna forma de conducta humana.

El **comportamiento típico**, como se acaba de anotar, es tener (el sujeto activo) en su poder determinadas re-

presentaciones, esto es, mantener materialmente tales objetos bajo el poder del agente.

El **objeto material** del delito es el mismo que el de la figura del artículo 128, primer párrafo, primera hipótesis, del Código Penal, o sea, representaciones de menores de dieciocho años dedicados a actividades sexuales explícitas o de sus partes genitales con fines predominantemente sexuales, que podrán fijarse, almacenarse o transmitirse en un soporte físico o *en uno magnético*.

No hay congruencia entre la parte objetiva del tipo y su parte subjetiva. Ello es así, puesto que la norma contiene un elemento subjetivo distinto del dolo, en virtud del cual el agente debe tener las representaciones de menores o de sus partes genitales, con fines inequívocos de distribución o comercialización. Se trata, por ello, de un delito mutilado de dos actos (especie de los delitos con tendencia interna trascendente), desde que el sujeto activo debe ejecutar la tenencia de los objetos materiales del delito teniendo en miras la realización de una actividad posterior suya. En virtud de este carácter, entonces, de alguna manera, la consumación formal del hecho típico aparece anticipada hasta la estructura de lo que, materialmente, constituye una tentativa inacabada. Concretamente, es suficiente que, en el momento de la tenencia, esté presente la intención de proceder más tarde a la distribución o comercialización de las representaciones de los menores o de sus partes genitales. Pero no hace falta que se ejecute esto último que, aunque realmente decisivo, sólo tiene que estar incluido en los propósitos del autor.

Las exigencias inherentes a este componente subjetivo distinto del dolo hacen que el tipo subjetivo de la figura sólo sea compatible con el dolo directo.

El error acerca de aquellas circunstancias que pertenecen al tipo penal excluye el dolo y, con ello, la responsabilidad.

Desde el punto de vista del sujeto activo, se trata de un tipo penal común, ya que no está limitado el ámbito de los posibles agentes: puede ser sujeto activo cualquier persona.

Sujeto pasivo sólo puede ser un menor de dieciocho años, de uno u otro sexo.

El delito se **consuma** cuando comienza la tenencia.

La figura, por su carácter de delito de tenencia, no admite la **tentativa**.

1.2.4. A su vez, la nueva ley **sustituye el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal** —que antes aludía a "Violación de Secretos"—, por el siguiente: "Violación de Secretos y de la Privacidad".

La **privacidad**, así, ha sido erigida en un **nuevo modo de ataque al bien jurídico "libertad"**, que **se añade a la violación de secretos**, como modo de ser particular de la ofensa a dicho objeto jurídico, que caracteriza a los distintos delitos comprendidos en el capítulo. En pocas palabras, hoy por hoy, la libertad penalmente protegida puede ser afectada, entre otras alternativas, mediante la violación de secretos y atentados a la privacidad.

Para acercarnos a la comprensión del concepto de "privacidad" parece conveniente realizar algunas consideraciones.

En primer lugar, cabe anotar que, bajo el título "Violación de secretos", el Código Penal resguarda todo lo que la persona desea mantener fuera del conocimiento de extraños o reducirlo al conocimiento de un número limitado, ya se trate de sus pensamientos, sus acciones o acontecimientos o circunstancias que le conciernan[16].

Conforme la doctrina jurídica prácticamente unánime, lo que la violación de secretos tutela es esa "**esfera de intimidad**" del ser humano[17].

En la Constitución Nacional, este derecho a la intimidad "...está principalmente presupuesto por el art. 18, cuando establece que «el domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación»"[18].

Lo protegido bajo el concepto de **intimidad** es, todo aquello que integra el ámbito de la vida privada de las personas "aun cuando no sea secreto", que se tiene derecho a proteger de cualquier intromisión indeseada.

16 Cfr. CREUS, Carlos/BUOMPADRE, Jorge Eduardo, *Derecho penal. Parte especial*, 7ª edición actualizada y ampliada, Astrea, Buenos Aires, 2007, t. 1, p. 382.

17 V., por todos, NÚÑEZ, Ricardo C., *Derecho penal argentino*, Editorial Bibliográfica Argentina - Bibliográfica Omeba, Buenos Aires, 1967, t. V, p. 95.

18 V. NINO, Carlos Santiago, *Fundamentos de derecho constitucional. Análisis filosófico, jurídico y politológico de la práctica constitucional*, 1ª edición, 1ª reimpresión, Astrea, Buenos Aires, 2000, p. 333.

19 Los juristas aluden aquí a "privacidad", y no a "intimidad", pero, en nuestra opinión, es a éste último concepto al que se aplican las afirmaciones que ellos realizan, y que nosotros transcribimos en el texto principal.

20 V. ABOSO, Gustavo E./ZAPATA, María Florencia, *Cibercriminalidad y Derecho penal*, B de f, Montevideo - Buenos Aires, 2006, p. 119.

En este sentido, y con mayor profundidad, ABOSO y ZAPATA señalan que la intimidad[19] de una persona se vincula directamente con una razonable expectativa de reserva de las proyecciones de nuestra personalidad que constituyen el ámbito nuclear donde la persona puede desarrollar su plan de vida[20]. Pero ella no se limita únicamente a las personas, sino que alcanzas muchas veces zonas compartidas (v. gr., el núcleo familiar y el domicilio) donde las personas puedan llevar adelante proyectos comunes, como así también ciertas relaciones profesionales (relación médico/paciente, cliente/abogado, etc.) y, en la actualidad, el uso de determinados sistemas o medios de comunicación masivo[21].

Pues bien, como antes se ha subrayado, a la intimidad, así entendida, el capítulo agrega la privacidad, como modo de ofensa a la libertad individual merecedor de específica previsión legal.

Debe quedar claro, pues, que uno y otro concepto **deben diferenciarse**[22], aun cuando en los mismos antecedentes parlamentarios que precedieron a la sanción de la ley nacional nº 26.388 ellos hayan sido tratados con poca precisión o, incluso, directamente confundidos.

La separación de estos conceptos surge necesaria como una elemental derivación del principio interpretativo según el cual *donde la ley distingue, el intérprete debe distinguir*.

No se nos pasa por alto que, antes de la reforma[23] —e incluso después—, ciertos juristas **han equiparado las nociones de "intimidad" y "privacidad"**[24]. Pero, para nosotros, la inclusión de la privacidad **a la par** de una expresión como la de "violación de secretos", que unánimemente se reconoce como individualizadora de una ofensa a la intimidad, impone la diferenciación.

Hay quienes, como GELLI, que aducen que el derecho de la **intimidad se desprende del de privacidad** protegido por el **artículo 19** de la Constitución Nacional, pero no se confunde con éste último; no obstante, esta constitucionalista también analiza el derecho a la intimidad en el contexto del artículo 18 de la ley suprema[25].

---

21 Cfr. ABOSO/ZAPATA, *Cibercriminalidad*, p. 119.

22 Lo entiende también así, por ejemplo, el vocal Pérez Barberá, de la Cámara de Acusación de Córdoba, en su voto minoritario en el precedente "**Bondone**" (Sent. nº 49, del 29/10/2010).

23 Parece ser el caso de NÚÑEZ, *Derecho penal argentino* (t. V, p. 95), quien alude a "esfera de intimidad o de reserva".

24 El mismo ordenamiento jurídico suele emplear los conceptos de "intimidad" y "privacidad" como sinónimos. Parece ser éste el caso de la **Constitución de la Provincia de Córdoba**, cuyo **artículo 50**, bajo la rúbrica "**Privacidad**", refiere: "Toda persona tiene derecho a conocer lo que de él conste en forma de registro, la finalidad a que se destina esa información, y a exigir su rectificación y actualización. Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando tengan un interés legítimo. La ley reglamenta el uso de la informática para que no se vulneren el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos".

25 V. GELLI, María Angélica, *Constitución de la Nación Argentina. Comentada y concordada*, La Ley, Buenos Aires, 2001, pp. 182 y ss., y 161 y ss.

26 CSJN, 11/12/1984, "**Ponzetti de Balbín**", *Fallos*, 306:1892. En este pronunciamiento, el cimero tribunal federal expresaba: "El **derecho a la privacidad e intimidad** se fundamenta constitucionalmente en el art. 19 de la ley suprema. En relación directa con la libertad individual protege jurídicamente un ámbito de autonomía individual constituida por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o actos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad" (la negrita y la bastardilla son nuestras). Para una mayor corroboración de nuestro aserto en el texto principal, v. considerandos 5º y 8º.

27 CSJN, 20/04/2010, "**Baldivieso**", publicado en La Ley, 26/05/2010, p. 7.

28 La ministra argumenta: "La intimidad o privacidad, entendida en sentido lato, se encuentra protegida por nuestro derecho vigente con desigual intensidad según cuál sea el aspecto de la vida privada que se busca resguardar; no es el mismo tipo de aseguramiento el que provee el artículo 19 de la Constitución Nacional que el resultante del artículo 18 y otras cláusulas, que establecen fórmulas similares, de los pactos de derechos humanos incorporados por el artículo 75, inciso 22 de la Constitución Nacional. El primero de los preceptos mencionados está dirigido a excluir de todo tipo de interferencia estatal aquellas acciones que en modo alguno afecten a terceros, es decir, que no generen efectos dañosos sobre otras personas. En la medida que esto último haya sido debidamente establecido, la prohibición de interferir en tal tipo de acciones es absoluta. La protección acordada por el artículo 18 de la Constitución Nacional se refiere a la exclusión de terceros (los funcionarios públicos entre ellos) de ciertos ámbitos propios de la persona, a los que también se puede llamar "privados" o "exclusivos". Por antonomasia, cae en esta categoría el domicilio o vivienda, pero también incluye el artículo 18 de la Constitución Nacional a los papeles privados y a la correspondencia epistolar. A diferencia de la protección asignada por el artículo 19 de la Constitución Nacional, la interferencia en estos ámbitos privados por parte de las autoridades públicas no se halla excluida de manera absoluta, sino que se la sujeta a determinados requisitos, tal como la orden de autoridad competente".

29 Quizás por su mayor plausibilidad dogmático-jurídica y porque aporta más claridad conceptual.

La Corte Suprema de Justicia de la Nación, en el precedente "**Ponzetti de Balbín**"[26], ha **equiparado implícitamente intimidad a privacidad**. Sin perjuicio de esto, es pertinente que, en el reciente caso "**Baldivieso**"[27], el Alto Cuerpo federal, al menos en el voto de la ministra Argibay[28], adhiere expresamente[29] a una concepción según la cual **deben distinguirse nítidamente** los conceptos de "intimidad" y "privacidad".

Es ésta, justamente, y como hemos visto, la interpretación que postulamos: intimidad y privacidad son **dos nociones que merecen una clara diferenciación**.

Mientras que la intimidad se muestra como aquel conjunto de cuestiones que el ser humano tiene derecho a mantener en una zona de reserva, el "bien de la **privacidad**" se relaciona —conforme aduce NINO— con el derecho que tienen los ciudadanos a que no se los moleste por "...las acciones voluntarias que no afectan a terceros"[30], y encuentra su fundamento constitucional en la primera parte del artículo 19 de la Constitución Nacional, que dice: "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados".

Con todo, es inconcuso que las **nuevas tecnologías han elevado los riesgos** para el **derecho a la intimidad y a la privacidad**.

En la actualidad, existen cientos de bases de datos con información propia del ámbito de la vida privada de las personas, y sus huellas e imágenes digitales quedan registradas en profusos lugares en la Web, videocámaras de ingreso a edificios, tarjetas de acceso a oficinas, correos electrónicos, comunicaciones por chat, búsquedas en Internet y mensajes de texto telefónicos (SMS).

No obstante que se han aprobado marcos legales para ponerle límite al uso que se haga de estos datos —tales como, por ejemplo, el **habeas data** pergeñado en la reforma constitucional del año 1994[31], la **ley nacional nº 24.766**[32] y la **ley nacional nº 25.326**[33]—, incesantemente aparecen nuevos casos de robo de identidad, sustracción de información personal o venta masiva de bases de datos personales.

El Derecho penal no puede quedar al margen de este estado de cosas. La legislación criminal debe escoltar estos avances con normas adecuadas a la realidad tecnológica de hoy.

1.2.5. La ley nacional nº 26.388 **reemplaza el artículo 153 del Código Penal** por el siguiente:

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

"En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

"La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

"Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

Con relación al delito de **violación de correspondencia**, la reforma actúa en *dos direcciones*.

En primer lugar, la ley de reforma agrega a las figuras existentes de violación de correspondencia el término "**comunicación electrónica**". Amplía, pues, el objeto material del delito de violación de correspondencia,

30 NINO, *Fundamentos*, t. 1, p. 304.

31 El artículo 43 de la Constitución Nacional prescribe: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

32 Ella, publicada en BON el 30/12/1996, deja "sujeto a la responsabilidad que correspondiera conforme con el Código Penal" (artículo 12) a quienes incurrieren en infracciones contra la **confidencialidad** de la información comercial en poder de personas físicas o jurídicas.

33 Este conjunto normativo, sancionado el 4/10/2000, incorpora como artículo 157 bis del Código Penal, el siguiente: "Será reprimido con la pena de prisión de un mes a dos años el que: 1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere 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".

esto es, el objeto sobre la que ha de recaer físicamente la acción que tipifica dicha infracción.

De este modo, se han actualizado los tipos legales y ha quedado resuelto el problema de la **atipicidad de la violación de correspondencia electrónica**.

Por "**comunicación electrónica**" debe entenderse todo mensaje enviado por un remitente a un destinatario, a través de un sistema electrónico[34]. Quedan incluidos los mensajes de correo electrónico, los *chats*, los fax, las llamadas a través de VoIP (*Voice over Internet Protocol*)[35] o un mensaje de texto (SMS) remitido de un celular a otro. Su contenido puede consistir en la voz, caracteres alfanuméricos o signos y gráficos de diversa índole que permiten algunos sistemas informáticos.

La comunicación es tal "asegura PALAZZI", tanto mientras está en tránsito como cuando queda almacenada en un casillero de mensajes, bandeja de entrada, contestador automático analógico o digital, o *voicemail*[36].

Algunos tribunales habían considerado atípicas las acciones realizadas sobre correos electrónicos, y si bien en el caso "**Lanata**" (Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala VI, 4/3/1999) se concluyó que el correo electrónico podía ser equiparado a la correspondencia tradicional en los términos de los artículos 153 y 155 del Código Penal, la lectura del fallo parecía dar la idea de un empleo de la analogía en el ámbito del Derecho penal[37], y ésta, como es sabido, es inadmisible en dicho terreno cuando conduce a resultados desfavorables para el imputado.

En segundo término, la ley nacional nº 26.388 añade un último párrafo al artículo 153 para dar sustento a una figura cualificada en la que el mayor reproche deriva de que la comisión del delito por parte de un funcionario público que abusa de sus funciones deteriora la confianza pública en el correcto desempeño de tales funcionarios.

Se materializa, así, un **delito especial impropio**, es decir, una figura que guarda correspondencia con el tipo común de los párrafos 1°, 2° y 3° del artículo 153, del que puede ser autor un sujeto no cualificado. En el tipo legal del párrafo 4°, es decisivo el deber especial —y no una posición del autor en sí—, de la que surge el deber. Los caracteres particulares del autor se emplean, aquí, para agravar la punibilidad para el sujeto específico.

Podría decirse que la comisión del delito por parte del sujeto especial defrauda específicas expectativas normativas que forman parte del rol que —en su condición de tal— desempeña el funcionario público[38]. La

34 Con buen tino, PALAZZI postula que la interpretación de lo que constituye "comunicación electrónica" debe llevarse a cabo "... de acuerdo al desarrollo actual de las comunicaciones. Hoy en día [aduce este autor], las comunicaciones no ocurren sólo entre dos personas sino también entre varias e incluso con máquinas. Por ejemplo, el banco puede enviar un resumen de cuenta a la casilla de correo electrónico del cliente, el diario *online* envía un resumen de noticias, un servidor comunica al usuario si el mensaje anterior que envió llegó o no a destino, el servidor de la universidad avisa de eventos a sus alumnos, o que el casillero se está por llenar y debe vaciarlo. Todas {estas son comunicaciones electrónicas, pues que se comunica algo a un tercero. ¿Tiene que intervenir una persona? Si entendemos que por lo menos debe haber un emisor o destinatario humano, muchas situaciones quedarán fuera de la protección penal. Pero hoy en día [enfatiza PALAZZI] la relación con numerosas empresas y sistemas está automatizada a través de ordenadores, y con ellos también hay comunicación" (cfr. PALAZZI, Pablo A., *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, Abeledo Perrot, Buenos Aires, 2009, p. 75).

35 Es un tipo de hardware y software que permite a la gente utilizar Internet como medio de transmisión de llamadas telefónicas, enviando datos de voz en paquetes, usando el IP en lugar de los circuitos de transmisión telefónicos. Dicho "IP", o *Internet Protocol*, consiste en un número único e irrepetible que identifica a cada ordenador que accede a la red en determinado momento.

36 V. PALAZZI, *Los delitos informáticos*, p. 75.

37 Es que la resolución expresaba: "...el correo electrónico posee características de protección de la privacidad más acentuadas que la inveterada vía postal a la que estábamos acostumbrados, ya que para su funcionamiento se requiere un prestador del servicio, el nombre del usuario y un código de acceso que impide a terceros extraños la intromisión en los datos que a través del mismo puedan emitirse o archivarse. Sentadas estas bases preliminares, nada se opone para definir al medio de comunicación electrónico como un verdadero correo en versión actualizada. En tal sentido, la correspondencia y todo lo que por su conducto pueda ser transmitido o receptado, goza de la misma protección que quiso darle el legislador al incluir los arts. 153 al 155 en la época de redacción del Código sustantivo, es decir, cuando aún no existían estos avances tecnológicos" (Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala VI, 4/3/1999, "**Lanata**").

38 Cfr. JAKOBS, Günther, "Sobre el tratamiento de los defectos volitivos y de los defectos cognitivos", en JAKOBS, Günther, *Estudios de derecho penal*, traducción de Enrique Peñaranda Ramos, Carlos Suárez González y Manuel Cancio Meliá, UAM Ediciones - Editorial Civitas, Madrid, 1997, p. 129. El jurista alemán aduce que "...los seres humanos viven, en la medida en que lo hagan en sociedad, en un mundo *socialmente* configurado de una determinada manera; tienen un *status* especial..., y vienen definidos, por tanto, por un haz de derechos y deberes". Uno de los fundamentos de la responsabilidad penal "...es la inobservancia de los límites trazados por ese *status* especial" (v. JAKOBS, Günther, "La competencia por organización en el delito omisivo. Consideraciones sobre la superficialidad de la distinción entre comisión y omisión", en JAKOBS, *Estudios*, pp. 347 y 348).

conducta del agente, en síntesis, vulnera deberes que afectan tan sólo a personas con un status especial o, con mayor precisión, forman parte de un status especial.

1.2.6. Igualmente, la reforma **incorpora al Código Penal un artículo 153 bis** que expresa:

"Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

"La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

Es el delito de **acceso ilegítimo a un sistema informático**.

Se lo llama también **intrusismo informático no autorizado** o ***hacking***[39], y supone vulnerar la confidencialidad de la información en sus dos aspectos: la exclusividad y la intimidad.

Por lo demás, él constituye una **modalidad propia** de ilicitud informática, porque el tipo legal describe una conducta que sólo puede verificarse en relación con un sistema de tratamiento automatizado de datos o una representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático, los que aparecen como **objeto del delito**.

Precisamente, el texto legal hace referencia a "sistema o dato informático de acceso restringido". Éste es, entonces, el **objeto material sobre el cual recae la conducta típica**.

Sistema informático es todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

A su vez, el *dato informático* consiste en toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.

En los términos de la descripción legal, uno y otro deben ser "de acceso restringido", o sea, de acceso acotado o circunscripto a determinadas personas; no se prohíbe, pues, el acceso a sistemas o redes informáticas abiertas, o al contenido publicado en un sitio de Internet público.

Es un delito de **acción**, de **resultado**, **instantáneo** y, como acaba de verse, **resultativo**.

La **conducta típica** consiste en *acceder* a un sistema o dato informático de acceso restringido, es decir, entrar al sistema o conocer el dato.

En razón de ser un tipo resultativo, el acceso puede lograrse "por cualquier medio", sea éste **remoto** —utilizando el sujeto activo las redes públicas de telefonía o transmisión de datos— o **directo** —sentándose el autor frente a una computadora e ingresando a ella tomando conocimiento de su contenido, leyendo el "dato" que está en la pantalla, o copiando archivos o software para acceder después a su contenido[40]—.

En el **tipo normativo** se advierte la existencia de un **elemento normativo jurídico expresivo de un eventual tipo de justificación genérica concurrente**, pues, a diferencia de los tipos penales comunes, aquí el precepto penal reconoce y anuncia que la posible concurrencia de una causa de justificación genérica (prohibición, mandato o permiso fuerte), excluyente del tipo prohibitivo o preceptivo, no es excepcional. Es que el acceso debe darse *sin la debida autorización o excediendo la que posea* el sujeto activo.

El **tipo subjetivo** es doloso presupone que el sujeto activo conozca que está realizando un acceso ilegítimo al sistema o dato informático de acceso restringido, y que tenga voluntad de ejecutarlo. Reclama, pues, el dolo directo.

Pero, además, la descripción legal incluye un **elemento subjetivo cognitivo distinto del dolo**, ya que el agente debe realizar el comportamiento prohibido *a sabiendas*. Es un **componente subjetivo expreso, que fuerza el dolo directo**, desde que exige un conocimiento superlativo de lo esencial de la parte objetiva del tipo legal, agudizando lo meramente doloso hasta transformarlo en directo.

Sujetos activo y **pasivo** del injusto pueden ser cualquier persona.

El delito se **consuma** con el ingreso al sistema informático o el conocimiento del dato informático de acceso restringido, y admite la tentativa. El ingreso

39 Para un interesante texto sobre la evolución del *hacking* y las distintas versiones de la "cultura *hack*", v. COLEMAN, Gabriella, "The Anthropology of Hackers", en The Atlantic, disponible en World Wide Web: http://www.theatlantic.com/technology/print/2010/09/the-anthropology-of-hackers/63308/(accedido el 2 de noviembre de 2010).

40 V. PALAZZI, *Los delitos informáticos*, pp. 103 y 104.

al sistema o el conocimiento del dato son el resultado que consuma el delito, sin que tal resultado determine la creación de una situación antijurídica duradera. Es que, como hemos anotado, se trata de una tipo penal instantáneo.

La figura esta sometida a un régimen de *subsidiariedad* expresa y relativa. Se aplica *si no resultare un delito más severamente penado*. Esta hipótesis se da cuando el intrusismo informático no autorizado es un elemento integrante del tipo de otra figura o cuando el mismo hecho constituye el *corpus* del delito más grave. No se produce el desplazamiento si el otro delito tiene una pena inferior al del acceso ilegítimo a un sistema informático. Si éste, por fin, es un hecho distinto del otro delito, los dos hechos operan en concurso real.

Un interrogante de especial importancia es el relativo a la posibilidad de aplicar esta disposición legal al ***ethical hacking*** o a las tareas que —mediante herramientas de software dedicadas a tal fin— desarrollan los expertos en seguridad informática para determinar las eventuales falencias de las redes.

Es que la denotación de la voz "*hacking* ético" comprende actividades tan variadas como, por ejemplo, la investigación académica, doméstica o empresarial sobre virus informáticos; y la labor de empresas de seguridad que testean sistemas de bloqueo y *firewalls* (programas que sirven para filtrar lo que entra y sale de un sistema conectado a una red), entre muchos otros usos que pueden revestir estas manifestaciones de *ethical hacking*.

Sin arriesgar respuestas definitivas en torno a esto, parece innegable que, en la práctica, si el *hacking* ético se lleva a cabo con consentimiento del dueño o titular de la red que está siendo analizada (p.ej., a través de un contrato de servicios de seguridad informática), existe una autorización legal por parte del "ofendido", que excluye el elemento del tipo legal que exige que el acceso se realice "sin la debida autorización o excediendo la que posea".

1.2.7. El conjunto normativo que examinamos **sustituye el artículo 155 del Código Penal**, por el siguiente:

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

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

Como puede apreciarse, se actualiza el delito de **publicación indebida** del artículo 155 empleando la misma técnica legislativa del artículo 153 reformado, es decir, agregando el giro lingüístico "**comunicación electrónica**" al elenco de objetos materiales del delito.

Hemos visto ya que la "**comunicación electrónica**" es el mensaje enviado por un remitente a un destinatario, a través de un sistema electrónico.

No sólo es reprochable violar la privacidad de una correspondencia mediante su acceso o interceptación; también lo es el publicar el contenido de una carta o correo electrónico destinados a permanecer en la esfera íntima de las personas, y no a ser divulgado.

La **acción típica**, pues, es la de *hacer publicar* la correspondencia, comunicación electrónica, pliego cerrado, o despacho telegráfico, telefónico o de otra naturaleza, esto es, la de difundir por medio de la imprenta o de otro procedimiento cualquiera.

De allí que la ley nacional nº 26.388 *aggiorne* la norma del artículo 155 del Código Penal sancionando a quien *indebidamente* publique tanto una correspondencia tradicional como una digital. La disposición legal incluye un **elemento normativo jurídico expresivo de un eventual tipo de justificación genérica concurrente**. Es que, al demandar que la publicación sea "indebida", el precepto penal reconoce y anuncia que la posible concurrencia de una causa de justificación genérica (prohibición, mandato o permiso fuerte), excluyente del tipo prohibitivo o preceptivo, no es excepcional.

Desde el punto de vista de la intensidad de ataque al objeto material del bien jurídico, el delito es **de peligro hipotético** o **potencial**, habida cuenta que el tipo legal incorpora un elemento normativo de valoración sobre la potencialidad lesiva de la acción del agente, cuya concurrencia habrá de ser constatada por el órgano jurisdiccional pertinente. Es que la publicación indebida se castiga sólo "*si el hecho causare o pudiere causar perjuicios a terceros*".

Por lo demás, el último apartado de la regla consagra una **causa de justificación específica** "con cierta

41 Cfr. NAVARRO, Guillermo Rafael/BÁEZ, Julio C./AGUIRRE, Guido J., "Artículo 155", en AAVV, *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, David Baigún/Eugenio Raúl Zaffaroni (dirección), Marco A. Terragni (coordinación), Hammurabi, Buenos Aires, 2008, t. 5, p. 761.

semejanza a la del art. 111 [del Código Penal] y que, como dicho precepto, disipa la antijuricidad del hecho"[41]; ella exime de responsabilidad penal a quien revela una correspondencia cuyo contenido es de palmario interés público.

La alocución "**interés público**" designa lo que es de utilidad para todos los habitantes, ya del país todo, ya de una comunidad regionalmente determinada.

1.2.8. Por virtud de la ley de reforma, se ve **sustituido el artículo 157 del Código Penal**, por el siguiente:

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

El legislador añade el término "datos" a la anterior redacción de la norma para poner al día a la figura delictiva y proteger penalmente la información que está en poder de la administración pública y que, por ser secreta, no debe ser revelada a terceros.

Una vez más, la ley opta por ampliar el **objeto sobre el cual recae la conducta típica**.

De tal suerte, el reproche penal recaerá sobre quien *descubriere, manifestare o diere a conocer*, no sólo hechos, actuaciones o documentos secretos, sino también "datos" secretos, vale decir, representaciones de hechos, manifestaciones o conceptos secretos, contenidos en un formato físico o, incluso —y en lo que interesa a los fines de la cibercriminalidad— magnético.

1.2.9. Asimismo se ha **sustituido el artículo 157 bis del Código Penal**, por el siguiente:

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

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

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

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

"Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años".

A la par de esto, se deroga el inciso 1° del artículo 117 bis del Código Penal, que señalaba: "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".

Se consideró de apropiada técnica legislativa unificar en una sola norma las hipótesis de los artículos 117 bis, inciso 1°, y 157 bis del Código Penal, porque existía coincidencia en que la primera de estas disposiciones en ciertos casos no protegía el honor, pese a su ubicación en el Título 2 del Libro Segundo del digesto criminal.

Es indudable que todo acceso cognitivo no autorizado a un banco de datos reservado, importa una lesión al derecho a la "intimidad" y la "privacidad" de la persona física o de existencia idea que es titular de los datos.

Como acertadamente aducen DE LANGHE y REBEQUI, el Código Penal tipifica aquí varios delitos "... que tienen como nota común el que en ellos se protege la voluntad de una persona de que no sean conocidos determinados hechos que sólo deben quedar reservados a ella o a un círculo reducido de personas, es decir, que pueden ser calificados de *secretos*, y también el derecho de la persona a controlar cualquier información o hecho que afecte su vida privada y... su *intimidad*"[42].

1.2.10. La ley nacional nº 26.388 instituye el delito de **fraude informático**[43].

Lo hace incorporando como **inciso 16 del artículo 173 del Código Penal**, el siguiente texto:

"El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

Se pretendió, así, despejar definitivamente las dudas suscitadas en los tribunales sobre en qué tipos legales (de los delitos contra la propiedad) debe subsumirse la conducta.

---

42 *Vid.* DE LANGHE, Marcela/REBEQUI, Julio M., "Artículo 157 bis", en AAVV, *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, David Baigún/Eugenio Raúl Zaffaroni (dirección), Marco A. Terragni (coordinación), Hammurabi, Buenos Aires, 2008, t. 5, p. 811.

43 Un prolijo estudio de esta figura delictiva, puede verse FÍGARI, Rubén E., "Reflexiones sobre la defraudación informática (ley 26.388)", en "elDial.com", Suplemento de Derecho de la Alta Tecnología, Sección Doctrina, 12/8/2009, disponible en World Wide Web: http://www.eldial.com.ar/bases/sql/ver_rl_ttt.asp?id-4500&base-50&Numingr-1 —elDial.com - DC1170— (accedido el 4 de noviembre de 2010).

44 V., *mutatis mutandis*, FARALDO CABANA, Patricia, "Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática", en Eguzkilore, nº 21, San Sebastián (España), diciembre de 2007, p. 36, disponible en World Wide Web: http://www.

En la nueva regla, el legislador equipara a la estafa, y a efectos meramente penológicos, una conducta que carece de alguno o varios de los elementos propios de la estafa común, no siendo posible, por lo tanto, acudir al concepto de estafa que recoge el artículo 172 del Código Penal para interpretarlas[44]. En todo caso, esta última figura genérica podrá servir como punto de **contraste y comparación**, para compararla con la regulación del fraude informático incluida en el nuevo artículo 173, inciso 16.

La descripción del artículo 173, inciso 16, materializa un delito de **medios determinados**, de **resultado** e **instantáneo**, que puede cometerse a través de **una acción o una omisión**, cuando el sujeto activo ocupa una posición de garante que lo responsabiliza por la producción de un resultado al no intervenir en el curso causal.

Es, además, un delito **informático propio**, en tanto puede concebirse sólo en relación con un sistema informático, el que, en esta infracción, opera como *medio para perpetrar el ilícito*.

La **conducta típica** consiste en *defraudar*, lo que, en el contexto del Capítulo 4 ("Estafas y otras defraudaciones") del Título 6 ("Delitos contra la propiedad") del Libro Segundo del Código Penal significa *perjudicar patrimonialmente a un tercero mediante fraude*.

No es suficiente que el agente defraude a otro valiéndose de cualquier conducta, sino que es necesario que lo haga **mediante** una *técnica cualquiera de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos*. El sujeto activo debe, pues, **operar un ordenador** y, con ello, modificar el correcto funcionamiento de un dispositivo que realiza el tratamiento automatizado de datos o la misma transferencia de los datos.

Dicha alteración del normal funcionamiento del sistema informático o la transmisión de datos se verifica cuando se *modifica internamente el sistema* o, sin hacer esto, se *hacen variar los efectos del sistema* mediante el ingreso, la modificación o la supresión de datos —frecuentemente, datos de identidad— con los cuales aquél debe funcionar conforme fue programado. En este último supuesto, puede tratarse de la introducción de **datos falsos** o del ingreso, modificación o supresión indebida, por no autorizada, de **datos reales, auténticos**, como así también de la manipulación de los **ya contenidos en el sistema** en cualquiera de las fases de proceso o tratamiento informático.

Quedan comprendidos en estas hipótesis los casos de *superación de los controles de cliente* mediante *cookies* falsificados o datos capturados en formularios *web*, los *ardides en la autenticación* requerida para ciertas operaciones a través del aprovechamiento de un defecto en la función "olvidó su *password*" y los *ataques relacionados con el control de acceso* a un sitio *web*, entre otros.

El **tipo subjetivo** es doloso y requiere dolo directo. Es que, la propia idea de "defraudar" supone la intencionalidad del agente dirigida a la finalidad de lograr el perjuicio patrimonial de un tercero.

Cualquier persona puede ser **sujeto activo** o **pasivo del delito**.

El **resultado** se plasma en la producción de un *perjuicio patrimonial*, pues este último es consustancial a la noción de "defraudar" como conducta delictiva que ofende la propiedad ajena. Este perjuicio tiene lugar cuando disminuye el valor del patrimonio, ora mermando su activo, ora aumentando su pasivo.

Puesto que es un delito instantáneo, se consuma en el momento en que se produce el resultado, sin que éste determine la creación de una situación antijurídica duradera.

Hemos anotado que, en relación con el fraude informático, el tipo genérico de la estafa del artículo 172 del Código Penal muestra utilidad como *piedra de toque* para apreciar las **similitudes y diferencias** entre una y otra figura.

Pues bien, tradicionalmente se ha aseverado que, para que se cometa el delito de estafa, debe existir un *ardid o engaño* del autor, que haya inducido a un tercero en *error* determinante de una *disposición de propiedad pecuniariamente perjudicial* para él o para otro. Sin error —se decía— no hay estafa, así como no la hay sin ardid, aun cuando mediante alguna maniobra se logre un beneficio indebido. Por esto —se enfatizaba—, el que utilizando una moneda falsa u otro medio ingenioso logra sacar de un aparato automático de venta el artículo que éste contiene, no comete estafa, sino hurto, porque aun cuando exista maniobra no existe ninguna mente errada.

Frente a la estafa común, el fraude informático **carece de la exigencia de los elementos de "engaño" y de "error"**, a lo que se suma que el acto de dispo-

ivac.ehu.es/p278-content/es/contenidos/boletin_revista/eguzkilore_num21/es_numero21/adjuntos/02%20Faraldo.indd.pdf (accedido el 31 de octubre de 2010).

sición patrimonial **no es realizado por la víctima de un engaño** —como en la estafa común—, sino por el propio autor del delito, a través del sistema informático. Es consustancial al fraude informático que se trate de una disposición "no consentida", elemento que no está presente en la estafa común, porque allí el acto de disposición lo realiza el sujeto pasivo del delito en perjuicio propio, con consentimiento viciado por el error, o el sujeto pasivo de la acción en perjuicio de tercero, siendo irrelevante que el tercero que sufre el perjuicio haya consentido o no. El hecho de que nos encontremos aquí ante una conducta subrepticia, que da lugar a una transferencia de activos patrimoniales realizada sin consentimiento del titular —asegura FARALDO CABANA— "...aproxima la forma de comisión de esta figura delictiva más al hurto que a la estafa"[45].

1.2.11. También se creó la figura del **daño informático**[46].

Se lo llama también **sabotaje informático** o ***cracking***.

En efecto, la ley incorpora como **segundo párrafo del artículo 183 del Código Penal**, el siguiente:

"En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

La disposición legal prevé dos figuras delictivas diferentes, a saber: la alteración, destrucción o inutilización de productos informáticos, y la venta, distribución o introducción en un sistema informático de programas destinados a causar daños.

A su vez, en el **inciso 6 del artículo 184** se incorpora una agravante del daño, según la cual éste será más severamente penado cuando mediante la siguiente circunstancia: "Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

1.2.11.1. La primera hipótesis consagra un delito **de acción**, **de resultado**, **resultativo**, **instantáneo** y de **pluralidad de actos, mixto alternativo**.

Por lo demás, se trata de un **delito informático impropio**, pues prevé un injusto —el daño— que no sólo puede perpetrarse en relación con un sistema informático, sino también respecto de cosas muebles o inmuebles, o animales (artículo 183 CP).

Las **conductas típicas** son las de *alterar*, *destruir* o *inutilizar* datos, documentos, programas o sistemas informáticos.

Altera dichos objetos quien los cambia o modifica; los *destruye*, quien los deshace, los rompe o les ocasiona un grave daño; y los *inutiliza*, quien los vuelve ineptos para cumplir su función.

Puede advertirse que el legislador prevé tres comportamientos distintos, pero **es indiferente que se realice una u otra acción, o todas ellas**, por entenderse que no se añade mayor desvalor al injusto.

La figura es abierta en cuanto a los medios que deben causar el resultado típico. De tal suerte, podrá lograrse la alteración, destrucción o inutilización mediante **virus informático**[47], **Caballos de Troya**[48], "**gusanos**"[49], ***cancer routines***[50], **bombas lógicas**[51] y **otras amenazas similares**. Es frecuente que el sujeto activo, para acceder al dato, documento, programa o

45 V. FARALDO CABANA, "Los conceptos", pp. 36 y 37.

46 Un detenido análisis de esta figura delictiva, puede verse FÍGARI, Rubén E., "Daño informático (arts. 183, 2º párr. y 184 incs. 5º y 6º del CP Ley 26.388)", en "elDial.com", Suplemento de Derecho de la Alta Tecnología, Sección Doctrina, 9/9/2009, disponible en World Wide Web: http://www.eldial.com.ar/bases/sql/ver_rl_ttt.asp?id-4556&base-50&Numingr-1 —elDial.com - DC11A8— (accedido el 4 de noviembre de 2010).

47 Por "**virus informático**" se entiende aquel *software* malicioso que tiene por objeto alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario.

48 Los llamados "**Caballos de Troya**" consisten en la *introducción de una rutina no autorizada dentro de un programa de uso habitual*, provocando que el programa actúe en las ocasiones que define el manipulador de forma distinta a como debía, realizando operaciones no previstas, tales como, por ejemplo, las de borrar ficheros, alterar datos, ordenar pagos o bloquear el sistema.

49 Los "**gusanos informáticos**" son programas que, sin alterar los archivos de programas, se alojan en la memoria de un ordenador y tienen la *propiedad de duplicarse a sí mismo, con la frecuente consecuencia de causar problemas en la red*, a veces simplemente consumiendo ancho de banda.

50 Las "**cancer routines**" son programas maliciosos o destructivos que tienen la particularidad de que *se reproducen, por sí mismos, en otros programas*, arbitrariamente escogidos.

51 Las "**bombas lógicas**" son una *parte de código insertada intencionalmente en un programa informático y que permanece oculto hasta cumplirse una o más condiciones* preprogramadas, verificadas las cuales se ejecuta una acción maliciosa, como —por ejemplo— el borrado de archivos.

sistema informático, y dañarlo, emplee las llamadas "***backdoors***" o "puertas traseras", que son métodos que permiten eludir los procedimientos normales de autenticación a la hora de conectarse a una computadora.

Los **objetos de la acción** pueden ser un *dato*, un *documento*, un *programa* o un *sistema informático*.

Hemos visto ya que, por *dato informático* debe interpretarse toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.

Documento informático es toda representación de actos o hechos, fijada, almacenada, archivada o transmitida utilizándose un soporte magnético o informático.

Por otro lado, el *programa informático* consiste en un conjunto de instrucciones o comandos que, que una vez ejecutados, realizarán una o varias tareas en un ordenador.

Finalmente, el *sistema informático* es todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

Esta figura delictiva ha venido a llenar el **vacío que presentaba el tipo penal de daño** (artículo 183 CP) que sólo contempla las cosas muebles, y dejaba fuera de su ámbito de aplicación al daño producido sobre **bienes intangibles**.

Así, al incluir los datos, documentos, programas y sistemas informáticos como objeto de delito de daño, se logra penalizar todo ataque, borrado, destrucción o alteración intencional de dichos **bienes inmateriales**.

Es sabido que el delito de daño del artículo 183, así como el de hurto (artículo 162 ibídem), tienen como objeto material del ilícito una *cosa mueble ajena*.

Una *cosa* es un objeto corporal susceptible de tener un valor (artículo 2311 CC).

Un *objeto* es corpóreo cuando es *material*, y esta cualidad, por su parte, se satisface con la posibilidad de que el objeto pueda ser detectado materialmente.

Con arreglo a la reforma de la ley civil efectuada por la ley 17.711 (artículo 2311, párrafo 1°, CC), quedan comprendidos dentro del concepto de *cosa*, los sólidos, líquidos, fluidos, gases y la energía —cualquiera que sea su naturaleza— en cuanto sea detectable materialmente y, como tal, pueda pertenecer a un patrimonio.

Lo expuesto permitiría postular que la información computarizada sea considerada como una nueva forma de energía, a la cual corresponde aplicar el régimen de las cosas (artículo 2311 CC).

Sin embargo, debe reconocerse que el legislador, al tiempo de elaborar la figura penal que castiga el daño[52], no tuvo en consideración, como objeto material del ilícito, al dato informático.

De tal suerte, aun cuando la aceptación del dato informático como objeto material de la figura del artículo 183 del Código Penal pueda aparecer respetuosa de la *observancia formal* del principio de legalidad penal, la conclusión pareciera ser otra si a dicho tipo legal le agregamos, como **dato relevante**, el ***estado de cosas de referencia*** al que atendió al legislador al estructurar la descripción típica.

Es que, si el ***contenido de injusto*** **de una conducta delictiva** ***viene determinado por la pena que en abstracto reprime al injusto***, y si ***ésta se establece conforme el estado de cosas*** **en el que reparó** ***el legislador*** **para elaborar el tipo penal**, ese contexto debe ser tenido en cuenta a la hora de analizar si una conducta no prevista por el encargado de sancionar la ley puede subsumirse en cierta descripción típica por él sancionada.

Lo dicho conduce a tener por justificada la creación de este tipo legal.

Es que, insistimos, la norma soluciona el problema que se había generado en la jurisprudencia que consideraba atípica la destrucción de datos o programas de ordenador, o incluso la difusión de virus informáticos en redes de computadores.

La falta de inclusión en la histórica tipificación del artículo 183 —hoy, artículo 183, 1º párrafo, CP— de los "datos, documentos, programas o sistemas informáticos", había llevado en numerosos casos a los tribunales y a la doctrina jurídica a concluir que su destrucción resultaba atípica. Por eso, el párrafo que introduce la ley nacional nº 26.388 materializa la principal modificación que requería nuestro ordenamiento jurídico penal.

El **tipo subjetivo** del delito es doloso, siendo admisible sólo el dolo directo. Como lo ha sabido considerar buena parte de nuestra doctrina jurídica, él consiste en

52 O la que reprime el hurto (circunstancia que señalamos porque conduce a meditar igualmente sobre la conveniencia de crear un tipo penal específico de *hurto informático*).

53 Cfr. CREUS/BUOMPADRE, *Derecho penal*, t. 1, p. 629.

un *damnun iniuria datum*, es decir, "...un daño injuriosamente infligido, lo que, en resumidas cuentas..., no significa más que sostener que tiene que tratarse de una acción lanzada de manera directa a infligir el daño, a querer el daño de la cosa *como delito en sí*"[53]. El agente, entonces, debe conocer que está dañando el dato, documento, programa o sistema informático, y la intención de llevar a cabo tal conducta.

No hay en la figura ningún componente subjetivo distinto del dolo.

Cualquier persona puede ser **sujeto activo** del ***cracking***. Para su realización alcanza con la conducta de un solo sujeto activo.

Es un delito común y admite todas las formas de participación criminal.

Sujeto pasivo también puede ser cualquier persona.

Este delito instantáneo se **consuma** con la alteración, la destrucción o la inutilización de los datos, documentos, programas o sistemas informáticos. Éstas constituyen el resultado que sigue a la acción típica y que resulta *separable* espacio-temporalmente de la conducta.

Es admisible la **tentativa**.

Según el criterio de la intensidad de ataque al objeto material del bien jurídico, el daño informático es un **delito de lesión**, pues exige la afectación física del soporte material del bien jurídico.

1.2.11.2. Junto a la figura penal que acabamos de presentar —a la que podríamos denominar *daño informático "stricto sensu"*, y que, como acabamos de ver, se manifiesta en la hipótesis de quien *alterare*, *destruyere* o *inutilizare* datos, documentos, programas o sistemas informáticos—, se prevé una nueva modalidad de daño, ya que se castiga a quien "vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

Es, también, un delito **de acción**, **de resultado**, **resultativo**, **instantáneo**, de **pluralidad de actos, mixto alternativo**, y **de peligro hipotético**.

Por el contrario, se trata de un **delito informático propio**, ya que únicamente puede concebirse en vinculación con un sistema y un programa informático.

Las **conductas típicas** son las de *vender*, *distribuir*, *hacer circular* o *introducir en un sistema informático*, cualquier programa destinado a dañar.

Vende el programa, la persona que lo traspasa o entrega a un tercero a cambio del precio convenido.

Los *distribuye,* quien las entrega, por sí o terceros, a sus destinatarios.

Hace circular el programa, quien lo hace pasar de unas personas a otras.

Por último, *introduce* el programa en el sistema informático, quien lo mete o hace entrar en un dispositivo que realiza el tratamiento automatizado de datos.

Lo vendido, distribuido, hecho circular o introducido en el sistema debe ser un ***programa destinado a dañar***.

Sin lugar a dudas, y aunque no lo dice la gramaticalidad de la regla, se trata de un *programa informático*, o sea, un conjunto de instrucciones o comandos que, que una vez ejecutados, realizarán una o varias tareas en un ordenador.

Pero, además, el programa ha de estar "destinado a dañar", esto es, ha de ser un virus o un código malicioso, con aptitud para causar perjuicios al *hardware* o al *software* del sistema informático.

Según PALAZZI, el *spyware*[54] no entra dentro de esta categoría si no causa o puede causar un daño, a menos que se considere que el consumo de ciclos de CPU incide en la performance del ordenador; sin embargo, asegura el jurista, "...entendemos que no fue la idea del legislador penalizar con esta reforma al tipo de programas espías, que en todo caso afectan otros bienes jurídicos como la privacidad"[55].

Debe tratarse de un programa cuya "característica definitoria" sea la estar destinado a dañar, por lo que quedan fuera de la incriminación las herramientas usuales de trabajo informático, tales como los programas de formateo, de borrado o de administración de archivos, los que, aunque pueden usarse para borrar información, no tienen como función principal producir tal perjuicio.

Partiendo del entendimiento de que los programas destinados a provocar daños (p.ej., *virus makers*, herramientas específicas de destrucción de datos, etc.) tienen una aptitud dañosa elevada, la ley reprocha a quien —de distintos modos— incorpora en el tráfico comercial un programa de tales características, con conocimiento o la mera representación del daño a produ-

54 El ***spyware*** o **programa espía** es un programa que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en éste, y que comúnmente se emplea para obtener datos sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas. Sin embargo, también ha sido utilizado por organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software.

55 V. PALAZZI, *Los delitos informáticos*, p. 191.

cir. Es que, mediante tal proceder, el agente de alguna manera ayuda a quien usará la herramienta a cometer el delito de daño.

El **tipo subjetivo** de la infracción es también doloso, pero, a diferencia de la figura anteriormente analizada, aquí parece admisible el dolo eventual, ya que el autor debe tener el conocimiento, o *aún la mera representación*, de que vende, distribuye, hace circular o introduce en un sistema informático *un programa destinado a dañar*.

Sujeto activo del delito puede ser cualquier persona, habida cuenta que es una infracción común y admite todas las formas de participación criminal.

Sujeto pasivo también puede ser cualquier persona.

Se trata de un delito instantáneo que se **consuma** con la venta, distribución, circulación o introducción en el sistema informático de *un programa destinado a dañar*. Ha de quedar claro que son éstas, y no la misma producción de un daño, las alternativas que materializan el resultado que sigue a la acción típica y que es *separable* espacio-temporalmente de la conducta.

Es admisible la **tentativa**.

Hemos aseverado que es un **delito de peligro hipotético**: lo es porque, al exigir la ley que el objeto de la acción sea un "programa destinado a dañar", incorpora un elemento típico normativo, que requiere del órgano jurisdiccional pertinente una valoración sobre la potencialidad lesiva de la acción del agente.

1.2.11.3. Dijimos que la ley añade como agravante del daño la siguiente circunstancia:

"Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

Es una circunstancia agravante que repara en la particular potencialidad lesiva que posee la destrucción o inutilización de sistemas informáticos empleados en la prestación de servicios públicos, es decir, servicios que presta el Estado en la órbita de las administraciones públicas y que tienen como finalidad la cobertura de determinadas prestaciones que involucran a la ciudadanía en general.

1.2.12. Finalmente, la ley nacional nº 26.388 sustituye el **artículo 197 del Código Penal** por el siguiente:

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

Este delito contra los medios de comunicación contempla en su nueva redacción cualquier clase de comunicación, y no sólo las antiguas comunicaciones telegráficas y telefónicas.

Una vez más, el legislador **amplía el catálogo de objetos materiales del delito**, pero lo hace, no ya incluyendo una específica nueva especie de comunicación, sino aludiendo, en forma genérica, a *cualquier comunicación de naturaleza distinta de las que se realizan a través del telégrafo o por vía telefónica*.

La textura abierta de la expresión" comunicación "... de otra naturaleza" indudablemente permite incluir en la denotación del concepto, entre otras, a las comunicaciones que se llevan a cabo empleando un sistema informático.

Quedan atrapadas, en consecuencia, tanto las comunicaciones públicas como las privadas, incluyendo este último concepto el correo electrónico, la voz a través de IP, los mensajes de chat o los mensajes de texto a través de celulares (SMS).

VI. Reflexión final

1. Sin perjuicio de que, en alguna oportunidad, nos hemos pronunciado a favor de la **conveniencia de legislar sobre la cibercriminalidad en una ley específica**[56], y no en una modificación del Código Penal, pensamos igualmente que la ley nacional nº 26.388 posee una **trascendencia singular**.

Es que, por su intermedio, se ha posibilitado que el Código Penal contemple infracciones que, como los delitos informáticos, no podían ser previstas por el legislador al momento de la sanción de dicho digesto.

De esta forma, se han **llenado lagunas de punición** que presentaba nuestro ordenamiento jurídico en esta materia.

Pero, además, en esta oportunidad, el legislador parece haber procurado emplear una **técnica legislativa prolija**. Así lo demuestra, creemos, el rudimentario análisis que hemos procurado presentar.

Desde este punto de vista, entonces, puédese afirmar que la ley nacional nº 26.388, *prima facie*, ha logrado su cometido **respetando básicamente el principio de subsidiariedad del Derecho penal** al que hemos aludido al comienzo del texto.

56 Cfr. AROCENA, Gustavo A., "Acerca del principio de legalidad penal y de «hackers», «crackers», «defraudadores informáticos» y otras rarezas", en Ley, Razón y Justicia, año 4, nº 6, enero-julio de 2002, pp. 110 y 111.

Lo dicho es así, pues las nuevas figuras delictivas se presentan como **herramientas indispensables** para solucionar problemas a los que las disposiciones de las **restantes ramas de ordenamiento jurídico** (Derecho administrativo, Derecho civil, etc.) **no pueden dar adecuada respuesta**.

2. Sin perjuicio de esto, juzgamos pertinente llevar a cabo una reflexión adicional, que en nada se enlaza con el estudio de las normas de Derecho penal material sancionadas por la ley nacional nº 26.388, sino que se refiere al Derecho procesal penal "vinculado" con aquellas disposiciones.

A la hora de concebir una **política criminal seria** para la persecución, el juzgamiento y el eventual castigo del delito informático, **no es suficiente la tipificación** —por más perfecta y acabada que sea— de las distintas hipótesis de ciberdelito que deben ser previstas por el legislador penal.

Tampoco la imprescindible **adecuación de las estructuras y las herramientas de la Parte general** del Derecho penal.

Antes bien, resulta imprescindible la creación de **estructuras procedimentales destinadas a la elaboración y acreditación de la hipótesis fáctica** a subsumir en las nuevas figuras delictivas que se instituyen.

El aserto precedente adquiere consistencia y justificación particular ante el hecho —ya mencionado en este texto— de que la República Argentina ha adherido en el año 2010 al **Convenio sobre Cibercriminalidad de Budapest** (de noviembre de 2001), que incluye una disposición general que establece: "Los Estados firmantes **adoptarán las medidas legislativas o de otro tipo** que se estimen necesarias para **instaurar los poderes y procedimientos** previstos en la presente sección a los efectos de **investigación o de procedimientos penales específicos**" (**artículo 14.1**) y reglas específicas que indican que las Partes sancionarán tales medidas para la **conservación inmediata de datos informáticos almacenados** (**artículo 16**), la **conservación y divulgación inmediata de los datos de tráfico** (**artículo 17**), el **registro y decomiso de datos informáticos almacenados** (**artículo 19**), la **recogida en tiempo real de datos de tráfico** (**artículo 20**) y la **interceptación de datos relativos al contenido** (**artículo 21**).

Es que, rasgos salientes de los delitos informáticos, como —por ejemplo— su extraterritorialidad**, su** intemporalidad **y la** intangibilidad del instrumento y el objeto sobre el cual recae la conducta típica**, deben ser tenidos en cuenta por el legislador procesal, para que éste construya métodos de investigación y esclarecimiento del ciberdelito adecuados a tales caracteres**[57]**.**

Si, a la par de la determinación exacta de los ilícitos comprendidos en el ámbito de la delincuencia informática, el Derecho penal realizador no pergeña los instrumentos de comprobación judicial idóneos para la acreditación de tales delitos, se arriba a la inconcusa violación del **principio de racionalidad penal legislativa** según el cual el legislador **sólo debe sancionar leyes que prevean delitos apriorísticamente susceptibles de acreditación fáctica en un debido proceso penal**[58].

En otros términos, si el legislador no quiere incurrir en la creación de puro Derecho penal simbólico, debe corroborar que la hipótesis fáctica a construirse en el procedimiento encuentre métodos de constatación probatoria idóneos para su específico cometido, como así también recursos humanos, materiales y técnicos suficientes para cumplir dicho objetivo.

Y éste es, en nuestra opinión, un desiderátum que, hoy por hoy, se encuentra demasiado alejado de la realidad.

Bibliografía

ABOSO, Gustavo E./ZAPATA, María Florencia, *Cibercriminalidad y Derecho penal*, B de f, Montevideo-Buenos Aires, 2006.

ALCHOURRÓN, Carlos E./BULYGIN, Eugenio, "Definiciones y normas", en ALCHOURRÓN, Carlos

57 En vinculación con esto, puede verse CORCOY BIDASOLO, Mirentxu, "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", en Eguzkilore, nº 21, San Sebastián (España), diciembre de 2007, pp. 31 y ss., disponible en World Wide Web: http://www.ivac.ehu.es/p278-content/es/contenidos/boletin_revista/eguzkilore_num21/es_numero21/adjuntos/01%20Corcoy.indd.pdf (accedido el 2 de noviembre de 2010); también JIMÉNEZ GARCÍA, Joaquín, "Delito e informática: algunos aspectos de derecho penal material", en Eguzkilore, nº 20, San Sebastián (España), diciembre de 2006, pp. 208 y ss., disponible en World Wide Web: http://www.ivac.ehu.es/p278-content/es/contenidos/boletin_revista/ivckei_eguzkilore_numero20/es_numero20/adjuntos/14Gimenez_J.pdf (accedido el 2 de noviembre de 2010).

58 V. AROCENA, Gustavo A., "Racionalidad penal", conferencia dictada en el "Primer Congreso Nacional de Derecho Mínimo —La desesperanzadora evolución del Derecho penal y la política criminal en Argentina—", en Córdoba, el día 24 de abril de 2008.

E./BULYGIN, Eugenio, *Análisis lógico y derecho*, Centro de Estudios Constitucionales, Madrid, 1991.

AROCENA, Gustavo A., "Acerca del principio de legalidad penal y de «hackers», «crackers», «defraudadores informáticos» y otras rarezas", en Ley, Razón y Justicia, año 4, nº 6, enero-julio de 2002.

– "Racionalidad penal", conferencia dictada en el "Primer Congreso Nacional de Derecho Mínimo —La desesperanzadora evolución del Derecho penal y la política criminal en Argentina—", en Córdoba, el día 24 de abril de 2008.

CÁRDENAS, Claudia, "El lugar de comisión de los denominados ciberdelitos", en Política Criminal, nº 6, 2008, A2-6, p. 4, disponible en World Wide Web: http://www.politicacriminal.cl/n_06/a_2_6.pdf (accedido el 21 de octubre de 2010).

CESANO, José Daniel, *La política criminal y la emergencia (Entre el simbolismo y el resurgimiento punitivo)*, Mediterránea, 2004.

COLEMAN, Gabriella, "The Anthropology of Hackers", en The Atlantic, disponible en World Wide Web: http://www.theatlantic.com/technology/print/2010/09/the-anthropology-of-hackers/63308/ (accedido el 2 de noviembre de 2010).

CREUS, Carlos/BUOMPADRE, Jorge Eduardo, *Derecho penal. Parte especial*, 7ª edición actualizada y ampliada, Astrea, Buenos Aires, 2007.

DE LANGHE, Marcela/REBEQUI, Julio M., "Artículo 157 bis", en AAVV, *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, David Baigún/Eugenio Raúl Zaffaroni (dirección), Marco A. Terragni (coordinación), Hammurabi, Buenos Aires, 2008.

FARALDO CABANA, Patricia, "Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática", en Eguzkilore, nº 21, San Sebastián (España), diciembre de 2007, disponible en World Wide Web: http://www.ivac.ehu.es/p278-content/es/contenidos/boletin_revista/eguzkilore_num21/es_numero21/adjuntos/02%20Faraldo.indd.pdf (accedido el 31 de octubre de 2010).

FÍGARI, Rubén E., "Daño informático (arts. 183, 2º párr. y 184 incs. 5º y 6º del CP Ley 26.388)", en "elDial.com", Suplemento de Derecho de la Alta Tecnología, Sección Doctrina, 9/9/2009, disponible en World Wide Web: http://www.eldial.com.ar/bases/sql/ver_rl_ttt.asp?id-4556&base-50&Numingr-1 —elDial.com - DC11A8— (accedido el 4 de noviembre de 2010).

– "Reflexiones sobre la defraudación informática (ley 26.388)", en "elDial.com", Suplemento de Derecho de la Alta Tecnología, Sección Doctrina, 12/8/2009, disponible en World Wide Web: http://www.eldial.com.ar/bases/sql/ver_rl_ttt.asp?id-4500&base-50&Numingr-1 —elDial.com - DC1170— (accedido el 4 de noviembre de 2010).

GELLI, María Angélica, *Constitución de la Nación Argentina. Comentada y concordada*, La Ley, Buenos Aires, 2001.

GONZÁLEZ RUS, Juan José, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", en Revista Electrónica de Ciencia Penal y Criminología (RECPC), num. 01 (1999), disponible en World Wide Web: http://criminet.ugr.es/recpc/recpc_01-14.html (accedido el 2 de noviembre de 2010).

GRANERO, Horacio R., "Delitos informáticos: muchas gracias", disponible en "elDial.com", Suplemento de Derecho de la Alta Tecnología, editorial del 11/6/2008, disponible en World Wide Web: http://www.eldial.com.ar/publicador/comodin/comodin.asp?archivo-CC102A.html&pie-CC102A&titulo-Por%20Horacio%20R.%20Granero (accedido el 26 de octubre de 2010).

JAKOBS, Günther, "La competencia por organización en el delito omisivo. Consideraciones sobre la superficialidad de la distinción entre comisión y omisión", en JAKOBS, Günther, *Estudios de derecho penal*, traducción de Enrique Peñaranda Ramos, Carlos Suárez González y Manuel Cancio Meliá, UAM Ediciones - Editorial Civitas, Madrid, 1997.

– "Sobre el tratamiento de los defectos volitivos y de los defectos cognitivos", en JAKOBS, Günther, *Estudios de derecho penal*, traducción de Enrique Peñaranda Ramos, Carlos Suárez González y Manuel Cancio Meliá, UAM Ediciones - Editorial Civitas, Madrid, 1997.

JIMÉNEZ GARCÍA, Joaquín, "Delito e informática: algunos aspectos de derecho penal material", en Eguzkilore, nº 20, San Sebastián (España), diciembre de 2006, pp. 208 y ss., disponible en World Wide Web: http://www.ivac.ehu.es/p278-content/es/contenidos/boletin_revista/ivckei_eguzkilore_numero20/es_numero20/adjuntos/14Gimenez_J.pdf (accedido el 2 de noviembre de 2010).

LUZÓN PEÑA, Diego Manuel, *Curso de Derecho penal. Parte general*, 1ª edición, 1ª reimpresión, Universitas, Madrid, 1999.

CORCOY BIDASOLO, Mirentxu, "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", en Eguzkilore, nº 21, San Sebastián

(España), diciembre de 2007, pp. 31 y ss., disponible en World Wide Web: http://www.ivac.ehu.es/p278-content/es/contenidos/boletin_revista/eguzkilore_num21/es_numero21/adjuntos/01%20Corcoy.indd.pdf (accedido el 2 de noviembre de 2010).

NAVARRO, Guillermo Rafael/BÁEZ, Julio C./AGUIRRE, Guido J., "Artículo 155", en AAVV, *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, David Baigún/Eugenio Raúl Zaffaroni (dirección), Marco A. Terragni (coordinación), Hammurabi, Buenos Aires, 2008.

NEGROPONTE, Nicholas, *Ser digital (being digital)*, traducción de Dorotea Pläcking, Atlántida, Buenos Aires, 1995.

NINO, Carlos Santiago, *Fundamentos de derecho constitucional. Análisis filosófico, jurídico y politológico de la práctica constitucional*, 1ª edición, 1ª reimpresión, Astrea, Buenos Aires, 2000.

NÚÑEZ, Ricardo C., *Derecho penal argentino*, Editorial Bibliográfica Argentina - Bibliográfica Omeba, Buenos Aires, 1967.

PALAZZI, Pablo A., *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, Abeledo Perrot, Buenos Aires, 2009.

PILNIK ERRAMOUSPE, Franco D., "Delitos informáticos en la legislación argentina", en Actualidad Jurídica, Suplemento Penal, nº 154, octubre de 2010.

RIQUERT, Marcelo A., "Algo más sobre la legislación contra la delincuencia informática en Mercosur a propósito de la modificación al Código Penal Argentino por ley 26.388", en Centro de Investigación Interdisciplinaria en Derecho Penal Económico (CIIDPE), disponible en World Wide Web: http://www.ciidpe.com.ar/area2/DELINCUENCIA%20INFORMATICA.RIQUERT.pdf (accedido el 25 de octubre de 2010).

SILVA SÁNCHEZ, Jesús María, *La expansión del Derecho penal —Aspectos de la política criminal en las sociedades postindustriales—*, 1ª edición, reimpresión, Madrid, 2001.