# "LEGISLACIÓN ARGENTINA EN MATERIA DE DELINCUENCIA INFORMÁTICA"

Marcelo Alfredo Riquert**

Sumario: I. Introducción. II. Breve recordatorio de normas específicas previas: 1. Confidencialidad de la información y empresa; 2. Confidencialidad de la información y bases de datos fiscales; 3. Propiedad intelectual y software; 4. Protección de datos personales: 5. Falsedades documentales, documento electrónico y firma digital; 6. Defraudaciones y medios informáticos. III. Las novedades introducidas por Ley 26388: a. En materia de protección de datos personales: a.1. Acceso ilegítimo a banco de datos personales, a.2. Proporcionar o revelar información registrada secreta, a.3. Inserción ilegítima de datos personales; b. Nuevos conceptos y equiparaciones de documento, firma, suscripción, instrumento privado y certificado; c. Defraudaciones y medios informáticos 2; d. Normas vinculadas a la punición de la ciberpornografía infantil; e. Daño en datos, documentos, programas o sistemas informáticos; f. Comunicaciones vía electrónica; g. Intrusismo informático. IV. Algunos problemas sin solución clara. V. Valoración inicial del texto legal reformista

## I. Introducción

En junio de 2008 se produjo una vasta reforma al Código Penal argentino por vía de la Ley 26388[1], que ha venido a saldar la mayoría de las "deudas" de nuestro legislador nacional en materia de consideración de las nuevas tecnologías de la comunicación, hecho que veníamos denunciando desde más de una década atrás y que comprende variados

** Profesor Titular Regular de Derecho Penal a cargo de la Cátedra 1 de Derecho Penal 1 (Parte General), Facultad de Derecho de la Universidad Nacional de Mar del Plata (Argentina). Juez de la Cámara de Apelación y Garantías en lo Penal del Departamento Judicial Mar del Plata.

[1] Sancionada el 4/6/08, promulgada de hecho el 24/6/08 y publicada en el B.O. del 25/6/08.

ángulos de aproximación que van desde la preocupación por brindar adecuado amparo jurídico a estos avances así como respuesta, incluso de naturaleza penal, ante su uso abusivo[2].

Ante la novedad normativa –fruto de la consideración de 16 proyectos, según especifica el dictamen de las Comisiones de Justicia y Asuntos Penales y de Sistemas, Medios de Comunicación y Libertad de Expresión del Senado–, que impactó adicionando las modificaciones, sustituciones o incorporaciones verificadas en doce tipos penales, así como la derogación de otros dos, con este breve trabajo pretendemos ofrecer una sintética aproximación sobre aquellas al ocasional interesado en esta singular problemática[3].

Vale la pena recordar que habíamos señalado que algunas carencias de la ley argentina eran singularmente curiosas si se tiene en cuenta, como recuerda Palazzi con su reconocida ilustración, que los virus informáticos están lejos de ser novedosos, al menos, en la teoría, habiendo sido el propio John von Neumann quien expuso a fines de la década del '40 la idea del programa que se reproduce (1949, *"Theory and organization of complicated automata"*), hablando a mediados de la década siguiente de la posibilidad teórica de crear un autómata capaz de reproducirse a sí mismo (1955, *"The computer and the brain"*); mientras que, en la práctica, inicia su desarrollo en los Laboratorios Bell en la década del '60 y se terminan popularizando veinte años después[4].

En cuanto al medio argentino, ha sido destacado entre los primeros casos de trascendencia en los que medió el uso de un sistema informático,

---

[2] Ccte.: Jorge Zavala Baquerizo, *"Criminología e Informática. La Informática y el Derecho a la Intimidad"*, pub. en la "Revista Jurídica Online", Facultad de Jurisprudencia y Ciencias Sociales y Políticas de la Universidad Católica de Santiago de Guayaquil, Sección Artículos, "Criminología" (www.revistajuridicaonline.com). Versión en papel de la "Revista Jurídica" N° 11, 1996, pág. 70.

[3] Para profundizar el tema remitimos a lo expuesto en la monografía *"Delincuencia Informática en Argentina y el MERCOSUR"*, prologada por el prof. Dr. David Baigún, EDIAR, Bs.As., 2009, 260 páginas.

[4] Cf. Pablo A. Palazzi, *"Virus informáticos y delito de daño"*, pub. en "Revista de Derecho Penal y Procesal Penal", Ed. LexisNexis, año 2006, Nº 4, pág. 674. Hoy, destaca el nombrado, se han expandido a todos los ámbitos de la informática y las telecomunicaciones, funcionando en las más diversas plataformas y sistemas (pág. 675).

hace ya más de un cuarto de siglo, la causa "Agüero Vera, Daniel y otros", en la que se ventiló la cuestión de una falsedad ideológica que permitió a alumnos de las carreras de Licenciatura en Administración de Empresas y Contador Público Nacional de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires, obtener su título universitario sin haber aprobado la totalidad de las materias[5]. En el último párrafo del considerando 1 de la resolución de la Sala 1º de la Cámara Nacional en lo Criminal y Correccional, fechada el 15 de febrero de 1983, se describe la parte pertinente del hecho en los siguientes términos: *"En todos estos casos, la mecánica de la maniobra consistía en la adulteración de las notas correspondientes a las evaluaciones finales que los respectivos titulares de cátedra o responsables de los cursos han consignado en las actas oficiales… Estas planillas, falseadas luego de la entrega de ellas por los titulares posibilitó que el sistema de información electrónica reproduzca el listado oficial ya falseado y en muchos casos, la errónea expedición de títulos universitarios"*[6].

En función del reducido objeto de esta propuesta se evitarán incursiones sobre conceptos generales respecto de la delincuencia informática, de los que nos ocupamos en trabajos previos a los que remitimos. Sin perjuicio de ello, es importante recordar que, habida cuenta de las posibilidades que brindan las nuevas tecnologías de la comunicación y la aparición en escena de un nuevo espacio, el virtual o ciberespacio, en materia de delincuencia, facilitando la afectación de bienes jurídicos a una distancia y con una velocidad hasta no hace tanto impensadas, resulta un lugar común la afirmación de estar en presencia de una problemática frente a la que el proceso de homogeneización legislativa y de cooperación en los ámbitos sustantivos y adjetivos, es una necesidad ineludible si se quiere evitar la existencia de "paraísos" de impunidad[7].

---

[5] Curiosamente, el recordatorio lo formuló el profesor alemán Klaus Tiedemann en un viejo artículo: *"Criminalidad mediante computadoras"*, trad. por Amelia Mantilla de Sandoval, pub. en la revista "Nuevo Foro Penal", N° 30, octubre-diciembre 1985, pág. 482.

[6] El fallo está publicado en J.A., 1984-III-76/91.

[7] Abundando, puede recordarse con Federico Santiago Díaz Lannes que, ya en 1992 en el marco del Coloquio de la Asociación Internacional de Derecho Penal celebrado en Wurzburgo, se recomendó que, verificándose la insuficiencia de los tipos penales existentes, se promoviera su modificación o la creación de otros nuevos, sin perjuicio de

Ciertamente, la reciente reforma rescata a la legislación argentina de una situación en que el atraso era notable, incluso, ciñéndonos al cotejo regional.

Dejamos en la ocasión expresamente fuera de consideración lo relativo al impacto que, so pretexto de persecución del delito, se viene observando a propósito de tales facilidades técnicas[8]. Baste recordar que en muchos países se vienen adoptando medidas legislativas que ocasionalmente incluyen sanciones, obligando a los prestadores de servicios de telecomunicación (PST: término que abarca tanto a los prestadores de servicio de Internet –PSI- como a los de otros servicios de telecomunicaciones, como los celulares) a crear una infraestructura que permita a los organismos encargados de la persecución penal acceder a la totalidad de una telecomunicación específica transmitida a través de sus instalaciones. Por esto, autores como Daphne Gilbert e Ian R. Kerr hablan de un cambio de papel en los PST, pasan de *"leales guardianes de la información personal de los clientes a "agentes del Estado", de centinelas de la vida privada a partícipes activos en la lucha contra la cibercriminalidad"*[9].

---

la vigencia del principio de subsidiariedad (así, en su artículo *"Los delitos informáticos: necesidad de su regulación y jurisprudencia relativa al tema"*, pub. en la biblioteca jurídica online "elDial.com", Suplemento de Derecho de la Alta Tecnología, 5/6/08, sección "Doctrina", acápite "b"). Al presente, como destaca Palazzi, se ha llegado a la firma por más de 40 países desarrollados de la Convención de Cibercriminalidad de Budapest (del 23 de noviembre de 2001), habiendo sido Argentina invitada a integrarla recientemente (cf. noticia en su trabajo *"Análisis del proyecto de ley de delitos informáticos aprobado por el Senado de la Nación en el año 1997"*, versión borrador inédita del mes de marzo de 2008, gentilmente facilitada por el autor, pág. 2).

[8] Esta temática la hemos desarrollado en particular en la obra *"Crisis Penal. Política Criminal, Globalización y Derecho Penal"*, Ediar, Bs.As., 2007.

[9] Gilbert y Kerr, *"¿Delegar en el sector privado? Los PSI como agentes del Estado"*, pub. en AAVV *"Derecho a la intimidad y a la protección de datos personales"*, Yves Poullet, María Verónica Pérez Asinari y Pablo Palazzi coordinadores, Heliasta, Bs.As., 2009, pág. 227. Con tono general, Ernesto Velásquez Baquerizo apuntaba lustros atrás que la sociedad tecnologizada se encuentra inmersa en una amenaza a la libertad y privacidad individuales, corriendo peligro la estabilidad de la relación entre el individuo y el Estado, pudiéndose desequilibrar los valores y garantías que han sido ejes del Estado de Derecho (en su trabajo *"Sociedad informatizada y derecho constitucional"*, pub. en la "Revista Jurídica Online", Facultad de Jurisprudencia y Ciencias Sociales y Políticas de la Universidad Católica de Santiago de Guayaquil, Sección Artículos, "Criminología"

## II. Breve recordatorio de normas específicas previas

Es claro que la reforma mencionada no es la primera ocasión en que nuestro legislador se ocupó de esta problemática. Incluso, parte de la reforma ha venido a corregir algunos defectos de "intervenciones" anteriores en el texto del Código histórico, según se verá, sin perjuicio de que adoptando una metodología ciertamente ecléctica, ha oscilado entre ocasiones en que abordó la consideración de las modernas TIC en su incidencia penal modificando en forma directa aquel texto sustantivo y otras en que ello plasmó en disgregadas leyes especiales. En síntesis, el cuadro normativo previo es el que sigue.

### 1. Confidencialidad de la información y empresa

La primera norma considerando las nuevas tecnologías de la información fue la Ley N° 24.766 (1997) de *"Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos"*. Introdujo la protección del secreto de las informaciones de personas físicas o jurídicas almacenadas en medios informáticos (bases de datos), penándose su ilegítima divulgación conforme las penalidades del Código Penal para el delito de violación de secretos (art. 156: multa de $ 1.500 a $ 90.000 e inhabilitación especial de seis meses a tres años). El art. 2° dice:

> *"La presente ley se aplicará a la información que conste en documentos, medios electrónicos o magnéticos, discos, ópticos, microfilmes, películas u otros elementos similares"*.

Estableció la protección de la información secreta, confidencial, de la empresa y personas físicas y lo es sólo de la contenida en bases de datos no estatales. Autores como Creus y Buompadre, justamente al tratar al art. 156 del CP, han considerado al tipo de la ley especial como un "régimen particular de secreto"[10].

---

(www.revistajuridicaonline.com). Versión en papel de la "Revista Jurídica" N° 12, 1996, pág. 54).

[10] Cf. Creus-Buompadre, *"Derecho Penal. Parte Especial"*, Astrea, Bs.As., 2007, Tomo 1, 7° edición actualizada, pág. 400, parág. 892.

2. Confidencialidad de la información y bases de datos fiscales

En orden cronológico sigue la *"alteración dolosa de registros fiscales"* que también en 1997 introdujera la vigente Ley Penal Tributaria y Previsional Nro. 24.769 (art. 12). En dicha figura se hace concreta referencia al *registro o soporte informático* como objeto de protección en paridad con el tradicional registro o soporte documental, en este caso, cuando sea del fisco nacional[11]. Dice:

> *"Será reprimido con prisión de dos a seis años, el que de cualquier modo sustrajere, suprimiere, ocultare, adulterare, modificare o inutilizare los registros o soportes documentales o informáticos del fisco nacional, relativos a las obligaciones tributarias o de recursos de la seguridad social, con el propósito de disimular la real situación fiscal de un obligado"*.

3. Propiedad intelectual y software

La Ley Nº 25.036 (1998) modificó la Ley de Propiedad Intelectual Nº 11.723, brindando protección penal al *software*. Ello a partir de la inclusión de los programas de computación en sus arts. 1, 4, 9, 55 bis y 57, ampliando así los objetos de protección de las conductas que ya se tipificaban en los términos de los arts. 71, 72 y ss. de esta última, los que no fueron a su vez adecuados en consonancia con aquellos[12]. Vale la pena recordar la amplitud del primero, que dice:

> *"Será reprimido con la pena establecida por el art. 172 del Código Penal el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta ley"*.

La escala penal conminada en abstracto, por integración, es de un mes a seis años de prisión. Por ley 26285 (B.O. del 13/9/07), se ha introducido una nueva modificación a la Ley de Propiedad Intelectual

---

[11] Al respecto, hemos analizado en extenso de este tipo penal en nuestro trabajo *"Cuestiones de Derecho Penal y Procesal Penal Tributario"*, EDIAR, Bs.As., 2º edición, 2004, págs. 139 y ss.

[12] Nos hemos ocupado del tema en el capítulo VII de la monografía *"Informática y Derecho Penal Argentino"*, Ad-Hoc, Bs.As., 1999.

que recorta el universo de supuestos típicos. En este caso, eximiendo del pago de derechos de autor a la reproducción y distribución de obras científicas o literarias en sistemas especiales para ciegos y personas con otras discapacidades perceptivas, siempre que la reproducción y distribución sean hechas por entidades autorizadas. Esto rige también para las obras que se distribuyan por vía electrónica, encriptadas o protegidas por cualquier otro sistema que impida su lectura a personas no habilitadas, estando a cargo de aquellas entidades autorizadas la asignación y administración de las claves de acceso a las obras protegidas. No se aplicará la exención a la reproducción y distribución de obras que se hubieron editado originalmente en sistemas especiales para personas con discapacidades visuales o perceptivas, y que se hallen comercialmente disponibles. Con relación a estas últimas, el art. 36 reformado finaliza diciendo: *"Asimismo, advertirán* (las obras reproducidas y distribuidas en sistemas especiales) *que el uso indebido de estas reproducciones será reprimido con pena de prisión, conforme el art. 172 del Código Penal"*.

El vinculado a la propiedad intelectual es uno de los ámbitos donde en forma paulatina se comienza a hablar más abiertamente sobre la necesidad y/o conveniencia del sostenimiento de la intervención del derecho penal. Carnevale recuerda que el uso masivo de los archivos en formato MP3 y de las redes P2P es considerado un fenómeno social y cultural que ha revolucionado tanto la industria musical como la cultura en sí, por lo que genera la pregunta frente a esta situación sobre si tiene sentido perseguir penalmente una conducta socialmente aceptada y practicada por millones de personas y, además, si se trata realmente de una problema social o de una lucha por los intereses económicos que hay en juego[13].

4. Protección de datos personales

La Ley Nº 25.286 (2000) de Protección de Datos Personales (reglamentaria del proceso constitucional de Hábeas Data, art. 43 C.N.),

[13] Carlos A. Carnevale, *"Derecho de autor. Internet y piratería. Problemática penal y procesal penal"*, Ad-Hoc, Bs.As., colección Monografías, N° 11, 2009, págs. 14/15. Para la ampliación sobre esta temática, en particular la tesis del "copyleft", véase nuestro trabajo *"Delincuencia informática…"*, ya citado, págs. 98/105.

había incorporado al Código Penal dos nuevos tipos, el 117bis dentro del Título II correspondiente a los *"Delitos contra el Honor"* y el art. 157bis en el capítulo III de la *"Violación de secretos"* del Título V *"Delitos contra la Libertad"*. La nueva ley 26388, ha derogado el primero y modificado al segundo, por lo que volveremos sobre este punto luego.

5. Falsedades documentales, documento electrónico y firma digital

La Ley Nº 25.506 de Firma Digital (2001)[14], además de fijar su propio régimen de sanciones (contravencional) en los arts. 40/46, había incorporado un nuevo artículo al cierre de la Parte General del código sustantivo argentino, realizando así la equiparación de sus conceptos centrales a los fines del derecho penal. Este era el artículo 78 bis (cf. art. 51 de la Ley citada), que decía:

> *"Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente".*

La norma ha quedado derogada en virtud del art. 14 de la reciente Ley 26388 que, a su vez, por su art. 1° incorporó, a modo de reemplazo, tres nuevos párrafos finales al art. 77 del C.P., por lo que también avanzaremos sobre la cuestión al tratar las modificaciones recientes.

6. Defraudaciones y medios informáticos

Por Ley 25.930[15] se incorporó como inciso del art. 173 del Código Penal, el siguiente:

---

[14] Sancionada el 14/11/01, promulgada el 12/11/01 y publicada en el Boletín Oficial del 14/12/01. Puede consultarse además en "Anales de Legislación Argentina", La Ley, Boletín Informativo Nº 34, Año 2001, pág. 1 y ss. Ha sido reglamentada por Decreto 2628/2002, del 19/12/02. Puede ampliarse lo concerniente a este acápite con lo expuesto oportunamente en nuestra colaboración "Delitos Informáticos", pub. en la obra colectiva *"Derecho Penal de los Negocios"*, dirigida por los Dres. Daniel P. Carreras y Humberto Vázquez, Astrea, Bs.As., 2004, págs. 303/346.

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

> *"Art. 173… 15) El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciese por medio de una operación automática"*.

Advertimos de inicio el apartamiento a la propuesta que sobre la figura del "fraude informático" había elaborado el proyecto de ley de delitos informáticos que se elaborara en el ámbito de la Secretaría de Comunicaciones de la Nación (res. 476/01)[16]. Se trata, además, pese a las críticas que suscitó por incompleto, del texto reproducido como inc. "I" del art. 175 del anteproyecto de reforma integral[17]. Donna, tras reprobar la génesis de la reforma, señala que se ha buscado en forma imprecisa garantizar la seguridad de operaciones con tarjetas de crédito, compra o débito, en beneficio de los usuarios y consumidores, y de las empresas emisoras o administradoras del sistema[18].

En principio, como apuntan Estrella y Godoy Lemos, con relación al verbo típico habrá de tenerse presente que el uso debe considerarse típico en la medida que lo sea conforme al destino habitual de la tarjeta o datos, de modo que se descarta la mera tenencia de una tarjeta robada como subsumible en esta figura[19]. Concuerda Donna diciendo que *"Debe repararse en que hasta tanto no sea realmente empleada en perjuicio de otro –esa tarjeta obtenida con ardid o engaño de su legítimo emisor–, este tipo penal no*

---

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

[17] Ya citado, pág. 265.

[18] Cf. su *"Derecho Penal. Parte Especial"*, Tomo II-B, 2º edición actualizada, 2007, págs. 574/575.

[19] Cf. su *"Código Penal. Parte Especial. De los delitos en particular"*, Hammurabi, Bs.As., T. 2, 2º edición, 2007, pág. 595.

*quedará perfeccionado, porque se requiere el perjuicio de toda defraudación"*[20]. El contenido conceptual de tarjeta de compra, de crédito o de débito, nos viene determinado por la Ley 25.065 (arts. 2 y 4), a cuyo texto remitimos[21].

Esta previsión legal vino a dar respuesta, al menos parcial, a algunos de los casos que habitualmente fueran denunciados como de patente inseguridad jurídica (por su discutible encuadre típico entre diversas figuras) o de lisa y llana atipicidad[22]. Así, señalamos oportunamente que en los casos de maniobras ilegales con cajeros automatizados, atendiendo a la falta de previsión expresa en la normativa punitiva argentina, podía decirse que seguíamos en la discusión sobre si configuraban el delito de estafa (art. 172 CP) o el de hurto (art. 162 CP), situación en otros países ya superada. Por ej., el C.P. español de 1995, que en el pto. 2 de su art. 248 considera reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero. Es claro que no es exactamente lo mismo que ahora se ha incorporado a nuestro digesto punitivo, ya que la norma española parece ser de mayor amplitud (como el proyecto local antes mencionado), pero debe resaltarse que las maniobras urdidas mediante el uso de tarjetas de compra, crédito o débito, sean originales a las que se accediera en forma permanente o transitoria o copias gemelas por el doblado de la banda magnética, así como usando datos de ellas en forma no autorizada, son cada vez más frecuentes y la nueva norma viene a dar una respuesta satisfactoria a esta problemática[23].

---

[20] Ob.cit., pág. 578. Recuerda, sin embargo, en nota al pié 803 la existencia previa de jurisprudencia contradictoria referente al uso de la tarjeta.

[21] Ccte.: Creus-Buompadre, ya citados, pág. 555.

[22] En este sentido, Hugo y Gustavo Vaninetti, recuerdan el listado de maniobras defraudatorias más usuales en el medio informático según publicara la Comisión Federal de Comercio de Estados Unidos, que incluye desde pedidos de donaciones, subastas, ventas en pirámide, oferta de viajes y vacaciones, oportunidades de negocios, premios supuestos, inversiones, productos y servicios milagrosos, el cuento de la novia hasta el llamado "fraude nigeriano" (puede verse en detalle en su trabajo *"Estafa en internet"*, pub. en E.D., T. 211, 2005, págs. 682/683).

[23] Toda la discusión previa a esta norma la hemos largamente expuesto en la citada obra *"Derecho Penal de los Negocios"* (parág. 120 "Transferencia no consentida de activo patrimonial en perjuicio de tercero mediante manipulación informática", pág. 334 y ss), a

Excede la pretensión de este breve comentario el análisis sistematizado de los posibles supuestos más frecuentes, baste tener presente que –conforme lo ha realizado Jorge Buompadre– las variables pueden agruparse en torno a casos en que está involucrada una tarjeta verdadera (utilizada para defraudar; obtenida mediante ardid o engaño utilizada para defraudar; utilizada por su titular una vez agotado el crédito concedido; utilizada por un tercero autorizado una vez agotado el crédito concedido; utilizada una vez cancelada o caducada; o utilizada por persona no autorizada), una falsificada o adulterada para defraudar, una hurtada o robada para defraudar, una perdida utilizada para defraudar, una codificada o instrumento similar provisto de banda magnética utilizada para obtener distintos servicios (telefónico, de fotocopiado, de expendio de combustibles, etc.), además del uso de datos contenidos en una tarjeta magnética[24].

Sin perjuicio de ello, coincidiendo con nuestra postulación inicial, autores como Ferro apuntaron que esa dejó incólumes problemas como el del apoderamiento de dinero electrónico por medio de transferencias no autorizadas y las maniobras realizadas por medios automatizados sin la utilización de tarjetas o de sus datos y la falsificación, alteración, supresión o eliminación de datos o programas informáticos[25]. En idéntica

---

la que remitimos por razones de brevedad. En concordancia, dice Alejandro O. Tazza que *"Los más destacable de esta reforma es que resuelve... el tan cuestionado supuesto que dividía a la doctrina y la jurisprudencia acerca del tipo penal aplicable cuando se obtenía un beneficio económico mediante la realización de una operación automática o mecánica en la que no existía un sujeto pasivo personal que por error provocaba el desplazamiento patrimonial propio de esta figura"* (en su trabajo *"Estafas con tarjetas de crédito y falsificación de moneda extranjera y otros papeles"*, pub. en L.L., diario del 5/5/05, pág. 2). En igual sentido, Creus-Buompadre apuntan que el nuevo precepto legal *"colma un vacío normativo... fundamentalmente en aquellos casos en que el autor usaba una tarjeta magnética para extraer dinero de un cajero automático"* (ya citados, pág. 554).

[24] Puede verse el detalle en su comentario al art. 173 inc. 15 del CP en AAVV *"Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial"*, dirigido por David Baigún y Eugenio Raúl Zaffaroni, Hammurabi, Bs.As, 2009, Tomo 7, págs. 267/268.

[25] Cf. Alejandro H. Ferro, *"La criminalidad informática. A propósito de la sanción de la ley 25930"*, pub. en la "Revista de Derecho Penal y Procesal Penal", ed. LexisNexis, 2007, nº 2, pág. 306.

línea, en el marco del análisis del *"phishing"*[26], Toselli, Nicolosi López y Chouela concluyen que, siendo que este tipo de maniobras apunta a la obtención de datos electrónicos, sean provenientes o no de tarjetas de esta clase, ya que en muchas ocasiones los estafadores informáticos apuntan a datos relacionados directamente con cuentas bancarias, claves de acceso al servicio de *"home banking"* o contraseñas, el principio de legalidad vedaría el encuadre de este orden de conductas en la previsión en comentario[27].

---

[26] Los antes citados Vaninetti y Vaninetti, sintetizan la modalidad diciendo que consiste en la emisión de correos electrónicos que muestran la apariencia de ser comunicados de bancos o negocios-empresas de Internet, mediante los cuales reclaman la atención de sus clientes para actualizar claves de acceso o confirmar números de tarjetas de crédito utilizando de enlaces, en la mayoría de los casos, las llamadas "páginas espejo" (simulan la institucional oficial). Recuerdan que conforme la consultora Gartner Research, un estudio realizado en 2004 indicó que el phishing había crecido el 400 % en los últimos diez meses y que el 3 % de los encuestados reconoció haber facilitado información personal o financiera a páginas fraudulentas, calculándose que unas dos millones de personas fueron perjudicadas en alrededor de dos mil cuatrocientos millones de dólares, o sea, una pérdida promedio de mil doscientos dólares por persona (trabajo citado, págs. 687/688). Demócrito Reinaldo Filho apunta que el phishing es una modalidad de "spam" en que el mensaje, además de no deseado, es también fraudulento (en su trabajo *"A infeção do sistema DNS – a nova modalidade de phishing e a responsabilidade do provedor"*, pub. en "Alfa-Redi. Revista de Derecho Informático", Nº 84, Julio de 2005, disponible en www.alfa-redi.org). Agrega el nombrado que muy difícilmente podría exigirse responsabilidad de los proveedores de servicio (ISP) por este tipo de prácticas, sino solamente demandarles el aviso ante la detección y la adopción de medidas tecnológicas que minimicen las consecuencias (filtros, por ejemplo). Tanto desde la perspectiva civil como penal, la responsabilidad debe ser puesta en cabeza del "fisher". Señala finalmente como una excepción en el primer aspecto una nueva modalidad, el "pharming", en el que se redireccionan los programas de navegación (browsers) de los internautas hacia sites falsos sin necesidad de que estos cliqueen nada, sino aún sólo con poner la dirección correcta. Hay una versión extrema, en que se ataca directamente un servidor DNS (Domain Name System), lo que le otorga una escala masiva que afecta a todos los usuarios del servidor infectado. En este caso, dice el autor citado, el proveedor deberá responder (civilmente) por los daños provocados a sus usuarios por sus fallas de seguridad.

[27] Cf. Nicolás Toselli, Juan M. Nicolosi López y Diego A. Chouela, *"Nuevas formas de defraudación: phishing"*, pub. en la "Revista de Derecho Penal y Procesal Penal", ed. LexisNexis, 2007, nº 2, pág. 311.

El fenómeno del robo de identidad se ha ido expandiendo como una plaga asociada al crecimiento de la tecnología digital, indicando noticias periodísticas que según estadísticas de la Comisión Federal de Comercio de USA, sólo en ese país en los últimos cinco años los delitos con datos robados de cuentas bancarias y tarjetas de crédito afectaron a 27 millones de personas. Dicha Comisión sostiene que casi el 5 % de los adultos norteamericanos ha sido afectado cada año por este tipo de delitos, que ocupan el primer lugar en la lista de los que afectan a los consumidores, calculándose que el perjuicio a las empresas ronda los 50.000 millones de dólares y un 10 % de esa cifra a los consumidores. Gran repercusión se dio en junio de 2005 el descubrimiento de que el mes anterior un hacker había logrado ingresar en los sistemas de seguridad de las empresas Mastercard Internacional, Visa Internacional y American Express, apoderándose de los datos de 40 millones de clientes de esas tarjetas en el país citado[28]. El diario Washington Post proclamó que 2005 es el año de la filtración de datos, en el que por hechos como el referido podría llegar a 50 millones las víctimas de robo de datos. A su vez, el New York Times informó que los usuarios de tarjetas de crédito de Australia, Japón, China y otros países asiáticos fueron alertados de que sus cuentas corrían peligro si las usaban en transacciones con Estados Unidos o con empresas norteamericanas[29].

Este orden de situaciones viene impactando fuertemente en los costos empresarios, sólo en Argentina el negocio de protección de redes ha registrado un fuerte aumento en su demanda y se calcula que facturará un 15 % más durante 2005. El Centro de Investigación en Seguridad Informática (CISI), realizó un estudio según el cual el 43 % de las empresas ha reconocido haber tenido algún "incidente" en sus sistemas, lo que llevó a que el 63 % de las consultadas señalara que prevé una mayor inversión en la seguridad de sus sistemas de computación y almacenamiento de datos. Otro aspecto relevante es que alrededor del 15

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

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

% de las firmas encuestadas directamente no sabían si sus sistemas habían o no sido accedidos[30].

## III. Las novedades introducidas por Ley 26388

Pasamos ahora a la noticia e inicial tratamiento de las nuevas figuras incorporadas en la ley reformista de junio de 2008.

### a. En materia de protección de datos personales

Por su art. 3º comenzó sustituyendo el epígrafe del capítulo III del Título V (Delitos contra la libertad) del Libro II (De los delitos) del Código Penal, que pasó a ser el siguiente: *"Violación de Secretos y de la Privacidad"*. Es la misma propuesta que contenía el anteproyecto de reforma integral del código, cuya exposición de motivos decía en el considerando XII: *"Se ha modificado el Capítulo sobre violación de secretos que ahora se denomina "Violación de Secretos y de la privacidad". De este modo, se actualiza la normativa a los nuevos desarrollos tecnológicos e informáticos y se tipifican lesiones intolerables a la privacidad, mediante la utilización de artificios de escucha, transmisión, grabación o reproducción de imágenes o sonido"*[31].

Refleja además, sin dudas, la preocupación en torno a brindar un adecuado marco de protección penal a la privacidad (lo que se concreta

---

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

[31] Entre sus múltiples publicaciones en el medio virtual pueden citarse la oficial en http://www.jus.gov.ar/guia/content_codigo_penal.htm y la de los sitios "Pensamiento Penal" (www.pensamientopenal.com.ar) y "Derecho Penal Online" (www.derechopenalonline.com.ar) , que han elaborado sendos foros de discusión al respecto con amplia concurrencia e interesantes observaciones. En papel, puede verse en la sección "Actualidad" de la "Revista Nova Tesis de Derecho Penal y Procesal Penal", dirigida por Chiara Díaz y Erbetta, Nº 1, Rosario, 2007, pág. 197 y ss. La Comisión de Reformas fue creada por decreto 303 del 14/12/2004 del Ministerio de Justicia de la Nación. Su coordinador fue el Dr. Slokar, Secretario de Política Criminal y Asuntos Penitenciarios de la Nación, y estuvo integrada por los Dres. Baigún, Chiara Díaz, Da Rocha, De Luca, Di Matteo, Erbetta, Ferreyra, Hendler, Ochoa y Tizón. Participaron de las discusiones y fueron sustituidos los Dres. Donna y Yacobucci, ambos por renuncia, y el Dr. García Vitor, por fallecimiento. La cita corresponde a la "Revista Nova Tesis", pág. 225.

en diversas figuras), que fuera exteriorizada con claridad oportunamente en los fundamentos del proyecto de los senadores Ruben H. Giustiniani y Vilma L. Ibarra, donde sostenían que la *"reforma legislativa debe desarrollarse teniendo como única mira el respeto a la intimidad garantizado por nuestra Constitución Nacional, evitando cualquier intromisión de terceros que pueda dar lugar a la sociedad vigilada y controlada descripta por George Orwell. Tal obligación de preservar la confidencialidad e inviolabilidad de las telecomunicaciones tienen una un claro raigambre constitucional sustentado por los arts. 18, 19 y 33 de nuestra ley fundamental".* En modo concordante, señalan Feldstein de Cárdenas y Scotti que *"Vivir en una sociedad en que la información ha evolucionado hasta el punto de erigirse en una suerte de herramienta básica para optimizar la producción de bienes y servicios, impone la nece.*

A su vez, en el art. 14 dispuso la derogación del citado art. 117bis del digesto sustantivo, que había sido merecedor de varias críticas, partiendo por su inadecuada ubicación sistemática. Además, los arts. 7 y 8, sustituyeron los textos de los arts. 157 y 157bis, recibiendo este último en su nuevo inc. 3º parcialmente la conducta antes reprimida en el inc. 1º de la norma derogada citada.

a.1. Acceso ilegítimo a banco de datos personales

En su redacción conforme la LPDP, el art. 157 bis decía:

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

En este caso, a diferencia del derogado art. 117 bis, no se observaban en principio objeciones en cuanto a su ubicación sistemática, ya que las conductas tipificadas en la figura se relacionaban directamente con la violación de secretos en general. Como enseñaba el maestro Núñez, el bien jurídico protegido en este capítulo del Código Penal era la incolumidad de: a) la intimidad de la correspondencia y de los papeles

privados y, b) los secretos y la libre comunicación entre las personas[32]. Decíamos que, en función de la anterior reforma, se pasó a incluir: c) la información que se hallare registrada en un banco de datos personales, que se conecta con el primer aspecto (intimidad) en el inciso 1º del art. 157 bis y el segundo (secreto) en el inc. 2º, tratándose desde el punto de vista del autor de un delito común que preveía como agravante la realización por funcionario público.

Según se detalló, ahora se ha incluido como título del capítulo a la "privacidad" en forma expresa, lo que evita la necesidad de cualquier tipo de construcción como la anterior para dotar de sentido a la ubicación de la figura e interpretarla adecuadamente. El nuevo texto vigente (cf. art. 8 de la ley de reforma), es el siguiente:

> *"Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:*
> *1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;*
> *2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.*
> *3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.*
> *Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años".*

Con relación al inciso primero, se advierte que la redacción conforme la Ley 26388 es idéntica a la anterior, al igual que el monto de la pena conminado en abstracto y la circunstancia calificante de autoría por un funcionario público. La acción típica de acceder puede concretarse por cualquier medio ya que no se especifica modalidad de ingreso alguna, aunque el contexto de la reforma es claro en cuanto a que el legislador

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

quiso referirse a los medios informáticos[33]. La señalización de ilegitimidad del acceso importa la falta de consentimiento. Lógicamente, de contar con este no estaríamos frente a una conducta punible. Es conducta dolosa[34]. La lesión al bien jurídico protegido se concreta con el mero acceso[35]. Resulta admisible la tentativa.

Ledesma, al referirse a la acción penal, entendía que al no haberse modificado el art. 73 del digesto sustantivo por la LPDP incluyendo al art. 157 bis entre las excepciones que contiene, debía entenderse que la acción para perseguir este delito es privada[36], punto en el que entendemos le asistiría razón, ya que la exclusión se refiere taxativamente a los arts. 154 y 157, tratándose de un aspecto que no ha sido abordado en la reforma actual.

Finalmente, debe agregarse que la protección de datos personales ha sido complementada en la órbita contravencional por medio de la disposición 1/2003[37] de la Dirección Nacional de Protección de Datos Personales (autoridad de contralor de la ley de Habeas Data).

---

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

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

[35] Ccte.: Ledesma, quien refiriéndose al art. 157 bis 1º párrafo, entiende que es un delito formal o de pura actividad, que se consuma con el solo hecho de acceder, sin necesidad de la divulgación de datos ni de que se cause perjuicio, real o potencial (ob.cit., pág. 383).

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

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

a.2. Proporcionar o revelar información registrada secreta

a.2.1. En cuanto a "revelar" secretos, la reforma por Ley 27388 no se ha limitado a sustituir al art. 157 bis, sino que avanzó actualizando también la figura precedente. En efecto, por su art. 7° ha dispuesto la siguiente redacción para el art. 157 del C.P.:

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

Si se compara con el texto anterior, se advierte que el cambio en la "revelación de secretos por funcionario público" se ha ceñido a incluir la voz "datos" dentro del elenco de situaciones u objetos protegidos como secretos por ley cuya revelación por funcionario público es punible, lo que armoniza el tipo con las restantes modificaciones introducidas en este remozado capítulo. Es decir, que el bien jurídico sigue siendo el secreto de hechos, actuaciones, documentos y, ahora, "datos" que, al decir de Estrella y Godoy Lemos, *"tienen su origen y se mantienen dentro de la Administración Pública"* —no se incluye el secreto de los particulares—, por lo que se mantiene la histórica crítica de su ubicación sistemática, ya que *"Debería estar legislado en el Título IX del Código Penal, que tutela precisamente, a la Administración Pública como sujeto pasivo de los delitos que en su contra se cometen"* (tal como proponía el Proyecto de Soler de 1960). La acción típica es "revelar" el secreto, que los nombrados definen siguiendo a Núñez como *"en descubrirlo o manifestarlo a una persona que no está en el círculo de los obligados a guardarlo"*[38]. De tal suerte, enrolan con temperamento que compartimos entre quienes no equiparan con "divulgar", que importa publicar. Se trata de un delito doloso que puede ser cometido con dolo eventual y para cuya consumación basta la sola revelación.

a.2.2. En cuanto al inciso segundo del nuevo art. 157 bis, realizado el cotejo entre los textos transcriptos en el acápite anterior, ofrece algunas diferencias con el antecedente directo. Así, no contempla sólo la conducta

[38] Estrella y Godoy Lemos, ya citados, Tomo 2, 2° edición, págs. 281/282.

"revelare", sino también "ilegítimamente proporcionare", además que la información registrada no puede estarlo sólo en un banco de datos personales, sino en un simple "archivo", lo que le permite aprehender un universo mayor de casos, una mayor variedad de conductas. Ya se indicó el significado de "revelar", mientras que en cuanto a "proporcionar", es la acción de "hacer lo necesario para que una persona tenga algo que necesita, facilitándoselo o dándoselo"[39].

El tipo exige que el autor sea alguien obligado a preservar la información. Se trata de una figura dolosa. El dolo eventual es admisible[40]. La lesión al bien jurídico protegido se concreta con la simple revelación o el proporcionar la información[41]. También resulta posible la tentativa.

a.3. Inserción ilegítima de datos personales.

Según se anticipó, el llamado delito de "Falsedad en archivos de datos personales y suministro de información falsa", que estaba previsto por el art. 117 bis del C.P. ha sido derogado, manteniéndose parcialmente su redacción en el nuevo inc. 3º del art. 157 bis.

Para mejor ilustración, partimos recordando el texto derogado, que decía:

> *"1º. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.*
> *2º. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.*

---

[39] Así, la definición que brinda el "Diccionario Enciclopédico Ilustrado Larousse", ed. La Nación, Bs.As., 2005, pág. 945.

[40] Respecto de la anterior redacción del inciso 2º puntualizaba Donna la posibilidad de realización del tipo con dolo eventual (ob.cit., pág. 381).

[41] Ccte.: Ledesma, quien en cuanto al 2º párrafo del texto anterior, señalaba que el sujeto pasivo es el titular de los datos revelados que es, según el art. 2º de la ley 25.326, toda persona física o jurídica con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere al propia ley (ob.cit., pág. 385).

*3º. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.*
*4º. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena"*.

El cotejo con la norma vigente permite advertir que: a) el monto de pena conminado en abstracto es el mismo en lo básico, pero varía la situación del funcionario público que antes podía recibir una inhabilitación que la redacción permitía fuera de un mínimo de dos meses y ahora éste es de un año (y hasta cuatro, por lo que en el máximo, en definitiva, no hay cambio); b) el inciso primero se ha mantenido pero sufriendo algunos cambios de los que nos ocuparemos de inmediato; c) se eliminó el tipo del inciso segundo, aunque algo de la figura se puede considerar recoge el inciso segundo del art. 157 bis, que prevé el proporcionar información de un archivo o banco de datos personales, según ya vimos; d) desapareció la circunstancia calificante del inciso tercero, largamente criticada en función de que su articulación con el inciso primero posibilitaba la interpretación acerca de la extensión del tipo como la inadecuada recepción de una figura de peligro abstracto.

Es claro entonces que se valora positivamente no sólo el apartamiento de la redacción consagrada por la LPDP Nº 25286, sino también la ubicación sistemática. Había sido una crítica de alto consenso que, conforme su radicación en sede de "Delitos contra el honor" y descripción típica, se penaba el insertar o hacer insertar datos falsos aún cuando nadie se perjudique (ya que el inc. 3º consideraba a esta situación como agravante con la consecuencia ya mencionada para el inc. 1º) y, además, de cara al bien jurídico protegido (honor, en su vertiente objetiva) podría darse el caso que el dato falso no lo lesionara ni lo pusiera en peligro. Incluso, podría pasar lo contrario, es decir, el dato falso mejorara su crédito o fama.

Sin ir más lejos, justamente en función de una interpretación acotada del tipo en función del bien jurídico, se explicaba en los fundamentos del anteproyecto de reforma y actualización integral del Código Penal del año 2006, que se optaba por suprimirlo. Se decía: *"Se decidió suprimir el artículo 117 bis por su flagrante inutilidad, ya que por más que se inserten*

*falsedades en los bancos de datos personales, si no existe lesión al honor, no se verificará la tipicidad y, si existe tal lesión, el hecho no dejará de ser una injuria, una calumnia, una publicación o reproducción de las vertidas por un tercero o, bajo ciertas condiciones, un delito previsto como violación de secreto o de la privacidad (art. 146, segunda parte)"*[42]. En definitiva, se efectuaba la supresión de la figura y se la fusionaba en un nuevo artículo, el 146, con lo que se advierta la coincidencia en el camino seguido por el legislador en la Ley 26.388.

b. Nuevos conceptos y equiparaciones de documento, firma, suscripción, instrumento privado y certificado

Como señalamos oportunamente, la ley 26388 vino, por vía de su art. 1º, a incorporar tres nuevos párrafo finales al art. 77 del código sustantivo con el siguiente texto:

> *"Art. 77: …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 verifica así que mientras el segundo y tercero de los nuevos párrafos, referidos a "firma", "suscripción", "instrumento privado" y "certificado", siguen básicamente la redacción de la norma derogada; el primero, dedicado a la voz "documento", deja de lado la técnica anterior que incluía por equiparación (en otras palabras, cuando un tipo penal dice "documento", debe entenderse que incluye al "documento digital"), para pasar a dar una definición en la que dice que "comprende toda representación de actos o de hechos", declarando su independencia del soporte que se use para su fijación, almacenamiento, archivo o transmisión. En esto se ha seguido la opción del Anteproyecto de

[42] Cf. considerando XI "in fine" de los Fundamentos, pub. en la sección "Actualidad" de la "Revista Nova Tesis de Derecho Penal y Procesal Penal", dirigida por Chiara Díaz y Erbetta, Nº 1, Rosario, 2007, pág. 224.

Reforma Integral de 2006, que en su art. 69, dedicado a las "Definiciones" decía: *"Se considerará documento a la representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo que contenga datos"*. Se advierte así que se ha suplantado la probablemente innecesaria aclaración de que el archivo contenga datos por "o transmisión". Los fundamentos del anteproyecto nada aclaran sobre el particular, ya que respecto de este artículo sólo indican que *"…se formula una interpretación auténtica sobre el significado y alcance de algunos conceptos empleados"*[43].

Sin perjuicio de reconocer que *"Esta reforma traerá mayor coherencias al Código Penal"*, Palazzi ha entendido que si la intención del legislador fue crear nuevos tipos penales relacionados con las falsedades, *"hubiera sido más acertado, como técnica legislativa, incluirlos en el capítulo respectivo más que realizar estos cambios que luego requieren interpretaciones complejas. No obstante ello, es posible hablar de falsedades informáticas en nuestro derecho penal"*[44].

Por nuestra parte, con la nueva norma entendemos que cae la vieja observación de Baigún y Tozzini: *"debemos anticipar que el concepto de documento no tiene una definición legal que establezca sus límites y alcances en nuestro ordenamiento jurídico, cuyas ramas no ofrecen ninguna homogeneidad conceptual"*[45]. En esta línea, si se compara con las características comunes del concepto que los autores citados extraían de la doctrina del derecho privado, pueden validarse las de que siempre es representativo de un hecho o acto, que su concreción es siempre un producto humano (aunque lo documentado pueda ser un hecho humano o de la naturaleza) y que, como efecto derivado, tiene función probatoria; en cambio, el pensamiento de que documento es jurídicamente una "cosa mueble" ha quedado desactualizado[46]. A su vez, es claro ahora que se cuenta en

---

[43] En la versión papel de Ediar/AAPDP, pág. 71.

[44] En su obra *"Los delitos informáticos en el Código Penal. Análisis de la ley 26388"*, AbeledoPerrot, Bs.As., 2009, págs. 34 y 36.

[45] David Baigún-Carlos A. Tozzini, *"La falsedad documental en la jurisprudencia (elementos comunes a todos los tipos)"*, Depalma, Bs.As., 2° edición, 1992, pág. 37.

[46] Véase el detalle en la obra antes citada, págs. 44/45.

materia penal con una definición propia[47] que reemplaza la discusión para construirla que se realizaba a partir de los arts. 292/296 del C.P., que dividía en una corriente conocida comúnmente como "civilista" (por su apego a lo establecido por el Código Civil en relación a los actos jurídicos y su instrumentación pública o privada, conf. arts. 944, 979 y 1012) y otra que pretendía "autonomizar" el concepto de documento, asignándole un contenido diferente para el ámbito penal, clasificación que Baigún y Tozzini corregían proponiendo como más correcta denominación la que, siguiendo los resultados de estas posiciones, denominaba respectivamente como "restrictiva" y "ampliatoria" del tipo penal[48].

Habíamos oportunamente señalado que debía valorarse positivamente la reforma introducida por la Ley de Firma Digital, porque despejaba cualquier duda sobre el particular ya que, como destaca Orts Berenguer, es claro que las técnicas informáticas pueden ser un instrumento idóneo para cometer falsedades documentales, facilitando su modificación en alguna de sus partes o creando uno nuevo, para hacerlos discurrir por el tráfico jurídico[49]. El decreto reglamentario 2628/2002, aunque incurriendo en alguna superposición con el articulado de aquella ley, incorporaba un glosario de utilidad con conceptos un poco más sintéticos que los detallados en ella, los que siguen resultando imprescindibles para fijar la extensión de referencias contenidas en el texto vigente que se mantienen, según antes se puntualizó.

Así, por "firma electrónica" se entiende el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para poder ser considerada "firma digital" (art. 5, Ley 25.506), mientras que esta a su vez es el resultado de aplicar a un documento digital un procedimiento

---

47 En contra (aunque refiriéndose al art. 78 bis cf. Ley 25506), Creus-Buompadre, quienes señalaban que no se establecía con la norma indicada un concepto penal de documento sino que sólo se introducía una equivalencia expresa entre firma y documental digital con sus análogos en papel (ob.cit., Tomo 2, pág. 443, parág. 2393).

48 Puede consultarse en extenso en Baigún-Tozzini, págs. 45 y ss.

49 En su obra conjunta con Roig Torres, *"Delitos informáticos y delitos comunes cometidos a través de la informática"*, Tirant lo blanch, Colección "Los delitos", Nº 41, Valencia, 2001, p. 147.

matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control, susceptible de verificación para identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma (art. 2, Ley 25.506). De tal suerte, cuando un tipo penal integra en su tipo objetivo como elemento normativo *"firma"* —como los arts. 173 inc. 4º (delitos contra la propiedad: abuso de firma en blanco) y 289 del CP (delitos contra la fé pública), y 135 de la Ley 24.241 (delitos contra la libertad de elección de AFJP)—, o la acción de suscribir (*"suscripción"*) —art. 168 inc. 2º del CP (delitos contra la propiedad: suscripción de documento mediante violencia, intimidación o simulación de autoridad)—, queda claro que firma digital y firma electrónica no resultan ser sinónimos y que sólo la primera habrá de ser considerada a los fines de la tipicidad penal.

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

Como refiere Alejandro D. Fraschetti, tanto la firma ológrafa como la digital tienen dos funciones fundamentales: servir como medio de expresión de la voluntad y determinar la autoría de quien realiza un determinado acto jurídico, buscando además la última garantizar la inalterabilidad del documento suscripto. Según se ha visto, por la ley 25.506 se estableció la posibilidad de utilizar la firma digital cuando el ordenamiento jurídico exige la ológrafa, fijando algunas excepciones, e indicando como presunciones "iuris tantum" de su uso la autoría y la integridad del mensaje. Al respecto, indica el nombrado que la prueba en contrario de la presunción de autoría puede estar vinculada con la real

autoría del mensaje, es decir, con la voluntad real del titular, aún cuando todos los datos del certificado digital sean verdaderos[50].

c. Defraudaciones y medios informáticos 2

Con motivo de la sanción de la Ley 26388 se ha ampliado la protección penal frente a las defraudaciones por medios informáticos ya que por su art. 9 se ha producido la incorporación de un nuevo inciso, el 16, al art. 173 del C.P., con el siguiente texto:

> *"Art. 173... 16) El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".*

Se observa que se toma parte del proyecto referido –al tratar el tema con anterioridad–, la fórmula "manipulación informática" sobre un sistema o la transmisión de datos, pero no la referencia a que con ello se procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. Es que aquella propuesta seguía con mayor rigor el ejemplo provisto por el Código Penal español de 1995, que en el pto. 2 de su art. 248 considera reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero. Con razón señala Francisco Muñoz Conde que esta mención expresa de la manipulación informática como forma de comisión de la estafa, ha despejado las dudas que anteriormente había planteado la doctrina[51]. No obstante, corresponde señalar que la figura española referida también ha tenido sus críticas. Así, observa Amadeo que se trataría de una estafa sin engaño y sin disposición patrimonial voluntaria, por lo que en su consideración sería peligroso para el principio de legalidad la traspolación de esto a las estafas realizadas por

---

[50] Fraschetti, *"La Ley de Firma Digital y las presunciones de autoría e integridad"*, pub. en J.A., revista del 25/2/04, pág. 45.

[51] En su "Derecho Penal. Parte Especial", 11º edición, Tirant lo Blanch Libros, Valencia, 1996, pág. 363.

cualquier medio[52]. Corresponde aclarar que el tipo citado del CPE es aplicable al caso en que hay maniobra de desvío previa pero no al de simple utilización de tarjeta de otro o adulterada, para nosotros cubierto por el inc. 15 del art. 173, mientras que para España el último caso ha sido asimilado al robo mediante llaves falsas del art. 239 del CPE, ya que su último párrafo dice: *"A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia"*.

Algunos autores, como Alonso Salazar, dicen que la "estafa electrónica" no es ninguna estafa, por ausencia de un sujeto pasivo que realice el acto dispositivo, pero que sin embargo se asemeja a la hipótesis de la estafa triangular (el engañado y el estafado son personas diferentes), aunque aclara que en ésta, el engañado tiene la facultad de realizar un acto dispositivo perjudicial para el estafado, una lesión a su patrimonio y obtiene para sí o para un tercero un beneficio patrimonial antijurídico[53]. En definitiva, volviendo al "recorte" del texto consagrado en la novedad argentina, entendemos que esta omisión podría ser superada por vía de interpretación atendiendo la ubicación de la inserción pero, ciertamente, la redacción pudo ser mejor y ha quedado muy "abierta". A todo evento, la interpretación a realizar tendrá como un norte insoslayable el "cerrar" los alcances del tipo, hacerlo aplicable a los casos en que el bien jurídico afectado sea el patrimonio. Puede rescatarse que varias de las conductas que habíamos señalado quedaban fuera del inciso 15, tienen ahora recepción en la nueva norma[54].

Buompadre enfatiza que, no obstante esta novedad, la estafa genérica del art. 172 debe seguir siendo interpretada en su concepción tradicional, es decir, mantener la idea clásica de que el engaño, para ser típico, debe ser inducido a otra persona física. Esta nueva forma de estafa es entonces, respecto del tipo citado, una figura especializada por el

---

[52] En su artículo *"La informática y su incorporación en la Ley Orgánica 10/1995 del Código Penal español"*, pub. en J.A., T. 1996-III-1048/1056.

[53] En su trabajo *"Delito Informático. Análisis comparativo con el delito de daños y otros tipos del Código Penal costarricense"*, pub. en "Cuadernos de Doctrina y Jurisprudencia Penal", Ad-Hoc, Bs.As., T. 9-A, 1999, pág. 718.

[54] Ccte.: Buompadre, antes citado, pág. 276.

medio empleado (un sistema informático)[55]. Así, tras elogiar el ajuste del Código a las nuevas tecnologías, indica que la redacción no ha sido la más apropiada si la idea del legislador fue apartarse de la rígida construcción de la estafa tradicional para acabar con la impunidad que implicaba la imposibilidad de engañar a una máquina (ej.: transferencia no consentida de activos patrimoniales en perjuicio de un tercero). En ese caso, no debió introducirse una fórmula cuya única diferencia con la básica del art. 172 es el medio empleado para cometer el delito. Precisamente, al desaparecer el engaño y el error como elementos centrales del tipo de estafa, no era necesario incluir la referencia "al otro" como sujeto pasivo, exigencia que generaba toda la discusión de vacío de impunidad. Concluye el nombrado que estamos frente a un supuesto de "estafa impropia", en la que el engaño y el error han sido reemplazados por la maniobra informática, mientras que la disposición patrimonial en algunos casos la realizará una persona física y en otros la propia máquina[56].

d. Normas vinculadas a la punición de la ciberpornografía infantil

El problema de la extensión del tráfico de material y producción de contenidos de pornografía vinculada a los menores se ha visto facilitado por las nuevas tecnologías de la información y reflejado, en los últimos tiempos, en el incremento de procedimientos judiciales internacionales sobre los que a diario dan cuenta diversos medios periodísticos[57]. Hay quien, incluso, aventura la detección de un nuevo tipo de "delincuente sexual", que establece contacto con un niño por medio de Internet *"y está dispuesto a recorrer distancias quizás enormes, a través de Estados, continentes*

[55] Ob.cit., pág. 276.

[56] Ob.cit., págs. 279/280.

[57] En forma reciente se notició que, en el marco del "II Congreso Nacional de Policías Tecnológicas" celebrado en noviembre de 2009 en Madrid, se concluía la necesidad de utilizar "agentes encubiertos" para combatir la pornografía infantil en Internet, habida cuenta que la migración de los consumidores desde redes públicas P2P, como e-Mule o Kazaa, hacia foros restringidos, impone ganarse su confianza para localizarlos y detener a quienes producen y distribuyen material pornográfico infantil mediante tal herramienta de investigación no convencional (fuente: "Hoy Tecnología", noticia del 13/11/09, disponible en: www.hoytecnologia.com/noticias/agente-encubierto-nueva-arma/83774).

*y países, a fin de encontrarse con el niño y abusar sexualmente de él"*[58]. Estamos frente a una actividad gravemente disvaliosa en la que la nota de globalización se ha acentuado justamente por la aparición de herramientas que permiten la configuración de verdaderas "redes" delictivas.

Se trata, además, de un tema que genera alto nivel de consenso en cuanto a la necesidad de afrontarlo a nivel global, siendo muy importante la cantidad de documentos suscriptos sobre el particular, partiendo de la "Convención sobre los Derechos del Niño" de Naciones Unidas, en vigor desde 1990, aprobada en Argentina por ley 23849 y que goza de jerarquía constitucional, por vía del art. 75 inc. 22 desde la reforma de nuestra Carta Magna de 1994 y prevé en su art. 34 la protección al menor *"contra todas las formas de explotación y abusos sexuales"*, formando parte de las obligaciones que impone, como resalta Marcelo P. Vázquez, *"la adopción de todas las medidas de carácter nacional, bilateral y multilateral para impedir la incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal; la explotación del niño en la prostitución u otras prácticas sexuales ilegales; y la explotación del niño en espectáculos o materiales pornográficos"*[59].

Si bien no había norma específica, podía señalarse que el 128 del CP (cf. Ley 25087/99) punía al que "*produjere o publicare* imágenes pornográficas en que se exhibieran menores" o "*organizare* espectáculos en vivo con escenas pornográficas en que participaren menores" de 18 años. También al que "*distribuyere* imágenes pornográficas cuyas características externas hiciere manifiesto que en ellas se ha grabado o fotografiado la exhibición de menores" de 18 años "al momento de la creación de la imagen", y al que "*facilitare* el acceso a espectáculos pornográficos o *suministrare* material pornográfico a menores" de 14 años. Entendimos que la amplitud de las conductas descriptas permitía aprehender sin mayor problema los casos en el que el medio utilizado fuere Internet, aún cuando no era mencionado en forma expresa pues

---

[58] Cf. Marcelo P. Vázquez, en su trabajo *"La explotación sexual comercial de la niñez y su relación con la red Internet"*, pub. en CDJP, Ad-Hoc, Bs.As., Nº 18-19, 2005, págs. 644/645.

[59] Antes citado, pág. 646.

ningún otro lo había sido[60]. El anteproyecto de reforma integral mantenía este texto inalterado en su art. 161. La Ley 26388 ha modificado el tipo citado por su art. 2°, que ha consagrado la siguiente redacción:

> *"Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con 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".*

Puede de inicio anotarse que las escalas penales conminadas en abstracto no se han cambiado, al igual que el texto completo del último párrafo. Entre las modificaciones más significativas se cuentan: a) se pasó de no mencionar ningún medio a explicitar que puede ser por cualquiera; b) el elenco de conductas típicas anterior ("produjere", "publicare", "distribuyere" y "organizare", de sus primeros dos párrafos), se concentraron en el primer párrafo, en el que se agregaron las de "financiare", "ofreciere", "comerciare", "facilitare" y "divulgare"; c) con pena equiparada se incorporó en el nuevo segundo párrafo la conducta de "tenencia…con fines inequívocos de distribución o comercialización" de las representaciones pornográficas de menores.

---

[60] Así, en nuestro comentario al tipo de "Pornografía infantil y facilitación de pornografía a menores" (art. 128), publicado en AAVV, *"Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial"*, dirigido por Baigún y Zaffaroni, ed. Hammurabi, Tomo 4, Arts. 97/133 Parte Especial, Bs.As., 2008, págs. 653/694. Se expide en sentido concordante Valeria A. Lancman, en su trabajo *"La pornografía infantil y la Internet"*, pub. en el sitio web del profesor Terragni (www.terragnijurista.com.ar/doctrina/pornografia.htm).

El alcance jurídico del concepto de pornografía infantil viene delineado por la Ley 25763[61], cuyo art. 1º aprueba el *"Protocolo facultativo de la Convención sobre los derechos del niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía"* (Asamblea General de Naciones Unidas, sesión plenaria del 25 de mayo de 2000). El art. 2º inc. c) dice que *"por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o todo representación de las partes genitales de un niño con fines primordialmente sexuales"*. Adviértase la inclusión expresa de las simulaciones de acto sexual explícito de un menor, tema sobre el que bien destaca Palazzi que aún cuando en trámite parlamentario de la Ley 26388, conforme el texto proveniente de la Cámara de Diputados incluía estas actividades "simuladas" (también llamada pornografía infantil virtual), fueron excluidas en Senadores por considerárselo un tema controvertido pese a su previsión por el Protocolo citado[62]. En efecto, tanto en Estados Unidos como Brasil, por citar dos ejemplos, cláusulas similares generaron gran discusión por desajuste constitucional. Así lo entendió la Corte Suprema estadounidense al tratar la Child Pornography Prevention Act de 1996, al considerarla contrapuesta con el principio de libertad de expresión. En Brasil, la modificación del Estatuto del Menor y del Adolescente introducida por Ley 10764 de 2003, tuvo en su discusión parlamentaria la consideración del tema, que pretendió introducirlo el diputado Biscaia, iniciativa finalmente rechazada por la misma razón[63].

Refiriéndonos al texto ahora sustituido, habíamos señalado nuestra coincidencia con la acertada observación de Hugo Alfredo y Gustavo Juan Vaninetti sobre la necesidad de un debate acerca de la eventual incorporación de las figuras de posesión simple de material pornográfico infantil y posesión preordenada para venta, distribución o exhibición de

---

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

[62] En *"Análisis..."*, ya citado, pág. 7. Esto lo reitera en el trabajo *"Análisis de la ley 26388 de reforma al Código Penal en materia de delitos informáticos"*, pub. en "Revista de Derecho Penal y Procesal Penal", dirigida por D'Alessio y Bertolino, LexisNexis, Bs.As., N° 7/2008, julio, pág. 1214.

[63] Cf. Erick Iriarte, en su trabajo *"Brazil: o crime de divulgação de pornografia infantil pela Internet – Breves comentários à Lei 10764/03"*, pub. en la revista virtual "Alfa-Redi" (www.alfa-redi.org), sección "Delitos Informáticos".

material pornográfico infantil. Esta última está contemplada ahora en el 2° párrafo del tipo actual, recogiendo la previsión del Protocolo aprobado por Ley 25763, cuyo art. 3º dispone: *"todo Estado parte adoptará medidas para que, como mínimo, los actos y actividades que a continuación se enumeren queden íntegramente comprendidos en su legislación penal, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente... c) La producción, distribución, divulgación, importación, exportación, oferta, venta o posesión, con los fines antes señalados, de pornografía infantil"*[64]. Similar en el derecho comparado puede citarse el art. 189.1.B del C.P. español, vigente desde 1999. Si bien ofrece como dificultad la de probar tal preordenación, esto es un problema de índole procesal que en nada obstaculiza la razonabilidad del tipo[65].

En cuanto a la simple posesión, no incorporada en la reforma comentada, si bien tiene un antecedente importante en el Convenio sobre Cibercriminalidad de Budapest (2001), que estableció entre las conductas a receptar por los códigos penales de los países integrantes de la Unión Europea la de *"posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos"*, ciertamente se trata de un tipo que merece un debate amplio que no difiere demasiado del genérico alrededor de las figuras de "tenencia" punibles y los delitos de peligro abstracto, que excede el objeto de este trabajo. Por lo pronto, la Sala 1 de la CNCyC, ha señalado que *"La figura de la distribución de imágenes*

---

[64] Cf. Vaninetti-Vaninetti, *"La posesión simple y preordenada de material con pornografía infantil. Internet: su incidencia. Necesidad de una doble inclusión en el Código Penal"*, pub. en "El Derecho Penal. Doctrina y Jurisprudencia", ED, Nº 7, julio de 2007, págs. 6/12.

[65] Con relación a lo procesal, valga una breve digresión. Según informan Pablo Guillermo Lucero y Alejandro A. Kohen, el tipo de tenencia de representaciones con fines de distribución o comercialización referido sería en la C.A.B.A. de competencia del fuero local según la inteligencia del Tribunal Superior de Justicia de la C.A.B.A. en causa *"Ministerio Público – Fiscalía ante la Cámara con competencia en lo Penal, Contravencional y de Faltas N° 1 s/queja por recurso de inconstitucionalidad denegado en: Incidente de incompetencia en autos 'NNs/inf. Art. 00 –presunta comisión de un delito-'"*, expte. N° 6397/09, fallo del 27/08/09 (en su trabajo titulado *"La tenencia de representaciones sexuales explícitas relacionadas con la pornografía infantil, en medios informáticos, a los fines de su distribución o comercialización (art. 128, 2° párrafo, del Código Penal Argentino"*, pub. en la biblioteca jurídica online "elDial.com" (www.eldial.com.ar), Suplemento de Derecho Penal y Contravencional de la C.A.B.A., edición del mes de diciembre de 2009, sección Doctrina, nota al pié N° 1)

*pornográficas de menores de dieciocho años de edad que regula el artículo 128, 2º párrafo del Código Penal, castiga la distribución de imágenes pornográficas de menores de dieciocho años de edad y no el mero hecho de recibir este tipo de fotografías. Es necesario no sólo recibir, sino además, enviar a otras personas imágenes pornográficas de menores de edad. Aquí también es importante señalar que la descripción penal alude a la voz distribución de imágenes, hecho éste que descarta el mero envío de textos sólo referidos a ella"*[66].

Con relación al 2° párrafo, a la par de destacar su carácter de delito de peligro abstracto y perseguible de oficio (acción pública), puntualizan Lucero y Kohen que el visualizar online las representaciones sexuales de pornografía infantil sin grabarlas no implica su tenencia y que, en el caso de que quedaran grabadas por la configuración técnica de la computadora en la memoria caché, podría sostenerse que media una tenencia provisoria que no se corresponde con la segunda exigencia típica, cual es la voluntad de comercializar o distribuir tales representaciones sexuales[67].

e. Daño en datos, documentos, programas o sistemas informáticos

La ley 26388 vino a cerrar entre nosotros una de las más antiguas polémicas en la temática sobre los alcances de los tipos tradicionales para aprehender las modalidades generadas por el avance tecnológico, que era la que giraba en torno del tipo de daño. En efecto, algunos autores estimaban que el art. 183 del C.P., al tipificar el daño a una cosa mueble,

---

[66] Fallo del 25/4/02, causa Nº 18108 "N., G.A.", citado por Donna, de la Fuente, Maiza y Piña, en su obra *"El Código Penal y su interpretación en la jurisprudencia"*, Rubinzal-Culzoni editores, Tomo II, arts. 79 a 161, Bs.As./Santa Fe, 2003, pág. 630. Allí, puede consultarse la síntesis del caso "M., E." de la Sala V del mismo Tribunal (fallo del 16/10/02, causa Nº 19902), que sobreseyó respecto de la conducta de distribución sobre la base de entender que pune algo más que el simple envío a un destinatario, sino que presupone un número indeterminado de receptores, el que fuera revocado por prematuro por la Sala 1 de la C.N. de Casación Penal.

[67] Cf. el cuerpo principal del trabajo ya individualizado. Ccte.: Palazzi, *"Los delitos..."*, ya citado, págs. 57/58, donde menciona con idéntico criterio jurisprudencia (US vs. Stullock) y doctrina norteamericanas (Matthew J. Zappen y Ty Howard), aunque aclara que en el caso "US vs. Tucker", a partir de que el imputado sabía de la existencia del "cache" y que las imágenes se almacenaban allí por defecto, se concluyó que sí se daban los elementos del tipo penal de tenencia de imágenes de pornografía infantil.

podía comprender algunas de las nuevas realidades. En este sentido, debe recordarse que nuestros tribunales consideran *"cosa"* a la electricidad, los pulsos telefónicos y las señales de televisión o de cable (arg. cf. art. 3211 C.C.). De allí derivaría una posibilidad de aprehender típicamente algunas de las actividades que desarrollan los llamados *crackers* y *cyberpunks* (vándalos). A efectos de superar naturales objeciones de analogía prohibida, se habían propuesto de lege ferenda como alternativas: a) La reforma de dicho artículo agregando *intangible* a la lista de elementos pasivos de daño ("...cosa mueble o inmueble o un animal *o intangible*..."), precisando a su vez en el art. 77 del mismo Código Penal que con este término se hace referencia a datos manejados en sistema informático e incluyendo en el listado de agravantes cuando el daño en el equipo influya decisivamente en lesiones o muerte a una persona (así, Pablo O. Palazzi y Fabián García[68]); b) dictar una nueva ley especial al respecto.

Jurisprudencialmente, en el caso *"Pinamonti"*[69], se concluyó:1) el software es una obra intelectual en los términos de la Ley 11.723 (tema superado cf. L. 25.036); 2) dicha ley no contempla como acción típica el borrado o destrucción de programas de computación dentro de su elenco de figuras penales (arts. 71/72, que no fueron modificados por la L. 25.036); 3) tal conducta tampoco es aprehendida por el delito de daño (183 C.P.), pues el concepto de cosa es aplicable al soporte (diskette o disco rígido) y no a su contenido (programas o datos almacenados en ellos). En lo que ahora interesa, esta tercera conclusión hace de este caso el primero de trascendencia pública que presentó el problema. Le siguieron otros en el mismo sentido y algunos en contradicción[70]. Nos

---

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

[69] Fallo de la Sala 6º, CNCyCorr., Cap. Fed., 30/4/93. Puede consultarse en *"Informática y D.P.A."*, ya citado, págs. 154/155. En 2003, la misma Sala 6º se había apartado del primer precedente, resolviendo en sentido contrario en causa "Kohler Antelo" (fallo del 24 de noviembre), con referencia a la información científica contenida en una página web, a la estimó susceptible de ser objeto del delito de daño ya que el art. 2323 del C.C., al efectuar una enunciación no taxativa de los bienes muebles, hace referencia a las colecciones científicas (síntesis pub. en la "Revista Nova Tesis de Derecho Penal y Procesal Penal", dirigida por Chiara Díaz y Erbetta, Nº 1, Rosario, 2007, pág. 6).

[70] Puede consultarse el detalle sintetizado por Palazzi (ya citado, 2006, págs. 676/679), donde se incluyen "Vecchio", "Gornstein" (al que hemos anotado en el artículo *"Hacking,*

remitimos a anteriores trabajos ya individualizados para ver en extenso toda la situación previa a la reforma.

Baste para cerrar esta breve ilustración del problema recordar que el anteproyecto de Ley de Reforma y Actualización integral del Código Penal de mayo de 2006, también se había ocupado del tema en los arts. 187 y 188. En efecto, en los *"Fundamentos"* se expresaba haber receptado *"la figura del daño tecnológico, tomando en cuenta fundadas opiniones jurisprudenciales y doctrinarias, que entienden a la información, el dato y/o las imágenes almacenados en programas o soportes informáticos como nuevos bienes jurídicos a tutelar. Se agregó igualmente una figura agravada concerniente a medios de comunicación, vías de agua y energía. También se acordó incluir entre los casos agravados el referido a daños de sistemas informáticos o bases de datos públicos"*[71]. El primero de los artículos proyectados decía: *"Será reprimido con prisión de quince (15) días a un (1) año, el que por cualquier medio destruya en todo o en parte, borre, altere en forma temporal o permanente, o de cualquier manera impida la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo o durante un proceso de transmisión de datos. La misma pena se aplicará a quien venda, distribuya, o de cualquier manera haga circular o introduzca en un sistema informático, cualquier programa destinado a causar daños de los prescriptos en el párrafo anterior, en los datos o programas contenidos en una computadora, una base de datos o en cualquier tipo de sistema informático"*, mientras que el segundo calificaba la conducta *"…f) Cuando el daño se ejecute en sistemas informáticos o bases de datos públicos, o relacionados con la prestación de un servicio público"*.

La reciente reforma, insistimos, ha solucionado el problema de recepción típica a través de sus arts. 10 y 11, que incorporan un segundo

---

*Cracking, E-mail y dos fallos judiciales que denuncian lagunas en la legislación penal argentina"*, pub. en la "Revista Jurídica de Mar del Plata", Nº 1, año 2002, Ed. Gowa/UFASTA, Bs.As., págs. 229/250 y en el portal jurídico www.carlosparma.com.ar, en la sección "Doctrina Penal", agosto de 2002), "Debandi", "Kohler Antelo" (mencionado en la nota al pié anterior) y "Marchione" (que personalmente comentamos en el trabajo *"Algo más sobre el daño y sabotaje informáticos (en función del criterio de la Cámara Federal Criminal y Correccional)"*, pub. en "El Derecho Penal", dirigida por Carlos A. Mahiques, E.D., enero de 2006, pág. 5 y ss.).

[71] Pub. antes mencionada, considerando XV, pág. 231.

párrafo al art. 183 y sustituyen al art. 184, respectivamente, consagrando la siguiente redacción (en lo que aquí nos interesa):

> "Artículo 183: *"… (segundo párrafo) En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños"*.
>
> *"Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:...*
> *5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;*
> *6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".*

Comentando el texto agregado al art. 183, Palazzi aclara que en el contexto informático, "destruir" o "inutilizar" quiere decir borrar definitivamente sin posibilidad de recuperación. El hecho que exista un sistema de back-up no altera el delito de daño pues la restauración requiere un esfuerzo que ya implica reparar el daño causado[72]. En cuanto a su parte final, se trata con evidencia de la consagración de un delito de peligro al considerar que quien vende, distribuye, hace circular o introduce en un sistema informático un "virus", aún cuando en concreto no se utilice, será punible. Es que salvo aislados casos en que hay un interés académico mediante (que, sin dudas, quedarían fuera del alcance de la figura por inadecuación típica subjetiva), esta clase de programas están inequívocamente destinados a dañar. Naturalmente, cuando aludimos al interés académico no nos estamos refiriendo a las consignas —que Durrieu y Lo Prete califican de "escandalosas"— del tipo "sólo con fines educativos" que usan algunas páginas webs dedicadas a "instruir"

[72] En *"Análisis del proyecto…"*, pág. 19; en *"Análisis de la ley…"*, pág. 1220.

y proporcionar medios para "hackear". No se trata de habilitar la posibilidad de "educar para el delito"[73].

En el marco de un avance tecnológico incesante, el registrado en la telefonía celular ha provocado la proliferación de virus en tales aparatos, al punto que incluso se los cataloga o bien por su forma de infección en virus de fichero, de sector de arranque, de tabla de partición, de macro y multipartitas, o bien por su nivel de peligrosidad tecnológica (símil con la biología) en nivel de "tecnopeligrosidad" 1, 2, 3 o 4[74]. Vale aclarar que los "Servicios de comunicaciones móviles" tienen un régimen de protección penal bastante detallado por la ley 25891[75], que atribuye a la competencia federal (art. 15) el conocimiento de los delitos tipificados en sus arts. 10 a 14, por lo que la referencia a sistemas informáticos de comunicaciones de la nueva regla trascripta antes operaría en sentido residual respecto de este régimen especial[76]. Tanto la clonación de celulares como la

---

[73] Durrieu, Roberto y Lo Prete, Justo, en su artículo *"Delitos Informáticos"*, pub. en L.L., diario del 1/2/02, pág. 2. Palmario ejemplo de este orden de problemas es el recordatorio de Nehemias Gueiros Jr., cuando informa de casos como el del famoso programa creado por el grupo de hackers "Cult of the Dead Cow" (Culto de la vaca muerta) llamado "Back Orifice" (entrada o puerta trasera), para espiar en forma remota las claves tecleadas en una máquina, que está disponible gratuitamente en Internet, así como otras herramientas similares como el "Sub-seven". Sitios que auxilian a planear ataques a otros computadores como hack.co.za o astalavista.box.sk, hacen realidad la idea de que cualquiera que sepa teclear es capaz de producir alguno de estos comportamientos ilícitos, lo que lleva a concluir al autor citado que esto prueba que Internet es realmente incontrolable (en su artículo *"Insegurança na Internet: há remédio?"*, pub. en el portal jurídico "Mundo Jurídico" –www.mundojuridico.adv.br—, en 30/7/03.

[74] Cf. ilustra Tomás Martín Morello en su trabajo *"Los aparatos de telefonía celular como objetos e instrumentos de los delitos informáticos"*, publicado en el Suplemento de Derecho de la Alta Tecnología de la Biblioteca Jurídica Online "elDial.com" (www.eldial.com.ar), edición del 30 de junio de 2008.

[75] Pub. en el B.O. del 24/5/04.

[76] El art. 10 de la ley 25891 prevé prisión de un mes a seis años para *"el que alterare, reemplazare, duplicare o de cualquier modo modificare un número de línea, o de serie electrónico, o de serie mecánico de un equipo terminal o de un Modulo de Identificación Removible del usuario o la tecnología que en el futuro la reemplace, en equipos terminales provistos con este dispositivo, de modo que pueda ocasionar perjuicio al titular o usuario del terminal celular o a terceros"*. Con igual pena el art. 11 reprime al *"que alterare, reemplazare, duplicare o de cualquier modo modificare algún componente de una tarjeta de telefonía, o accediere por cualquier medio a los Códigos informáticos de habilitación de créditos de dicho servicio, a efectos de aprovecharse*

adquisición a sabiendas de celulares robados han tenido al presente tratamiento tribunalicio[77].

Autores como Demócrito Reinaldo Filho destacan incluso la posibilidad mediante virus del tipo "troyano" de virtualmente "secuestrar" el computador de un tercero y, desde ése, realizar maniobras ilícitas. Asimismo, hace hincapié en diversas cuestiones de prueba vinculadas a esta maniobra generadas en casos judiciales conocidos, como el caso inglés "Aaron Caffrey", en el que este joven de 19 años imputado bajo los términos de la ley de crímenes informáticos ("Computer Misuse Act") de "hackear" el servidor de una empresa finalizó absuelto (en octubre de 2003), bajo la alegación de haber sido tomado su computador por un virus troyano y, de esa forma, utilizado por un tercero para cometer el hecho que se le atribuyera. La falta de señales del virus en su computador, encontró por respuesta que este se autodestruyó después de la realizar la operación, lo que fuera admitido como explicación razonable por el jurado popular interviniente. El nombrado, propone como solución para esta dificultad forense la alteración de los principios tradicionales que rigen el "onus probandi" en el proceso penal, postulando en definitiva la inversión de la carga de la prueba en los casos en que se ensaye este tipo de defensa[78].

---

*ilegítimamente del crédito emanado por un licenciatario de Servicios de Comunicaciones Móviles (SCM)".* La pena será de seis meses a tres años, conforme el art. 12, para *"el que, a sabiendas de su procedencia ilegítima, adquiriere por cualquier medio o utilizare terminales celulares, Modulo de Identificación Removible del usuario (tarjetas de telefonía) o la tecnología que en el futuro la reemplace",* incrementándose a uno a seis años si ello se realizare con ánimo de lucro (art. 13 inc. a), o si cualquiera de los delitos anteriores fuere medio para perpetrar otro delito (art. 13 inc. b). Agravante genérico que incrementa las penas mínimas y máximas en un tercio constituye la autoría por dependientes de empresas licenciatarias de SCM o por quienes, atento al desempeño de sus funciones, posean acceso a las facilidades técnicas de aquellas.

[77] El "supra" citado Morello recuerda la sentencia condenatoria de mayo de 2008 respecto de la conducta de "clonación de celulares" dictada la causa N° 760/06 del Tribunal Oral en lo Criminal Federal N° 3 de Capital Federal, "Madkour" (elDial, AA34A3), y la opinión de la Sala 1 de la CNCyCFed en un procesamiento por presunta infracción al art. 12 de la ley 25891, resolución del 8/11/07, reg. N° 1323, "Remolina".

[78] Cf. su artículo *"Questões técnicas dificultam condenações por crimes cometidos na Internet"*, pub. en el portal "Mundo Jurídico" (www.mundojuridico.adv.br), el 28 de noviembre de 2003. Recuerda allí, además, dos absoluciones inglesas en similares términos en casos en

No es este el lugar para desarrollar este tema, pero simplemente adelantamos nuestra discordancia con este tipo de soluciones que buscan aumentar la efectividad en términos de condena pero a costa de sacrificar garantías cuyo reconocimiento ha sido el fruto de mucho sufrimiento y trabajo. Así, desde nuestra modesta perspectiva, el camino a seguir habrá de ser el dotar a la persecución pública de cuerpos especializados que estén a la altura de los desafíos técnico-periciales que se debe afrontar y capacitar a nuestros fiscales para que presenten el caso a juzgar con solidez, con una adecuada valoración de la prueba directa e indiciaria que se pueda obtener, sin resignar principios basales de un sistema procesal acusatorio, que es el que corresponde a un Estado de Derecho.

f. Comunicaciones vía electrónica

Existen muchas y variadas formas de comunicación electrónica. Siguiendo a Pablo Farrés puede recordarse como las más corrientes a los correos electrónicos, pero también lo son el acceso a un casillero personal de comunicación en una página web, la telefonía IP y las comunicaciones online como el Chat. Enfatiza que *"La comunicación electrónica es un género tan amplio que no reconoce limitación en el medio de transporte o de comunicación por el cual se realiza, bastando con que sea mediante un flujo eléctrico, comúnmente nanoeléctrico. Por ello puede ser una transmisión bajo redes abiertas o cerradas, fuera de redes, mediante comunicación alámbrica o inalámbrica, telefónica o de otra especie. Así, por ejemplo, un mensaje de texto en un celular (conocido vulgarmente bajo la sigla "SMS") también sería comunicación electrónica"*[79].

Las conductas disvaliosas respecto de las comunicaciones vía electrónica son consideradas en la reciente reforma argentina desde dos perspectivas: las que afectan el secreto y la privacidad, y las que conciernen a la seguridad del medio de comunicación mismo. En consecuencia, se han sustituido o incorporado tipos en los capítulos respectivos de la parte especial.

---

que se investigaban hechos de "pedofilia", concretamente, bajar desde la red pornografía infantil.

[79] En su trabajo *"La reforma de la ley 26388 al Código Penal. Los nuevos delitos informáticos"*, pub. en J.A. 2008-IV-1375. La cita textual corresponde al punto IV.

f.1. En lo que hace a la "Violación de secretos y de la privacidad", una de las discusiones concluidas ha sido la concerniente la protección o desprotección penal del correo electrónico[80]. Fueron numerosos los proyectos con estado parlamentario elaborados al respecto desde fines de la década pasada. Entre los últimos, aún cuando no llegara a dicho estadio de tratamiento, puede mencionarse que fue objeto de consideración en el ya referido anteproyecto de Ley de Reforma Integral y Actualización del Código Penal, cuyos arts. 138, 139, 142 y 143 lo incluyeron del siguiente modo: art. 138 (figura básica), *"…el que abriere indebidamente una carta, un pliego cerrado o un despacho telegráfico, telefónico, mensaje de correo electrónico o de otra naturaleza que no le esté dirigido; o se apoderare indebidamente de una carta, de un pliego, de un mensaje de correo electrónico, de un despacho o de otro papel privado, aunque no esté cerrado; o suprimiere o desviare de su destino una correspondencia o mensaje de correo electrónico que le esté dirigida…"*, calificando la conducta *"…si el culpable comunicare a otro o publicare el contenido de la carta, escrito, mensaje de correo electrónico o despacho"*; a su vez, el art. 139 califica la acción para *"…el que por su oficio o profesión se apoderare de una carta, de un pliego, de un telegrama o de otra pieza de correspondencia o de un mensaje de correo electrónico.- También si se impusiere de su contenido, la entregare o comunicare a otro que sea el destinatario, la suprimiere, la ocultare o cambiare su texto..."*.

El citado art. 142 del anteproyecto dice: *"…el que indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro tipo de envío de objetos o transmisión de imágenes,*

---

[80] Entre los fallos publicados más recientes que patentizaron las divergencias puede contarse el del Juzgado Nacional Correccional Nº 9, a cargo de la Dra. Ana H. Díaz Cano, causa "N/N", sentencia del 11/4/07, donde concluyó que el acceso indebido a una cuenta de correo electrónico mediante la utilización de un mecanismo tendiente a sortear la clave y la posterior presentación en un juicio civil de información que se encontraba archivada en esa cuenta, no encuadra en el delito de violación de correspondencia del art. 153 del CP, pues lo violado no fue una correspondencia, sino simplemente datos almacenados en una casilla de correo, ni tampoco se incurre en el delito del art. 157bis del mismo código, pues la casilla de correo "hackeada" y los datos dados a conocer no constituyen una base de datos personales ni la revelación de la información registrada en un sitio de esas características (pub. en LL, diario del 30 de julio de 2007, págs. 7/11). Remitimos para mayor detalle a las obras personales ya individualizadas, particularmente *"Protección de la intimidad…"*, donde se aborda el tema a partir del comentario al conocido caso con interpretación en contrario "Lanata" del año 1999.

*voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuviesen dirigidos…"*, agravando si el autor fuere funcionario público o integrante de las fuerzas armadas o de seguridad; y el art. 143 pune *"…el que, hallándose en posesión de una correspondencia o mensaje de correo electrónico no destinado a la publicidad, lo hiciere publicar indebidamente, aunque haya sido dirigido a él, si el hecho causare o pudiere causar perjuicios a terceros"*.

Dejando de lado una enumeración de iniciativas antecedentes que sería realmente extensa, pasamos al texto ahora vigente. La ley 26388 sustituyó por su art. 4 al 153 del C.P., mientras que por el 6° hizo lo propio respecto del art. 155. Estos dicen:

> *"Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.*
> *En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.*
> *La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.*
> *Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".*
>
> *"Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o*

*de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.*
*Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público".*

Como puede advertirse, no hay diferencia sustancial con el ante-proyecto, ya que las conductas de los arts. 142 y 143 de este último se encuentran incluidas en el segundo párrafo del art. 153 transcripto y en el 155. Si nos centramos en el art. 153, a la conducta de abrir se ha adicionado con relieve típico la de acceder indebidamente, lo que se ajusta a la actualización de objetos al incorporar las comunicaciones electrónicas y recoge una crítica que entendíamos insalvable para quienes proponían sobre la base de una interpretación histórica extensiva la suficiencia del texto anterior (era claro que "acceder" no es lo mismo que "abrir" y que no se podía "abrir" un mensaje que no estaba "cerrado").

En los términos actuales, resulta evidente que el legislador no se ha limitado al correo electrónico, sino que se adoptó una terminología de mayor amplitud como "comunicación electrónica" y, en concreto en el segundo párrafo, alude a "telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido", para acentuar el espectro de actividades del ámbito de la privacidad cuya apertura, acceso, apoderamiento, supresión, desvío, interceptación, captación, comunicación a terceros o publicación sean punibles.

Recuerda Palazzi que la "ratio legis" del último párrafo del art. 153 fue la intención de evitar la interceptación y acceso no autorizado a correos electrónicos de jueces y periodistas, según fuera ampliamente difundido por la prensa a mediados del año 2006. Destaca asimismo, la reiteración de la voz "indebidamente" en el texto, lo que pondera en cuanto refuerza la exclusión de toda posibilidad de imputar el delito en forma culposa y aventa el temor de algunos empresarios del sector que temían se pudiera aplicar esta figura a un ISP o proveedor de servicio de correo electrónico que desviare un e-mail por contener un virus o porque algún algoritmo o filtro lo clasifica como "spam"[81].

[81] En *"Análisis del proyecto…"*, ya citado, pág. 10. Así lo reitera en *"Análisis de la ley 26388…"*, ya citado, pág. 1216.

La publicación abusiva de correspondencia es también actualizada para que alcance a la "comunicación electrónica". Se ha agregado el último párrafo, que reconoce por origen la misma situación anteriormente mencionada y que, señala Palazzi, reproduce la idea subyacente en el art. 111 inc. 1° del C.P. (tipo de "calumnias"), al eximir de responsabilidad penal a quien revela correspondencia con la inequívoca intención de proteger el interés público[82]. Coincidimos en que resulta razonable y entendible el contexto en que se sancionó la norma, lo que no evita la inseguridad cierta que conlleva cualquier alusión a situaciones de dificultosa determinación o definición, como qué es el "interés público" que se intenta proteger.

f.2. Con respecto a la modificación en materia de "Delitos contra la seguridad de los medios de transporte y de comunicación", se ha sustituido (cf. art. 12, L. 26388) el texto del art. 197 del C.P. —"Interrupción o resistencia al restablecimiento de las comunicaciones—", por el siguiente:

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

Palazzi lo llama "daño a las comunicaciones" —preferimos su designación tradicional—, aclarando que incluye a las de cualquier clase y no sólo ampara la público sino cualquier clase de comunicación incluyendo las privadas como el e-mail, la voz a través de IP o los mensajes de chat o de texto a través de celulares (SMS)[83]. Si se compara con la redacción anterior, sólo se ha agregado "o de otra naturaleza", abriendo el tipo que se hallaba ceñido a la comunicación telegráfica y telefónica. Aquella fue objeto de gran discusión en torno a su conveniencia y ubicación sistemática, al punto de haber sido derogada la figura en varias ocasiones. Sin embargo, pareció primar finalmente la postura de quienes, como Eusebio Gómez, consideraban su inclusión justificada entre los delitos contra la seguridad pública, atendiendo a que las

---

[82] En *"Análisis del proyecto…"*, pág. 14.

[83] En *"Análisis del proyecto…",* pág. 23; en *"Análisis de la ley…"*, pág. 1220.

comunicaciones telegráficas y telefónicas *"resultan elementos indispensables en la vida contemporánea"*[84]. Si esta afirmación podía validarse en el momento en que se expresó (década del cincuenta), tanto más cuando se vive la "era de la comunicación y la información". En cuanto a la preferencia personal anticipada, se impone porque como señalan Estrella y Godoy Lemos, estamos frente a un artículo que contempla dos acciones típicas distintas que constituyen dos figuras autónomas entre sí: la primera consiste en interrumpir (es decir, cortar, detener, paralizar, suspender) o entorpecer (es decir, estorbar, dificultar, retardar, obstaculizar, sin llegar a interrumpir) la comunicación; la segunda, en resistir violentamente su restablecimiento (por un sujeto activo que puede o no ser el mismo que interrumpió la comunicación antes, pero si lo fuera, mediaría un concurso real ya que la primera acción no supone la segunda), es decir, ejerciendo violencia sobre las personas que procuran restablecer el servicio o fuerza en las cosas, como al destruir las reparaciones ya efectuadas[85].

Natural derivado de la reforma parcial, se ha mantenido sin adecuar el tipo del art. 192, que pune en forma autónoma al que ejecutare cualquier acto tendiente a interrumpir el funcionamiento de un telégrafo o teléfono destinado al servicio de un ferrocarril.

Podemos cerrar el punto recordando que el antes citado anteproyecto de reforma integral argentino se dedicó con mayor extensión y precisión al entorpecimiento de las comunicaciones, tipificando variadas conductas en los arts. 228 a 230. El primero dice lo siguiente: *"…el que interrumpiere o entorpeciere toda comunicación transmitida por cualquier medio alámbrico o inalámbrico, o resistiere violentamente el restablecimiento de la comunicación interrumpida"*. El art. 229: *"…el que alterare, reemplazare, duplicare o de cualquier modo modificare un número de línea, o de serie electrónico o mecánico de un equipo terminal o de un Módulo de Identificación Removible del usuario, de modo que resulte perjuicio al titular, usuario o terceros"*. El último contempla la punición para *"…el que alterare, reemplazare, duplicare o de cualquier modo modificare algún componente de alguna tarjeta de telefonía o accediere por cualquier medio a los códigos*

[84] Cf. citan Estrella y Godoy Lemes, ob.cit., Tomo 3, pág. 148.

[85] Antes citados, págs. 148/149.

*informáticos de habilitación de créditos de dicho servicio, a efectos de aprovecharse ilegítimamente del crédito emanado por un licenciatario de Servicios de Comunicaciones Móviles".*

g. Intrusismo informático

Habíamos señalado en su oportunidad que si bien el anteproyecto de Ley de Reforma Integral y Actualización del Código Penal argentino había avanzado en la solución de varios de los vacíos legales denunciados en la legislación penal, autores como Palazzi criticaban que en su art. 146 se mantuviere la tipificación del acceso ilegítimo a un banco de datos (introducida por Ley 25.326), pero no a la conducta más amplia de acceso a un sistema informático, apuntando que en el año 2005 cerca de 50 países legislaron como delito el acceso no autorizado a sistemas informáticos[86]. Esta idea vinculada con la noción de obligada armonización regional, el efecto criminógeno de las conductas de hacking y la importancia de proteger no sólo administrativamente la función social que desempeña el bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticas, impulsan a María Ángeles Rueda Martín ha expedirse también en el sentido de la necesidad de represión penal autónoma de las conductas de accesos ilícitos a sistemas informáticos[87]. Por nuestra parte, indicamos la conveniencia de profundizar la discusión sobre una alternativa que entendíamos viable, como la de intentar primero una contención por vía contravencional. La Ley 26388, por su art. 5 lo ha incorporado al código sustantivo como nueva figura mediante el art. 153 bis, con el siguiente texto:

> *"Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.*

---

[86] Palazzi, *"Breve comentario…"*, ya citado, pág. 1531.

[87] Rueda Martín, *"Los ataques contra los sistemas informáticos. Conductas de hacking. Cuestiones político-criminales"*, pub. en la "Revista Jurídica Online", Facultad de Jurisprudencia y Ciencias Sociales y Políticas de la Universidad Católica de Santiago de Guayaquil, Sección Artículos, "Derecho Penal" (www.revistajuridicaonline.com). Versión en papel de la "Revista Jurídica" N° 26, 2009, págs. 190 y ss.

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

El primer párrafo, que consagra la punición como conducta básica de quien con conocimiento y sin autorización o excediéndola[88], accede por cualquier medio a un sistema o dato informático de acceso restringido, al indicar *"si no resultare un delito más severamente penado"* fija con claridad el carácter subsidiario asignado a la figura, lógico si se atiende a que, en general, en el derecho comparado, se ha entendido que estamos frente a una conducta de "antesala" cuya punición ha sido producto de gran discusión. El segundo párrafo duplica la pena cuando el acceso fuere respecto de un sistema o dato informático de un organismo público estatal o un proveedor de servicios públicos o de servicios financieros. La distinción aparece razonable.

Sin embargo, entendemos que habiéndose optado por la criminalización de esta conducta disvaliosa resignando la vía contravencional, al menos podría haberse evitado la utilización de la pena privativa de libertad en la figura básica. Es claro que no sólo en el imaginario colectivo, sino en la mente del legislador, sigue instalada férreamente la idea de que "penar" significa "privar de libertad". No albergo dudas de que estamos frente a una conducta que tendría una respuesta punitiva más racional si se la hubiese conminado con multa o alguna inhabilitación especial o alternativa reparatoria.

Con la precisión de "acceso restringido" contenida al cierre del primer párrafo, se excluye la posibilidad de punir el acceso a redes, sistemas y

[88] Carranza Torres, Pereyra Rozas y Bruera, apuntan que el "exceso" en la autorización que se tiene es muy común en los ámbitos empresariales, en los que un directivo o empleado autorizado para acceder sólo a determinados sistemas, a determinado sector o a determinados datos o archivos, viola la directiva del empleador y accede a sistemas, partes de sistemas, datos o archivos respecto de los cuales carece de autorización. Naturalmente, se requerirá que el administrador del sistema haya adoptado los correspondientes recaudos o medidas de seguridad, como passwords, claves de acceso, etc. (en su trabajo *"La Ley de Delitos Informáticos 26388"*, pub. en JA 2008-III-647 y disponible en el sistema online de LexisNexis Argentina bajo referencia Lexis N° 0003/013978).

contenidos de sitios públicos. Destaca Palazzi que también quedan fuera del ámbito típico conductas como: a) la del testeo de seguridad de falencias de redes informáticas ("ethical hacking") en el marco de investigación académica, casera o empresaria, muchas veces realizado además con consentimiento de la "víctima", interesada en la detección de errores para su subsanación; b) la ingeniería inversa o reversa, que es la destinada a obtener información técnica a partir de un producto accesible al público (como programas de computación y componentes electrónicos), con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado, actividad que evidentemente no se relaciona con la "privacidad" sino, a todo evento, con la protección de la propiedad intelectual (ámbito en el que se encuentran reguladas sus limitaciones, recordando el nombrado que nuestro país, pese a haber aprobado el "Tratado de Derecho de Autor de la OMPI del año 1996", no lo ha reglamentado aún ni en lo civil ni en lo penal, por lo que bien podría incluirse este tema en el siguiente acápite, destinado a aquellos problemas que no tienen clara solución)[89].

### IV. Algunos problemas sin solución clara

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

A modo de simple enunciación de otros problemas, en el ámbito nacional —sin perjuicio de la significativa actualización que importó la Ley 26388—, siguen abiertas a interpretaciones divergentes cuestiones como de la tipificación o no del registro impropio de nombres de dominio (ciberocupación[90]) o del spamming (correo basura o publicidad no

---

89 En *"Análisis del proyecto…"*, ya citado, pág. 13; en *"Análisis de la ley…"*, pág. 1217.

90 Sobre el particular puede consultarse el exhaustivo trabajo de Eduardo G. Farah, *"El derecho penal frente al registro irregular de nombres de dominio en Internet"*, pub. en E.D., t. 197 (2002), págs. 954/968 (1º parte) y 1106/1118 (2º parte). Allí, luego de historiar el desarrollo internacional de la cuestión, su encarrilamiento por vías de resolución

solicitada[91]). Sobre la entidad cuantitativa que ha adquirido en el tráfico de e-mails el "spam", se ha presentado un reciente informe por "SophosLab" que determina que en el primer trimestre de 2008 ha encontrado diariamente 23.300 páginas web relacionadas con correos no deseados, lo que importa una nueva por cada 3 segundos. Su red de captura global de spam arrojó que un total del 92,3 % de todo el correo electrónico enviado en dicho trimestre era correo basura. El país más emisor de spam es USA (15,4

administrativa y/o civiles y comerciales, destaca la casi absoluta prescindencia por los actores de explorar la legislación penal involucrada, lo que califica de llamativo si se tiene en cuenta que se habla habitualmente de "uso indebido" o "fraudulento" o "de mala fe" de una marca, de "maniobra extorsiva" o "chantaje cibernético", de "piratería marcaria" (pág. 961). Hemos expuesto en varias ocasiones nuestra opinión sobre la atipicidad de la conducta a la luz del derecho penal marcario argentino, en concreto, del art. 31, inc. b), Ley 22362 (la última, en "Derecho Penal Económico y Delincuencia Informática", pub. en AAVV "Derecho Penal Económico", Fabián I. Balcarce director, Ed. Mediterránea, Córdoba, Tomo 3, 2006, págs. 233/236), conclusión que coincide parcialmente con la expresada por el nombrado (ver págs. 966 y 1108, donde luego de coincidir en general se exponen supuestos de tipicidad). Sin perjuicio de ello, advierte también distintas modalidades típicas respecto de las que esta conducta podría ser un primer paso. Así, por ejemplo, para defraudaciones básicas del art. 172 del CP o a la propiedad intelectual del art. 72bis, inc. c), Ley 11723 (ver pág. 1108) o para la competencia desleal del art. 159 del CP (pág. 1109).

91 Sobre los proyectos legislativos al respecto hemos informado en el artículo antes citado pub. en EDP, enero de 2006, págs. 25/26 y, previamente, tratamos su problemática en nuestra obra *"Protección penal de la intimidad en el espacio virtual"*, Ediar, Bs.As., 2002. Saliendo de la perspectiva penal, como señala Hugo A. Vaninetti, en Argentina no existe ninguna ley anti-spam, pero la LPDP Nº 25526 en su art. 27 posibilita una solución parcial (cita en apoyo la opinión de Fernández Delpech), cual es que cualquier persona cuyos datos figuren en una base de datos con fines de publicidad puede exigir en cualquier momento que sean retirados de la misma, lo que si no se cumple genera sanciones económicas y hasta la misma cancelación de la base de dato (en su trabajo *"Derecho a la intimidad e internet"*, pub. en JA, 2005-I, fascículo Nº 2, pág. 13). Naturalmente, quedan fuera los casos en que no se trata de ese banco de datos. Antes que el autor nombrado se había expedido en similar sentido Palazzi, diciendo que *"Los usuarios de internet tienen derecho a no recibir correos electrónicos no solicitados, pues... la ley argentina de Protección de Datos Personales recepta la doctrina del* opt-in *para el* spam*"* (en *"Aspectos legales del correo electrónico no solicitado (derecho a enviar, derecho a no recibir y a no distribuir correo electrónico"*, pub. en J.A., 2004-I, fascículo 6, pág. 22). En el caso de Brasil, según informa Rita de Cássia Lopes da Silva, hay un proyecto de ley, el 6210/02 elaborado por Ivan Paixao, limitando y criminalizando el envío de spam por Internet en su art. 5 con pena de hasta ochocientos (800) reales por cada mensaje, aumentado en un tercio en caso de reincidencia (ya citada, págs. 52 y 140/141).

%), seguido de Rusia (7,4 %), Turquía (5,9 %), China (5.5 %) y Brasil (4,3 %). Ningún otro de nuestra región figura entre los once primeros (que generan el 63,2 % del total)[92].

Asimismo, como es resaltado por Palazzi, se optó por no incorporar una figura que preveía el proyecto original de la Cámara de Diputados, la captación ilegal de datos, imágenes y sonidos y posterior difusión (art. 6° de esa iniciativa), en la inteligencia de que se trata de una cuestión controversial no estrictamente vinculada a la consideración de las nuevas tecnologías al digesto sustantivo[93]. En efecto, no puede pasar por alto la confluencia de diversos intereses a compatibilizar. De un lado, la necesidad de mantener adecuadamente cubierta la expectativa de respeto al derecho a la intimidad, a la privacidad, propia de un estado de derecho. Del otro, el conciliarla con el interés en el esclarecimiento de ámbitos de criminalidad ejecutados en general en las "sombras", como los casos de corrupción, en muchas ocasiones puestos a la "luz" por la tarea del periodismo de investigación que, al interés público, adiciona la libertad de prensa, de informar y también la libertad expresión.

Finalmente, con relación a todo el orden de problemas aún no considerados, parece importante recordar algo que no siempre se ha tenido presente aunque, en el fondo, resulte desde la academia la insistencia sobre un lugar común. Como apunta Arocena, *"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"*[94].

---

[92] Fuente: "DiarioTi", edición del 23/4/08, reproducido en la sección noticias de la revista electrónica "AlfaRedi", ya citada, el día 25/4/08.

[93] En *"Análisis del proyecto…"*, pág. 17; en *"Análisis de la ley…"*, pág. 1219.

[94] Gustavo A. Arocena, *"Acerca del principio de legalidad penal y de hackers, crackers, defraudadores informáticos y otras rarezas"*, pub. en portal jurídico del Centro de Investigación Interdisciplinaria en Derecho Penal Económico (www.ciidpe.com.ar), sección temática 2, "Derecho Penal Económico. Parte Especial". La cita corresponde al punto II, donde reclama asimismo la profunda reflexión acerca de las posibilidades del sistema jurídico de hacerse cargo de la incidencia de los progresos tecnológicos previo a la elaboración de nuevas normas. Habla de una suerte de criterio corrector, una regla que dijera: *"tantas nuevas reglas del Derecho penal para las conductas nocivas de la tecnología*

## V. Valoración inicial del texto legal reformista

Más allá de la limitación que impone lo que no es más que la noticia con brevísimo comentario del cuadro normativo local y que priman algunas remisiones a trabajos previos así como el rápido pasaje sobre muchos aspectos en una temática ciertamente variada y compleja, se pueden reafirmar las siguientes observaciones:

a) Asumiendo que el presentado a discusión Anteproyecto de Reforma y Actualización integral del Código Penal Argentino en el año 2006, sólo la ha generado en el ámbito académico, ya que en el político se negó al día siguiente de su conocimiento público —no habiendo logrado estado parlamentario—, sus aportes para la solución a algunas de las lagunas de punibilidad en su oportunidad denunciadas en el derecho interno han quedado ahora parcialmente reflejados por la Ley 26388 que, en realidad, se apoyó en otras iniciativas y abordó un abanico de conductas mayor con redacción propia. Esta, junto a las recientes N° 26362 y 26364, 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.

b) Sin perjuicio de ello, debe resaltarse que la Ley 26388 ha significado un sustancial avance sobre temas cuya consideración venía siendo reclamada desde mucho tiempo atrás, poniendo fin a antiguas discusiones jurisprudenciales y doctrinarias. Ello, sin perjuicio de algunos defectos que fuimos puntualizando y requerirán, seguramente, en el futuro nuevo debate y actualización[95]. 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.

c) Finalmente, el "aggiornamiento" de la legislación fondal pone de algún modo en evidencia que ha quedado como suerte de asignatura

---

*informática, cuanto inidóneas sean las reglas vigentes del ordenamiento jurídico penal para hacerles frente".*

[95] Ccte.: Palazzi, *"Análisis de la ley…"*, pág. 1222.

pendiente el correspondiente al ámbito procesal. Como señala Esther Morón Lerma, confluyen a instar la actualización en materia procesal factores diversos que van desde los problemas derivados del carácter trasfronterizo de los ilícitos informáticos, que complejiza su investigación requiriendo mayor cooperación judicial y policial y mayor inversión en unidades especializados para ello, hasta las importantes peculiaridades en materia de prueba, que demandan la adopción de nuevas reglas de juego en materia de prueba digital[96]. Téngase presente que, al igual que lo puntualiza la nombrada en su referencia al derecho español, en el nuestro también carecemos de normas precisas que regulen el modo en que deben producirse las intervenciones en las comunicaciones electrónicas, clonarse un disco rígido o leer un mensaje de un sms de un teléfono celular.

[96] Cf. su trabajo *"Delincuencia informática"*, pub. en la "Revista del Ministerio Público", Procuración General ante la SCJBA, La Plata, Año 6, N° 10, noviembre de 2009, pág. 24.