UNIVERSIDAD SIGLO 21

DELITOS INFORMÁTICOS

Especial atención a las leyes 26.388 y 26.904

Autor: Yair Turnes.

Año: 2016.

Carrera: Abogacía.

UNIVERSIDAD SIGLO 21

RESUMEN

En el presente trabajo se analizarán los denominados “delitos informáticos”, contemporáneos de la era de la información. Se estudiará brevemente el vocabulario propio de la temática, y se intentará dar una definición de autor para dichos delitos. En el nudo, se investigarán, uno por uno, los tipos penales relacionados con la materia bajo estudio, creados a partir de la ley 24.766 y hasta la novedosa ley 26.904, su relación con el Convenio de Ciberdelito de Budapest, como así también se analizarán cuestiones procesales aparecidas a partir de la existencia de nuevos medios de almacenamiento, transporte y existencia de datos. Finalmente, se verificarán cuáles son los desafíos que deben afrontarse en la materia, y se intentará intentando plasmar cuáles son las conductas que merecen, prontamente, atención legislativa en materia penal.

ABSTRACT

This work will analyse the so called “cyber crime”, in the contemporary information age. The main vocabulary of the theme will be briefly discussed and will attempt to give a copy right definition for such crimes. In the very centre of this paper the criminal offences related to the subject under study; created from the 24.766 law and up to the new novel 26.904 law, its relationship to the Budapest Agreement, as well as legal procedural issues, starting from the existence of new storage media transport or transmisson and existence of data. Finally there will be an attempt to find out which are the challenges that need to be met in the field. There will be an attempt to show which are the conducts that deserve promptly legislative attention in penal matter.

UNIVERSIDAD SIGLO 21

INDICE

INTRODUCCIÓN

Hace poco más de 30 años que la sociedad mundial ingresó de lleno en un proceso de revolución. Un proceso de revolución tecnológica.

En ese marco, la aparición de nuevas formas de comunicación y de información provocó, en un corto período de tiempo, y en forma intempestiva, el surgimiento de un abanico de lo más variado de conductas humanas.

Entre dichas conductas, se encuentran aquellas que la sociedad, poco a poco, fue considerando e identificando como más ofensivas, y propias del reproche penal.

Así, cuando se piensa en "delitos informáticos", la primer imagen que puede venir a nuestra mente es la de una persona huraña, abandonada, que desde la oscuridad de un habitación hacinada planifica un ataque con su computadora destinado a desviar dinero hacia sus cuentas de banco; o dispuesta desde dicho lugar a ingresar a las bases de datos mas protegidas del mundo.

Sin embargo, la problemática de los delitos en tecnologías es lejana a dicho paradigma, pero a la vez, más grave y cotidiana.

En efecto, en el año 1994 sólo 0,4 personas por cada 100 (de la población mundial) era usuaria de internet, en 2004 dicha suma ascendió a 14,2, en tanto en el año 2014 la cifra ya ascendía a 40,7, resultando un incremento exponencial y extremadamente veloz (datos estadísticos elaborados por el Banco Mundial). En Argentina, dichas cifras fueron 0 en 1994, 16 en 2004 y 64,7 en 2014.

En base a ello, y dado el alcance de la temática, el trabajo tendrá por objeto resaltar cuáles son las nuevas conductas disvaliosas que han aparecido en razón del avance de las Tecnologías de la Información y la Comunicación, dando lugar al nacimiento de los "delitos informáticos".

Asimismo, se analizará cuál ha sido la respuesta legislativa a las problemáticas surgidas por dichas conductas, y se estudiarán, como parte central del trabajo, los tipos penales que fueron siendo creados e incorporados a nuestro derecho penal de fondo.

En ese sentido, se diferenciarán dos tipos de delitos relacionados con las tecnologías: los que tienen a los elementos tecnológicos como componente sin los

cuáles su existencia no habría sido posible, y los que tienen a las tecnologías como medios para la comisión de delitos preexistentes.

En el análisis, partiremos por la comprensión de que la legislación se encuentra con un Código Penal que data de la década de 1920, el que si bien ha sufrido modificaciones, no termina de adaptarse al constante avance del desarrollo de las tecnologías y, junto a aquellas, a la aparición de conductas jurídicamente reprochables.

En ese marco, ante la aparición del primer computador programable en 1938-1939, los primeros virus en 1949 en los laboratorios del MIT (*Massachusetts Institute of Technology*), o la primer computadora personal comercializada masivamente por la empresa IBM, fue recién en el año 1996 que la ley de Secretos Comerciales (ley 24766) dispuso en su articulo 2 una norma penal relacionada con las más modernas tecnologías.

En efecto, y si bien la referida norma no establecía o creaba un tipo penal, si estableció el paralelismo de dichas conductas con la de violación de secretos, establecida en el artículo 153 del Código Penal de la Nación (*La presente ley se aplicará a la información que conste en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros elementos similares*).

Desde dicho hito, se estudiaran las distintas normas creadas en torno a los delitos con el uso de tecnologías, para culminar con la última norma agregada al digesto penal por medio de la ley 26.804, que modificó el artículo 131 del Código Penal de la Nación, para condenar a la conducta denominada "*grooming*".

La convivencia y dependencia de la vida actual con las computadoras, teléfonos, tarjetas, entre otros elementos informáticos, hace que la temática escogida sea de suma importancia, no sólo como trabajo autónomo, sino que la materia debe encontrarse en el centro del debate legislativo.

Por ello, la importancia de analizar también la respuesta legislativa a las conductas más reprochables surgidas con motivo de la aparición de las TIC´s y la indagación en torno a los tipos penales creados en tal sentido, para lo cual se observarán brevemente los conceptos de las TIC´s, se intentará develar cuáles eran las

falencias de nuestro ordenamiento jurídico en materia de criminalidad tecnológica, estudiándose las normas creadas en tal sentido.

De ahí que los objetivos de este trabajo serán generales y específicos. Por un lado, el objetivo general será: examinar la respuesta legislativa a las conductas reprochables surgidas con motivo de la aparición de las TIC´s. Por su parte, los objetivos específicos serán: i) develar las falencias de nuestro ordenamiento jurídico en materia de criminalidad tecnológica; ii) analizar el Convenio de Ciberdelito de Budapest y su importancia a nivel mundial como así también local; iii) describir e investigar los tipos penales que fueron incorporándose referentes a la criminalidad informática; y, por último, iv) analizar brevemente las primeras penalizaciones de conductas relacionadas con las TIC´s para concluir en el estudio de la ley 26.388 y de la ley 26.904.

UNIVERSIDAD SIGLO 21

CAPÍTULO 1
APROXIMACIÓN A LOS DELITOS INFORMÁTICOS

1. Introducción.

En este capítulo introductorio a la temática bajo estudio, se incorporarán palabras clave propias de los delitos informáticos, principalmente de aquellas que permitirán la delimitación de los tipos penales que formarán parte del estudio y por ende, la normativa a ser analizada, como así también asentirán a su precisa definición.

Sin el análisis de las palabras y los significados propios de las Tecnologías de la Información y la Comunicación, resultaría imposible comprender luego el alcance de las conductas negativas relacionadas con la informática, y su posterior penalización.

2. Terminología

Al referirnos a delitos informáticos, como agresiones novedosas al sistema jurídico, debemos comenzar por comprender que, como ello se encuentra relacionado directamente con el avance y desarrollo tecnológico, el primer obstáculo en el análisis de las nóveles situaciones disvaliosas es enfrentar un lenguaje igual de novedoso, desconocido para el común de la sociedad.

Ese primer obstáculo, se comprende al verificar que en los tiempos de Google y Facebook, el art. 153 del Código Penal de la Nación, se refería al "despacho telegráfico o telefónico". El hurto del art. 162 del referido Código de fondo, era solo de cosas muebles (aun sigue redactado igual); lo mismo sucedía con el delito de daño, denotando la lenta respuesta legislativa que tuvo la materia (Palazzi, P.A., 2012).

En otras palabras, nos hallábamos (y aún lo hacemos) frente a una ventaja del delito de más de 70 años, en la que las conductas reprochables que poco a poco se transformaron en delitos informáticos, se hallaban huérfanos e impunes.

Un ejemplo de esa irrupción de nuevos conceptos, puede ejemplificarse en que, hasta hace no mas de veinte años, la simple idea de enviar "mensajes de texto" con un teléfono celular parecía ilógico, carente de sentido. Sin embargo, hoy día hasta los mas

díscolos y negados de la tecnología comprenden de que se habla al mencionar el envío de un "SMS" (servicio de mensajes simples o *Short Message Service* en inglés).

Sin embargo, la incorporación de terminología y la adaptación social, resulta mas lenta que la aparición de las conductas reprochables, y por ende, es la primer barrera que enfrenta el derecho para hacer frente a las mismas.

En efecto, la necesidad que impone el principio de legalidad, propio de los estados de derecho, de crear tipos penales para la sanción de conductas disvaliosas, necesita de una más rápida respuesta legislativa, máxime teniendo en cuenta la pronta incorporación que el malevaje hace de la terminología específica. Dicho principio, enunciado como *Nullum crimen nulla poena sine praevia lege poenali*, y consagrado en el artículo 18 de la constitución nacional, limita el *ius puniendi* del Estado, haciendo necesaria la referida prontitud en la sanción de leyes específicas que tipifiquen conductas en confronte con el espíritu de los estados de derecho.

En ese marco, también resulta importante mencionar que el presente trabajo debe ser leído, siempre, teniendo en cuenta el momento exacto en el tiempo en el que fue escrito, ya que las apreciaciones sobre lo novedoso y lo tecnológico podrían ser un sinrazón en los tiempos venideros.

Claramente, hoy día la pólvora, un tren o la impresión de un libro no aparecen asociados a la palabra "tecnología", si bien hasta hace unos años eran elementos propios de tal designio.

Ello, por cuanto la tecnología se encuentra directamente asociada con la novedad, con aquella utilización del entorno en forma novedosa, convirtiéndose en una herramienta cuyos resultados no podrían haberse alcanzado. En realidad, lo que importará al desarrollo del trabajo son las nuevas tecnologías de la información y la comunicación.

Entonces, el punto de partida será establecer la definición de tecnología: la Real Academia Española la define como *"Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico"*.

Por su parte, Carlos A Ferraro y Carlos Lerch, en su libro *"Que es que en tecnología"* explican que la palabra tecnología no había aparecido hasta los primeros

años del siglo XVIII, y que el cambio fundamental vino dado por la edición de la *"Encyclopédie"*, editada entre 1751 y 1772, explicando que la palabra tecnología como "el conjunto ordenado de todos los conocimientos usados en la producción, distribución y uso de bienes y servicios" (Ferraro y Lerch, 2001).

La enciclopedia Encarta (versión 2004), por su lado, explica que "el termino proviene de las palabras griegas *tecné* que significa arte u oficio, y *logos,* conocimiento o ciencia, por lo que podemos definir a la tecnología como la ciencia o estudio de los oficios (Rosende, E., 2008 pag. 30).

Sentado dicho significado, corresponde referirnos al concepto de informática, el cual la real academia española la define como el *"Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras"*.

La computadora, conforme la definición de la referida academia, es una *"Máquina electrónica que, mediante determinados programas, permite almacenar y tratar información, y resolver problemas de diversa índole"*.

De tal manera, debe comprenderse que computadora no es sinónimo de PC (computadora personal), sino como su definición la encuadra, mas amplia y abarcativa: como una máquina capaz de almacenar y tratar información, como una unidad de procesamiento de datos.

Este procesamiento de datos, se encuentra a su vez definido como la aplicación sistemática de una serie de operaciones sobre un conjunto de datos, generalmente por medio de máquinas, para explotar la información que estos datos representan.

Con dicha definición se verifica la inclusión de teléfonos celulares, tabletas y elementos que, sin llegar a ser una computadora, permiten la ejecución de programas, accesos a internet, y manejo de datos, propios de las tecnologías de la información y la comunicación que importan al instituto en comentario.

También merece especial mención la "Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación", conocida como internet.

La internet, en su pensamiento primigenio, surgió como un desarrollo militar, cuya finalidad era crear una red de computadoras, que no dependieran de una central, que las administrara, sino que permitiera la interconexión de quellas en un mismo nivel, en un mismo plano, que funcionara independientemente entre sí.

Para lograr dicho designio, actualmente se utiliza el protocolo de interconexión TCP/IP V4, prácticamente agotado (como el número de patentes automotores, se han entregado todas las combinaciones posibles), por lo que se está migrando al protocolo TCP/IP V6, que permite miles de millones de combinaciones posibles más que su predecesor.

Dichos sistemas de comunicación, se basan en enlaces directos, cuya principal finalidad es la conexión de computadoras "entre sí", no dependiendo de ninguna computadora central, lo cual permite el funcionamiento de forma independiente de la labor de otras computadoras conectadas a la red.

Ese sistema, si bien es sólido y sostenible, arroja como contrapartida la ausencia de centrales que concentren información, y desde la órbita del derecho penal, complejizan la tarea de investigación.

Por su parte, es válido mencionar que dentro de dicho sistema, para que se produzca la conexión de una computadora a internet, esta debe tener asignado un número de IP, el cuál es provisto por un proveedor (los más conocidos en nuestro país son Fibertel, Arnet o Speedy), único e irrepetible en una determinada coordenada temporal.

A su vez, dichos proveedores se hacen acreedores de los números de IP a través de ISP (*internet service providers* o proveedores de servicios de internet) de mayor envergadura, los que, una vez más obtienen los paquetes de IP de cinco entidades de gestión repartidas en los distintos contenientes.

Así, desde México hacia el sur del continente, los números de IP se hayan administrados por LACNIC, África por AFRINIC, Australia y parte de Asia por APNIC, Europa, Groenlandia y la parte restante de Asia por RIPE y, finalmente, Estados Unidos y Canadá por ARIN.

De tal modo, y para una mejor comprensión de las distintas aristas que se analizaran a lo largo del presente, resulta relevante repasar conceptos como:

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Se compone por el hardware de entrada (por ejemplo mouse, teclado), hardware de almacenamiento (disco solido, unidad central de procesamientos), hardware de salida (monitor, parlantes) y hardware mixto (placas de red, modem).

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Firmware: el firmware es un bloque de instrucciones de máquina para propósitos específicos, grabado en una memoria, normalmente de lectura/escritura, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Si bien se halla dentro de la categoría de software, es aquel que viene pre cargado y permite la puesta en funcionamiento del hardware.

Sentado ello, debo remarcar que sería imposible intentar definir todos los conceptos que cohabitan y forman parte de la tecnología, la informática y la comunicación, por lo que a medida que el desarrollo del presente lo permita, se irán afianzando definiciones y conceptos propios de la temática.

3. Delimitación de los delitos informáticos.

Entonces, luego de un breve repaso por las definiciones necesarias para comenzar con el desarrollo en la materia, resulta preciso delimitar el grupo de conductas que formaran parte de los denominados “delitos informáticos”.

Compartiendo las palabras de los Dres. Catalá y Argüello, resulta sumamente complejo y discutida la existencia misma de una categoría de delitos con autonomía en la dogmática penal que podamos denominar informáticos (Tobares Catalá y Castro Argüello, 2009).

Algunos autores, incluso sostienen que es improcedente presentar con caracteres de modernidad delitos que no tiene otra nota en común que algún tipo de conexión con

ordenadores, descartando la existencia de delitos distintos de los tradicionales (Saenz Capel, 1999).

Sin embargo, luego de definir las palabras tecnología e informática, se devela el hito fundamental del trabajo en comentario: serán propios de la materia aquellas conductas, disvaliosas que contengan tanto en su descripción típica como en su objetivo dañoso la utilización de elementos informáticos.

Sobre el particular, aunque parezca una obviedad, cabe aclarar que la terminal informática que forme parte del tipo penal que se analice, en cada caso, deberá ser usada funcionalmente como la herramienta para la cual fue creada, o deberá ser objeto de un ataque informático que afecte su funcionamiento, su procesamiento de información, ya que la utilización como una simple cosa, carecerá de interés para este estudio, y para los delitos informáticos (Rosende, E., 2008).

Al hacer referencia al uso "para el cuál fue creada", no resulta ocioso mencionar que, por ejemplo, una computadora no fue ideada para la creación de documentos falsos, pero su uso para tal fin, mediante el uso de distintos programas, se encuentra dentro de las funciones que puede realizarse con el procesamiento automático de información propio del elemento.

En cambio, su uso como una simple cosa estará dado, por ejemplo, en caso de cometerse un homicidio al atacar con una notebook a otra persona, golpeándola hasta la muerte con la misma.

En torno a la clasificación de los estos delitos, en la recomendación Nro. 89 del Consejo de Europa (que años después realizaría el Convenio de Ciberdelincuencia o Ciberdelito de Budapest), estableció los delitos informáticos, clasificándolos como: fraudes informáticos, falsificaciones digitales, daños a las computadoras o los programas, sabotaje informático, acceso no autorizado, reproducciones no autorizadas de programas de computación, alteración de datos o programas, espionaje informático, uso ilegítimo de terminales informáticas y uso no autorizado de programas.

En todos los casos, se verifica que existe una utilización de las tecnologías, sea como medio o como fin, y que ello es lo que identifica los delitos informáticos y con tecnologías, diferenciándolos de otras ramas del derecho penal.

Para concluir, resulta apropiada la diferenciación realizada por el Dr. Eduardo Rosende, quien separa en dos grandes segmentos los delitos informáticos: por un lado, los delitos que no existían o que no podrían haber existido sin la existencia de las computadoras, y por otra parte, aquellos conformados por la utilización de la informática para la realización de delitos convencionales.

En el primer grupo, se encontrarán las amenazas lógico informáticas, fraudes informáticos, piratería, daños a la información digital, envío masivo de spam, entre otros (Rosende. E. 2008).

Por su lado, en el segundo grupo podríamos incluir las calumnias e injurias, pornografía infantil, defraudaciones, etc., conductas en las que se verifica que la informática es solo el medio en el que se desarrollan delitos tradicionales.

Dicha diferenciación, también es tomada por el Dr. Diego Migliorisi (2014), quién en su obra establece la existencia de ciberdelitos tipificados o delitos tradicionales del Código Penal, que se configuran a través de internet, y ciberdelitos propiamente informáticos.

En razón de las consideraciones vertidas a lo largo del presente, se verifica que podemos delimitar el ámbito de los delitos informáticos, como dijéramos presentemente, en aquellas conductas reprochables desde el derecho penal, que utilicen como medio o como fin, herramientas de procesamiento automático de información.

4. Aproximación a la definición de los delitos en tecnologías.

La delimitación del ámbito de aplicación de los delitos informáticos, permite a su vez delinear una definición de lo que serán los delitos informáticos.

El Dr. Rosende, reconoce en su obra una de las definiciones dadas por la Organización para la Cooperación y Desarrollo Económicos que sostiene que los delitos informáticos serán aquellos en los que se realice "*cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o transmisión de datos*" (Rosende. E., 2008).

Es decir, se establece que será un delito informático aquel en el que se utilice, como medio un sistema de procesamiento, por lo cual se deja abierta la puerta a las futuras tecnologías.

Por su parte, el profesor Ulrich Sieber (1998), especialista en la materia, en un informe presentado ante la Unión Europea, definió los delitos informáticos como aquellas conductas que se realizan mediante el uso de computadoras para la afectación de la privacidad, el patrimonio, la propiedad intelectual y la diseminación de contenido ilegal.

Por su lado, en la Reunión de Expertos en el Ciberdelito de la OEA, celebrada el 23 y 24 de junio de 2003 en Washington, se definió a los delitos informáticos como "toda conducta, atentatoria de bienes jurídicos relevantes, que supongan el uso de medios informáticos en algunas de sus fases de ejecución".

Asimismo, se ha propuesto que se entenderá por delito binario, la comisión del acto antijurídico, antisocial, típico, culpable y punible basado en los delitos tradicionales o independientes de estos, cometidos con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, pudiendo causar una afectación o no, a la propiedad y/o posesión binaria de que se trate (Azuara C. 2012).

En conclusión, luego de verificadas las distintas definiciones dadas por los especialistas en la materia, puede concluirse que un concepto apropiado es que serán delito informático aquella conducta que lesione uno o más bienes jurídicos protegidos por el derecho penal, realizados en forma típica, y que utilice como medio o lesione como fin unidades de procesamiento automático de información.

5. Conclusiones parciales

En el presente, se han incorporado conceptos y conocimientos propios de la temática escogida, que permitirán comprender en forma acabada el desarrollo del trabajo, ya que la existencia de definiciones técnicas y de mecanismos tecnológicos novedosos, hacen necesario realizar estas aclaraciones previas.

Asimismo, la conceptualización de los delitos informáticos permite la correcta delimitación del ámbito de aplicación de la materia, lo cual deviene en la adecuada individualización de las conductas que serán parte del análisis, y permitirán adelantar cuales son las acciones que precisan en forma inmediata la atención legislativa.

Así, en esta llamada "era de la información", justamente, lo que ha alcanzado valor digno de protección es la información intangible, antes siquiera considerada "cosa", y que actualmente requieren la protección del derecho.

Uno de los hitos mas importantes es la aparición, o mejor dicho, la puesta en valor, del bien jurídico llamado "información".

En palabras del Dr. Santiago Del Pino, ante la Organización de Estados Americanos, se trata de la equiparación de aquello que otrora era tangible con la información "virtual", aquella que no podemos sostener en nuestras manos, aquella que se aparta de la idea de bienes corporales.

En ese marco, la ley 24.766, si bien no estableció o creó un tipo penal específico, resinificó el concepto o término de "documentos" al reconocer su existencia en soporte informático; por primera vez una ley tomó "conciencia" de que un documento ya no era simplemente una hoja de papel con información, sino que esta última podía tener otro tipo de existencia, otra forma, otro sustento.

A partir de allí, fueron a lo largo del tiempo sancionadas una serie de normas que, aunque en forma tardía, cubrieron los vacíos legales que permitían el abuso de conductas moralmente reprochables, pero aún no legisladas.

Otrora, Saez Capel (1999) expresaba que la existencia de hechos ilícitos en Argentina, relacionados con medios informáticos, estaba fuera de toda duda, pero existían pocos instrumentos para detectarlos, a la vez que los casos descubiertos, no eran dados a conocer, y quedaban confiados a los especialistas en seguridad informática, y no a los tribunales.

Por otro lado, no puede perderse de vista que el fenómeno del ciberdelito es un proceso mundial, que traspone fronteras, y se presenta en forma prácticamente simultánea en todos los rincones del planeta.

La informática y la internet, son pilares fundamentales de la sociedad moderna en su modo globalizado, en el que la red proporciona infinidad de posibilidades a las personas para desenvolverse en sus quehaceres cotidianos, presentando iguales posibilidades para la realización de conductas reprochables. Resultaría ingenuo pensar que las enormes utilidades que aporta esta nueva era informática, no serán utilizadas también para el provecho ilegítimo de algunos -en su propio beneficio-, y en detrimento de terceros (Diaz G., 2010).

Poco a poco, la información y su interconexión mediante internet, se ha vuelto cotidiana, y hasta necesaria como herramienta en la gran mayoría de las actividades ociosas y laborales, cambiando la forma de relacionarse de la sociedad completa (Migliorisi, D., 2014).

Ello trajo aparejado la globalización del delito, presentando no sólo conflictos internos en los países en los que fue apareciendo, sino que, como nunca, hizo necesaria una planificación a nivel global en torno a los modos de respuesta y a la -hasta ahora- deficiente colaboración internacional para la creación de mecanismos que permitan una rápida respuesta frente al delito.

Así, un buen "manual" resulta el convenio de ciberdelito de Budapest, primer acuerdo de trascendencia suscripto entre diversas naciones con el objeto de armonizar las legislaciones internas; nacido, conforme surge de su preámbulo, de la necesidad de aplicar, con carácter prioritario, una política penal común con el objeto de proteger a la sociedad frente a la ciberdelincuencia.

En el convenio, además de las normas de fondo que mas adelantes se analizarán, se dispusieron una seria de hitos procesales tendientes a la pronta preservación de elementos de prueba informáticos, su preservación y confiscación.

Todo lo dicho hasta aquí, permite dimensionar el fenómeno del ciberdelito, su masificación y su peligrosidad, poniendo de manifiesto, en consecuencia, la necesidad de su estudio y comprensión.

CAPÍTULO II
ANÁLISIS DE LOS TIPOS PENALES

1. Introducción

En el presente capítulo nos adentraremos en el estudio de cada uno de los tipos penales creados por el legislador que, de un modo u otro se relacionan con las tecnologías de la información y la comunicación, formando parte de la dinámica de los delitos informáticos.

De tal manera, se comenzará con la ley de secretos comerciales, por ser aquella la cuál reconoció en forma expresa la existencia de una "nueva" información, que ya no era necesaria que estuviese presente en papel, sino que la dotaba de otros tipos de existencia, para concluir en delitos de corte netamente informáticos, como el caso del delito de "grooming", actualmente incorporado en el artículo 131 del Código Penal de la Nación.

2. Los primeros delitos relacionados con las nuevas tecnologías.

2.1. Análisis de las leyes 24.766 a la 25.520 relacionadas con la temática.

Como se manifestara precedentemente, la ley 24.766, denominada Ley de secretos comerciales, fue sancionada en el año 1996, y publicada en el boletín oficial el 30 de diciembre de dicho año, entrando finalmente en vigencia el 7 de enero de 1997.

La ley, si bien no creo un tipo penal específico, definió en su artículo segundo que "*La presente ley se aplicará a la información que conste en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros elementos similares*".

En otras palabras, tuvo en miras dos situaciones que marcaron una tendencia legislativa que devenía necesaria: por un lado, se reconocía el valor intrínseco de la información y, por el otro, que dicha información tenía distintas formas de existencia, apartándose de la visión clásica (sólo reconociendo la existencia tangible).

En palabras de Saez Capel, la informática ha tornado "*...una mera acumulación*

de datos en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico" (Saez Capel, 2001, pag. 121).

Por su parte, en la misma ley se dispuso que quien incurriera en la infracción de alguna parte de la ley en materia de confidencialidad, quedaría sujeto a la responsabilidad que correspondiera conforme con el Código Penal, y otras normas penales concordantes para la violación de secretos, sin perjuicio de la responsabilidad penal en que se incurra por la naturaleza del delito.

A partir de allí, y sin incorporarse en forma expresa, por primera vez nuestro ordenamiento penal tuvo una herramienta de protección para la información almacenada en un soporte informático.

Sin embargo, la normativa, aunque novedosa, no dejó de suplir el vació legal al respecto, toda vez que su aplicación se daba solo en torno a la información propia de su protección, es decir información empresarial.

Además de ello, el legislador en la redacción del artículo pareciera que intentó planear un trabalenguas jurídico sumamente complejo, creando un tipo penal de difícil configuración (Palazzi, P. 2000).

En primer lugar, el artículo remite a otros artículos de la misma ley a los efectos de clarificar quiénes serán los sujetos activos y cuáles serán las obligaciones que poseen para, luego, dejar un espacio abierto en torno a la consecuencia jurídica por su afectación.

Así, la frase "*...la responsabilidad penal que correspondiera conforme con el código penal y otras normas penales concordante para la violación de secretos…*" es extremadamente vaga, dificultando su aplicación, en tanto debía haberse hecho una remisión a las penas de alguno de los artículos que hablan de la violación de secretos en particular, y no una remisión abierta.

Por su parte, las acciones típicas que surgen de la ley, conforme la redacción del referido artículo, pueden dividirse en dos: por un lado, el uso de la información confidencial, sin causa de justificación o sin consentimiento de la persona que guarda dicha información o de su usuario autorizado, y por el otro, la revelación de la información confidencial (Palazzi, P, 2000).

Sobre este particular, bien corresponde hacer un paréntesis en torno al bien jurídico protegido por estos tipos penales, y por el valor intrínseco que conlleva la información en sí misma, sin importar el tipo de soporte en que se encuentre.

Este nuevo elemento, no resultó ajeno a la legislación vigente; en el artículo 2312 del Código Civil le daba tratamiento como objeto inmaterial susceptible de adquirir valor -pero diferente de una cosa-, y por ende susceptible de la protección del derecho (Rosende, E, 2007).

Hablar de bien jurídico protegido en sentido general, es hablar de aquel bien que el derecho en la plenitud del ordenamiento jurídico protege o resguarda. En los delitos relacionados con la materia bajo estudio, la información es el bien jurídico que por excelencia aparece a resguardo, sin perjuicio de que luego, cada tipo penal en particular, afectará uno o más bienes jurídicos, no siendo ninguno de ellos puro ni exclusivo (Catalá, G y Argüello, M, 2010).

Por su parte, es importante la aclaración que realiza el Dr. Rosende (2007) en cuanto afirma que no nos encontramos ante un nuevo bien jurídico surgido de la evolución social, sino que nos encontramos ante un derecho ancestral, cuya importancia ha sido potenciada al infinito por la sociedad de la información, y es esa sociedad la que busca una protección más efectiva y amplia.

Ley 24.769

Contemporánea a la ley 24.766 ya analizada, el 13 de enero de 1997 se promulgó la ley 24.769, referente al Régimen Penal Tributario, que estableció una serie de reproches penales a las conductas relacionadas a la materia.

Una de ellas, existente en el artículo 12 de la referida ley, peno la alteración dolosa de los registros relacionados con el fisco nacional. Así, el artículo en su redacción original disponía que "*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".

Dicha normativa, refrendó la postura de su antecesora en cuanto revalidó la existencia de soportes informáticos como un punto relevante y a ser tenido en cuenta al momento de merituar las conductas reprochables.

Posteriormente, por intermedio de la ley 26.735 se amplió la formula "*... del fisco nacional...*" por "*...del fisco nacional, provincial o de la Ciudad Autónoma de Buenos Aires...*", cubriendo así otro sinnúmero de situaciones, supliendo el vacío dejado por su antecesora.

Asimismo, la normativa incorporó el artículo 12 bis, que penó la modificación o adulteración de los sistemas informáticos o equipos electrónicos, suministrados u homologados por el fisco nacional, provincial o de la Ciudad Autónoma de Buenos Aires, siempre y cuando dicha conducta fuere susceptible de provocar perjuicio.

Volviendo al tipo penal creado por la ley 24.769, por vez primera se estaba ante un supuesto penal directamente estipulado a ser cometido sobre soportes informáticos (Palazzi, Pablo A., 2012), novel en su esencia, y más teniendo en cuenta el año de su sanción -1997-.

Previo al análisis del tipo penal que surge de la referida ley, es prudente remarcar que a través de las reglamentaciones RG2733, RG2899, RG2784 y RG3211 (entre otras) de la -entonces- DGI, se estableció la presentación de información en el organismo a través de soportes magnéticos, habilitando la vía informática.

De tal forma, en primer lugar corresponde mencionar que nos hallamos ante un delito de peligro, por lo que basta para su consumación la simple realización de la acción típica, sin requerirse la producción concreta de daño alguno.

El tipo penal protege los bienes jurídicos tutelados por la ley 24.769, poniendo a resguardo la actividad financiera del Estado y la recaudación de los tributos y los parámetros imprescindibles para el cumplimiento de las pautas de la seguridad social (Riquert, M. 2008).

Por su parte, las acciones típicas se encuentran taxativamente detalladas, siendo ellas las de sustraer, suprimir, ocultar, adulterar, modificar o inutilizar. La descripción del tipo penal permite corroborar, asimismo, que nos hallamos ante un tipo de delito

doloso directo.

Así, dentro de las pautas del tipo subjetivo, se aduna a la exigencia del conocimiento de los elementos del tipo objetivo (esto es, saber que se realiza alguna de las acciones típicas sobre un registro o soporte documental o informático del fisco nacional relativo a obligaciones tributarias o de recursos de la seguridad social y voluntad de hacerlo), lleva como nota adicional "el propósito de disimular la real situación fiscal de un obligado" (Riquert, M. 2008).

Resulta también importante mencionar que la falta de eficacia del método empleado en nada coarta los efectos comisivos, en tanto el delito se perfecciona con la realización de alguna de las acciones típicas descriptas por la norma.

Ley 25.036

El 11 de noviembre de 1998, casi un año después de las dos leyes que marcaron el comienzo de la normativa y la penalización de conductas relacionadas con la informática, se sancionó la ley 25.036, modificatoria de la ley de propiedad intelectual (11.723).

Una vez más, en este caso los legisladores escogieron insertar en la norma vigente una descripción que no diera lugar a dudas en torno a que el software y las bases de datos se hallaban protegidas, agregando a la descripción amplia de obras sujetas de protección, la fórmula "*...entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales...*".

En este sentido, la jurisprudencia de la Cámara Nacional de Casación Penal sostuvo que, "*a partir de la modificación manifestada por el legislador en la ley 25.036 que permite la incorporación de los programas de computación, fuente y objeto a los ejemplos enunciados en el art.1° de la ley 11.723, se inicia en el marco de intervención del Derecho Penal a través de las conductas descriptas en los arts. 71 y 72 de la Ley de Propiedad Intelectual para este tipo de creaciones*" (C. Nac. Casación Penal, Sala 4ª, 3/10/2000, "Roitman")

Autores como Catala y Argüello (2010) sostienen que con la reforma a la ley de propiedad intelectual se incorporaron herramientas de protección contra los ataques

que puedan presentarse en torno a la reproducción, venta, edición, falsificación de un programa de computación -software- a través de medios tecnológicos o virtuales.

La importancia de su sanción, puede verse reflejada, por ejemplo, en el fallo de la Cámara Nacional de Casación Penal en los autos "Pellicori, Oscar y otros s/ denuncia por defraudación", anterior a la reforma, en el que se sostuvo que el software era una obra *sui generis*, que se hallaba por fuera de la protección de la ley 11.723.

En efecto, se sostuvo que "*Si bien el artículo 1° de la ley 11.723 define cuáles son las obras del intelecto protegidas (artísticas, literarias, científicas y didácticas) y hasta las enuncia (aunque de manera no taxativa), el reconocimiento de la calidad de obra a otras no incluidas en la ejemplificación debe provenir de la interpretación judicial de ese elemento normativo del tipo, pero no es función que este último delegue en una norma complementaria, como ocurre en las leyes penales en blanco en sentido propio*" (Autodesk Inc. s/recurso de casación. Voto de los Dres. Catucci, Madueño, Bisordi. Sala I, Resolución del 19/07/1995).

De tal manera, deviene evidente que la sanción de la ley 25.036 suplió un gran margen de desprotección en que se hallaban los programas informáticos o software, máxime teniendo en cuenta la tendencia jurisprudencial.

Distinto marco se presenta a nivel doctrinario, en donde, por ejemplo Saez Capel (2001), sostuvo que "*...cuanto mas se profundiza en el análisis de la sustancia de los programas de computación, mas aparecen las características de obras literarias...*"; ello de conformidad con las definiciones que surgen de la Convención Internacional para la Protección de las Obras Literarias y Artísticas, suscripto en 1886, revisada en 1948 y de la Convención Universal sobre el Derecho de Autor, firmada en Ginebra en 1952, y por ende protegidas por los derecho de autor.

En esa marea revuelta de análisis dogmático, la norma suplió las interpretaciones al incluir directamente en la descripción del artículo 1ro de la ley 11.723 el software y las bases de datos.

En torno al tipo penal que surge de la ley, el legislador optó por remitir en su artículo 71 al artículo 172 del Código Penal que establece una pena de un mes a seis años de prisión para su autor, el que de cualquier manera y en cualquier forma

defraude los derechos de propiedad intelectual que reconoce esta Ley.

Dicha redacción, hace necesario un análisis de la defraudación. Como tal, aquella es toda lesión patrimonial producida con fraude, resultando la defraudación el género, cuyas especies son la estafa o el abuso de confianza como modalidades (Donna, E. 2001).

Objetivamente, el tipo exige la presencia de un ardid, la inducción al error y una disposición patrimonial, y desde el punto de vista subjetivo, requiere la plena voluntad del autor de producir la lesión al bien jurídico, guiada por la finalidad de lucro.

Al igual que en el artículo 173 del Código Penal, la ley 11.723 estableció, a su vez, en el artículo 72 casos especiales de defraudación a la propiedad intelectual, resultando los siguientes:

> *a) El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derechohabientes;*
>
> *b) El que falsifique obras intelectuales, entendiéndose como tal la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto;*
>
> *c) El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el título de la misma o alterando dolosamente su texto;*
>
> *d) El que edite o reproduzca mayor número de los ejemplares debidamente autorizados.*

Por su lado, a partir de la reforma introducida por la ley 23.741, se agregó el artículo 72 bis una serie de conductas negativas, orientadas a la penalización de aquellos que violan los derechos intelectuales con finalidades comerciales:

> *a) El con fin de lucro reproduzca un fonograma sin autorización por escrito de su productor o del licenciado del productor;*
>
> *b) El que con el mismo fin facilite la reproducción ilícita mediante el alquiler de discos fonográficos u otros soportes materiales;*
>
> *c) El que reproduzca copias no autorizadas por encargo de terceros mediante un precio;*
>
> *d) El que almacene o exhiba copias ilícitas y no pueda acreditar su origen mediante la factura que lo vincule comercialmente con un productor legítimo;*
>
> *e) El que importe las copias ilegales con miras a su distribución al público.*

Finalmente la ley 11.723 establece otros tipos penales de menor cuantía en sus artículos 73 y 74, pero su análisis escapa de los alcances del presente trabajo, al no presentar elementos distintivos ni diferentes respecto otros tipos penales.

En resumen, la norma bajo análisis incorporó la protección de los programas informáticos al equipararlos con obras literarias o artísticas, reconociendo, una vez más, el valor de la información.

Asimismo, es válido mencionar que la comisión de los delitos contra el *software*, requiere para su comisión, en prácticamente todos los casos, la utilización de elementos informáticos; por tal motivo, se erige como un tipo penal que tiene al elemento informático como objeto de la lesión, y como medio para la producción del resultado.

Ley 25.326

Pasando la mitad del año 2000, se sancionó la ley 25.326, denominada de protección de datos personales, que creó dos nuevos delitos relativos a las bases de datos.

La referida ley dispuso la incorporación como artículo 117 bis del Código Penal, las siguientes conductas negativas:

1°. 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.

2°. 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.

3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4°. 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".

Vale remarcar, rápidamente, que el artículo 1ro fue derogado por la ley 26.388, que dispuso la incorporación de la conducta allí contenida, como inciso 3ro del artículo 157 bis del Código Penal.

Por su lado, la ley 25.326 dispuso la incorporación del artículo 157 bis en el Código Penal, reprimiéndose con pena de prisión de un mes a dos años el que:

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

Dicha redacción, una vez más, fue modificada por la ley 26.388, siendo la redacción actual del referido artículo la 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.*

En base a lo expuesto, y teniendo en cuenta las modificaciones aludidas, los tipos penales serán estudiados al momento de analizar la ley 26.388. Sin perjuicio de ello, resulta atractivo dar una breve mirada a la construcción y espíritu de la referida ley.

En ese norte, su artículo 1ro establece su finalidad, siendo aquella la protección de los datos personales, en cualquiera fuere su lugar de asentamiento, como así también el acceso a los mismos.

Una vez más, nos encontramos frente a una ley que reivindica el valor de la información, cada vez más preciada.

Otro hito importante de la norma, es el aporte de definiciones de "datos personales", "datos sensibles", "archivo registro, base o banco de datos", "tratamiento de datos", "responsable de archivo, registro, base o banco de datos", "datos informatizados", "titular de los datos", "usuario de datos" y "disociación de datos".

Ello, en contraposición con la gran cantidad de normas con tipos abiertos, o que dejaban lugar a controversias, se presenta como un verdadero digesto en torno al tratamiento de "datos personales", estableciendo no sólo sanciones penales sino procedimientos administrativos para la protección es los datos bajo estudio.

Ley 25.506

La ley 25.506, si bien no creo un tipo penal, a partir de su sanción en el año 2001 se incorporó en el artículo 78 bis del Código Penal la definición de documento electrónico. Sin embargo, la fuente de su valor esta dado justamente por el reconocimiento del documento informático, firma electrónica y de la firma digital.

El texto de la norma dispuso: "*Equiparación a los efectos del derecho penal. Incorpórese el siguiente texto como artículo 78 (bis) del Código Penal: 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.*"

Para aquel entonces, existía una fuerte controversia en torno al valor de los documentos digitales, careciendo aquellos de una equiparación con los documentos de existencia "real"; y se hallaban en comparación en un estrato inferior.

Sin embargo, también es válido mencionar que la modificación dejó de lado los documentos públicos, situación que fue subsanada, como veremos mas adelante, por la ley 26.388, que derogó la norma bajo análisis, por lo que no quiere en este punto mayor análisis.

Ley 25.520 (ley de inteligencia), y sus modificaciones.

La referida norma, sancionada el 27 de noviembre de 2001, tuvo -en cuanto importa al presente trabajo-, la finalidad de regular la conducta de los agentes de inteligencia frente a la interceptación y captación de las comunicaciones, tarea que en aquel entonces tenían bajo su órbita.

En particular, la norma creó dos tipos penales especiales propios, ya que la calidad del sujeto activo permitirá la autoría frente a la conducta disvaliosa establecida. En efecto, los dos supuestos delictivos son aplicables sólo a aquellos que estuvieran realizando actividades reguladas por la misma norma.

Así, las conductas descriptas en el artículo 42 de la ley 25.520, cuya pena fue fijada entre un mes y dos años de prisión, eran las de interceptar, captar o desviar una serie de comunicaciones, requiriendo que tales acciones se produjeran en forma indebida -sin derecho-.

La clave de la penalización, entonces, estaba dada por la falta de autorización del agente en la interceptación, desvío o captación, ya que sin dicho calificativo, o mediante una autorización, manda, orden o cualquier tipo de habilitación, la conducta no podrá ser penada, resultando ello lógico en razón de las tareas propias de la, ahora, Agencia Federal de Inteligencia -conf. Ley 27.126.

Por su lado, el artículo 43 de la ley 25.520, penaba al que con orden judicial y estando obligado a hacerlo, omitiere destruir o borrar los soportes de las grabaciones, las copias de las intervenciones postales, cablegráficas, de facsímil o de cualquier otro elemento que permita acreditar el resultado de las interceptaciones, captaciones o desviaciones.

De tal manera, el artículo 42 se encargaba de penar al “agente de inteligencia”, por la realización de la interceptación sin orden, en tanto el artículo 43, castigaba a quien, con una orden concreta, no cumpliera con su designio.

Vale recordar, que mediante la ley 27.126, se modificaron los artículos 42 y 43, aumentando exponencialmente la pena para los delitos tratados, demostrando el interés de proteger la información individual de la injerencia estatal.

Una vez más, al igual que en la totalidad de los tipos penales hasta ahora analizados, en su faz subjetiva, el articulo 42 en su modalidad comisiva y el artículo 43 en su modalidad omisiva, requerirán de dolo.

2.2 La ley de telefonía celular – ley 25.891.

La ley 25.891 fue una de las denominadas "leyes Blumberg" – sancionada conjuntamente con la ley 25.866 y la ley 25.882-, y llevan el nombre de su impulsor, Juan Carlos Blumberg.

Es válido recordar que el hijo del nombrado Juan Carlos Blumberg -Axel Blumberg-, fue secuestrado y se solicitó por su rescate el pago de una suma de dinero. Días después, y aún habiéndose reunido el dinero, Axel Blumberg intentó escapar de su captores, y uno de ellos -José Díaz-, le quitó la vida al darle un tiro en la cien, presuntamente por haberle "visto el rostro".

A partir de aquel trágico episodio, Juan Carlos Blumberg encabezó una serie de marchas y protestas tendientes a agravar las penas de los casos con armas, secuestros, como así también expuso en torno a lo peligroso que resultaba la existencia de teléfonos celulares sin registrar, con los que se realizaban las llamadas extorsivas, lo cual dificultaba su localización.

En ese marco de clamor social se produjo la "apurada" sanción de la ley 25.891, que intentó fijar una serie de principios relacionados con la comercialización de terminales móviles y chips de telefonía, y creo tres tipos penales, agravados a su vez por el ánimo de lucro.

Sin embargo, la ley contiene una serie de errores que, sumados a la desidia legislativa y ejecutiva hacen que su letra sea casi obsoleta.

Brevemente, puede mencionarse que la misma nunca fue debidamente reglamentada, nunca se crearon los organismos a los que ella misma hace referencia, lo cual importa que no exista una forma clara de conocer, por ejemplo, si un celular ha sido denunciado como robado, hurtado o extraviado.

En ese sentido, el artículo 7mo de la norma determinó la creación, en el ámbito de la Secretaría de Comunicación de la Nación el Registro Público Nacional de

Usuarios y Clientes de Servicios de Comunicaciones Móviles, y el artículo 16 otorgó un plazo de 60 días a los efectos de que el Poder Ejecutivo la reglamentara.

Sin embargo, transcurridos más de 10 años desde su sanción, el Registro es inexistente, como así también su reglamentación y creación de organismos de control.

En segundo lugar, la ley dispone que la comercialización de los servicios de telefonía celular pueda realizarse, únicamente, a través de las empresas autorizadas. Sin embargo, no establece ningún tipo de sanción para aquel que se aparte de tal directiva, cercenando de tal forma cualquier tipo de acción penal al respecto.

En lo que hace a la creación de tipos penales, el artículo 10 reporta que "*Será reprimido con prisión de un mes a seis años, 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 Módulo de Identificación Removible del usuario o la tecnología que en el futuro la reemplace, en equipos terminales previstos con este dispositivo, de modo que pueda ocasionar perjuicio al titular o usuario del terminal celular o a terceros*".

Por su lado el artículo 11 sindica que "*Será reprimido con prisión de un mes a seis años, el 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 ilegítimamente del crédito emanado por un licenciatario de Servicios de Comunicaciones Móviles*"

De tal forma, ambos artículos adolecen de una redacción confusa, aunado a que la amenaza de pena resulta en una de las más amplias contempladas en nuestro sistema penal, yendo desde una de las más bajas -un mes- a otra que, por su cuantía, podría resultar de pleno cumplimiento efectivo -seis años-.

Asimismo, la redacción del artículo 11 hace dudar si el requerimiento final de "*… a efectos de aprovecharse ilegalmente del crédito emanado por un licenciatario…*" es aplicable a la totalidad de hipótesis conductuales o sólo a aquella que se encuentra inmediatamente antes.

Aunado a ello, difícilmente las licenciatarias "emanen" créditos, sino que los conceden, los otorgan, los venden, los comercializan, pero no los emanan (Vanossi, J. R. 2004).

Por su lado, el artículo 12 impone sanción para aquellos que, a sabiendas de su procedencia ilegítima, reciben o adquieren un teléfono o tarjeta sim, resultando tal disposición absolutamente innecesaria, por cuanto resulta idéntica al encubrimiento. De hecho, se erigiría como un tipo de encubrimiento especial por el objeto material del delito.

También resulta insólito que el artículo 13, aparezca como un agravante de sus antecesores pero, en realidad, sólo lo sea en parte. En efecto, para los artículos 10 y 11, aún cuando se hayan cometido con ánimo de lucro o con el fin de perpetrar otro delito la pena se mantiene exactamente igual; "*...con relación a estos dos artículos el art. 13 no agrega absolutamente nada; en otras palabras no habrá figura agravada para los delitos previstos en los arts. 10 y 11, pero sí, curiosamente, para el más leve previsto en el art. 12…*" (Vanossi, J.R. 2004).

Ello, a riesgo de aventurar conclusiones personales, tuvo su raigambre en la utilización de teléfonos celulares robados o adquiridos a sabiendas de su procedencia ilegítima para la perpetración de secuestros extorsivos y por ello la penalización en caso de ser utilizados para la comisión de otros delitos.

Razón de todo lo dicho hasta aquí, se verifica que la ley 25.891, si bien creo tres tipos penales que sirven de herramientas para desalentar el "consumo" de terminales robadas, cierto es que su deficiente redacción aunada a la falta de reglamentación hacen que sea de difícil aplicación.

De la lectura de los antecedentes parlamentarios a su vez se verifica que, existió por ejemplo, la idea de cercenar la venta de tarjetas de telefonía móviles, lo cual podría haber redundado beneficiosamente en la extirpación de la existencia de terminales móviles "huérfanas" o con líneas a nombre de personas inexistentes.

Sin embargo, existieron voces en disidencia, aduciendo, por ejemplo, que en el interior del país se tenían celulares para emergencias, y que aquellos que lo tenían con tal fin, no podrían acceder al pago de un abono mensual (ver en tal sentido voto de la

Senadora Silvia Gallego – senadora por la Provincia de La Pampa).

Un dato que ejemplifica la falta de eficiencia de la norma, se aprecia en los antecedentes parlamentarios, cuando el Senador Miguel Angel Pichetto, expresó "*¿Cuáles son los objetivos de este proyecto de ley? El primer objetivo es prohibir la venta de teléfonos celulares usados*".

Ello, no sólo no ha sido alcanzado, sino que la propia ley no prohibió, habiendo proliferado en forma incalculable la venta de terminales móviles usadas. Una rápida búsqueda en el sitio "mercadolibre.com.ar" de celulares usados, arrojó en el día de la fecha setenta y cinco mil seiscientos veinte ocho resultados.

Ahora bien, en torno a los tipos penales creados por la norma, resulta descriptivo traer a colación cuál fue el bien jurídico que intentó proteger la ley 25.891, que fueron expuestos en el proyecto de ley original.

En aquella presentación, se adujo que la clonación de teléfonos y la adulteración de tarjetas de telefonía ponían en peligro y lesionaban la seguridad y privacidad que necesariamente debe rodear al servicio de comunicación a través de terminales celulares y tarjetas de telefonía.

"*Así, el bien jurídico que subyace a maniobras que impliquen la alteración, reemplazo o duplicación de un número de línea y/o de serie de una terminal celular, está constituido fundamentalmente por la seguridad y correcto funcionamiento del servicio de telefonía móvil celular, que con conductas como las precisadas se ponen en peligro*" (proyecto de ley S.-1.160/03, Guillermo R. Jenefes. – Miguel A. Pichetto. – Jorge M. Capitanich).

Por su lado, en el caso de los artículos 10 y 11, las conductas típicas, desde la faz objetiva, se hallan taxativamente enumeradas, no requiriendo mayor análisis.

Ambas, a su vez, requieren de dolo directo, ya que el espíritu de la ley produce que la cualquier tipo de conducta que conlleve la finalidad comisiva resultará atípica, requiriendo en el primer caso el simple dolo, y en el segundo, que la finalidad de la conducta sea obtener un aprovechamiento ilegal.

Por su lado, el artículo 12 de la mentada norma, ha sostenido la jurisprudencia que aquel pretende englobar "…*aquellos comportamientos que no se encuentran*

descriptos en los artículos 10 y 11 pero que de algún modo se relacionan con aquellas maniobras, es decir que intenta incriminar la conducta de las personas que adquieren o utilizan teléfonos celulares o tarjetas de telefonía de origen ilegal, conociendo esta circunstancia. Queda comprendido en la descripción quien de cualquier forma se valga de estos materiales que hayan sido hurtados, robados, perdidos u obtenidos mediante fraude (ver los fundamentos de proyecto de ley de los Senadores Guillermo Jenefes, Miguel A. Pichetto y Jorge M. Capitanich, pág. 1095, Antecedentes Parlamentarios, tomo 2004-b, La Ley)..." (Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, Sala I, causa n° 41.916 "Figueredo, Jorge Antonio s/ procesamiento" Reg. n° 1207 del 14/10/08).

De tal forma, se verifica que el artículo 12 de la ley se presenta como un tipo penal residual, que intenta acoger todas aquellas conductas relacionadas con el tráfico ilegal de teléfonos celulares, cuya adquisición y/o tenencia resulte irregular.

En ese marco, ya se ha marcado el paralelo con la figura del encubrimiento. La jurisprudencia, en repetidas oportunidades ha sostenido que debe descartarse la participación de quien, por ejemplo, tiene en su poder un teléfono robado, ya que el robo apartaría a la figura bajo estudio (ver dictamen del Dr. Eduardo Ezequiel Casal, Procurador ante la Corte Suprema de Justicia de la Nación, fecha 27/12/2013, S.C. Comp. 607 L. XLIX).

En resumen, la ley 25.891 llegó en un momento socialmente tumultuoso y como respuesta a variadas protestas ciudadanas, por lo que la prontitud en su sanción trajo aparejado una serie de inconvenientes relacionados con su redacción y su forma.

Aunado a ello, al no haberse nunca reglamentado, la norma quedó coja, cumpliendo solo parcialmente los fines para los que fuera creada, no logrando su sanción conmover ni disminuir el comercio de terminales ilegales de celulares.

2.3. La defraudación con el uso de la tarjeta de crédito: ley 25.930.

La ley 25.930, aprobada el 9 de agosto de 2004, realizó dos modificaciones al Código Penal.

En primer lugar, insertó el inciso 15 al artículo 173, que contiene los tipos

especiales o específicos de defraudación, sancionando a quién defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.

Por su lado, se incorporó a la redacción del artículo 285 la equiparación de las tarjetas de compra, sea de crédito o débito, a la moneda nacional.

Respecto de esta norma, una vez más es el profesor Riquert (2014) quien sostiene que la norma presentó diversas falencias, e hizo necesaria la incorporación, luego, del inciso 16 a través de la ley 26.388, a los efectos de abarcar aquellas conductas relacionadas con las defraudaciones bancarias que no necesariamente incluyeran la utilización de tarjetas de créditos.

En torno al tipo penal introducido en el artículo 173 inciso 15 del Código Penal de la Nación, es válido recordar que se trata de una defraudación específicamente establecida. "*Algunas de las conductas que encuentran adecuación típica en el art. 173 inc. 15 del C.P. encuadran también en el delito de estafa. Por ello, toda vez que entre tales figuras existe un concurso aparente de leyes, en virtud del principio de especialidad para todos aquellos hechos cometidos con posterioridad a la sanción de la ley 25.930 se aplica el inc. 15 del art. 173*" (Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, elDial.com - AI2421).

De tal forma, el tipo penal requerirá para su concreción la existencia de ardid o engaño, o el uso ilegítimo de una tarjeta magnética o de sus datos, para provocar un acto de disposición patrimonial, vinculados por la relación de causalidad o de imputación objetiva. Finalmente, en el aspecto subjetivo, el dolo se configura al comienzo de la acción (es ex ante).

3. La gran reforma en materia de delitos en tecnologías: ley 26.388.

3.1. Análisis de cada uno de los tipos penales creados.

La reforma introducida por la ley 26.388 no sólo supuso la incorporación, como hasta aquel entonces, de hitos aislados relacionados con la criminalización de

conductas que involucraran, como medio o como fin, de elementos informáticos, sino que significó un cambio de perspectiva, e incluyó en forma orgánica conceptos legales que el avance tecnológico había dejado obsoletos (Palazzi, .P, 2012).

La ley fue sancionada el 4 de junio de 2008, y promulgada el 24 del mismo mes y año, convirtiéndose, luego de cuatro años desde la última norma relativa a la temática, en una sucinta pero suficiente -en aquel entonces- parche para una serie de conductas que resultaban "impunes", o cuya tipificación se complejizaba en razón de la deslucida redacción normativa.

Los legisladores, en este caso, optaron por realizar una serie de modificaciones al Código Penal de la Nación, incorporando al digesto de fondo términos y conductas abarcativas del fenómeno delictivo bajo estudio.

Así, el artículo 1ro de la ley 26.388, resinificó términos e incorporó al artículo 77 del Código de fondo una serie de aclaraciones, conforme veremos a continuación:

- 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.

Corresponde mencionar que, en torno al termino "documento", la ley se apartó de la formula que se estableciera a partir de la sanción de la ley 25.506, que como sostuviera anteriormente resultó parcial, por cuanto sólo incluyo a los instrumentos privados -en contraposición con los documentos públicos-, y utilizó una formula más efectiva y comprensiva, reconociendo al documento en sí mismo, ajeno al soporte en que se encuentre.

En ese marco, también vale recordar que en el artículo 14 de la ley 26.388, se dispuso derogar la disposición que surgía del artículo 51 de la ley 25.506.

A continuación del precitado artículo, se presentan los tipos penales propiamente dichos, que serán analizados de uno en uno, para una mejor y mas efectiva lectura.

- Pornografía infantil

(art. 128 CP).

La reforma introducida por el artículo 2 de la ley bajo estudio, modificó el artículo 128 del Código Penal de la Nación, relacionado con la pornografía infantil, incluido en el Título III. "*El único punto que une a todos los delitos que trata el Título III del Código Penal no es la honestidad, como se dice, sino lo sexual*" (Donna, E. 1999).

Así, la redacción vigente hasta ese entonces, establecida en la ley 25.087 (año 1999) disponía

"Será reprimido con prisión de seis meses a cuatro años el que produjere o publicare imágenes pornográficas en que se exhibieran menores de dieciocho años, al igual que el que organizare espectáculos en vivo con escenas pornográficas en que participaren dichos menores. En la misma pena incurrirá el que distribuyere imágenes pornográficas cuyas características externas hiciere manifiesto que en ellas se ha grabado o fotografiado la exhibición de menores de dieciocho años de edad al momento de la creación de la imagen. Será reprimido con prisión de un mes a tres años quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años."

La reforma estableció la siguiente redacción del artículo 128 del Código Penal de la Nación, actualmente vigente:

"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."

De este modo, se verifica que la reforma introdujo dos grandes modificaciones, sustanciales en la descripción del tipo penal. Por un lado, se reemplazó la palabra "imagen" por "representación", lo cual amplió el rango de cobertura de las piezas que infringen la norma.

En efecto, la representación incluye a las imágenes, pero también a los videos,

las fotografías, y hasta los dibujos. Representación, según la Real Academia Española significa figura, imagen o idea que sustituye a la realidad.

Por su parte, la norma amplió la nómina de sujetos pasibles de ser alcanzados por aquella, ya que ahora no solo se penará al que produce o pública, sino que el verbo típico es inmensamente más abarcativo.

De tal forma los verbos típicos quedaron alcanzados todos por la norma; "produce" quien elabora o crea; "publica" o "divulga" aquel que hace manifiesto un hecho a terceros, que hace notorio algo, por cualquier medio, para conocimiento de todos, "distribuye" quien hace entrega o pone a disposición de terceros el material de que se trata, hasta un número indeterminado de sujetos, "financia" el que provee los fondos para la empresa, "ofrece" aquel que la presenta y da voluntariamente a terceros, "comercia" el que obtiene un rédito para sí por la dación del material pornográfico y "facilita" aquel que acerca a otros algo para que, sin esfuerzo, pueda ser obtenido (Tobares Catalá, G.H. y Castro Argüello, M.J., 2009).

Asimismo, es válido mencionar que en la redacción se tipificó aquellas conductas relacionadas directamente con la autoría, pero también las secundarias, propias de los participes, que ayuda indirectamente a cometer el delito: financiar y facilitar (Palazzi, P.A., 2012).

Por otro lado, también debo indicar que la penalización incluye, a partir de la nueva redacción, la representación de las partes genitales del menor, con fines predominantemente sexuales, no siendo necesario ya la visualización completa de un menor.

En otro orden de ideas, un hito importante y definitivo que marcó el nuevo artículo 128 del Código Penal, es la incorporación de la aclaración de que las acciones típicas pueden realizarse "*por cualquier medio*", diferenciándose de la anterior redacción, vetusta y que parecía ajustarse más a la publicación tradicional impresa.

Ello, en consonancia con el espíritu de la ley 26.388, permite sin lugar a dudas afirmar que el medio comisivo puede darse tanto en la realidad como en el espacio virtual, sitio en el que ha proliferado exponencialmente la oferta y demanda de pornografía infantil (Oficina de las Naciones Unidas contra la Droga y el Delito,

2010).

En torno al bien jurídico protegido por el instituto, aquel es la indemnidad sexual de los menores, preserva a los menores de la explotación en la producción del material pornográfico (Tobares Catalá, G.H y Castro Argüello, M.J., 2009).

En igual sentido, en la Convención sobre los Derechos del Niño de las Naciones Unidas, en su artículo 34, compromete a los estados parte a proteger al niño contra distintas formas de explotación, entre ellas la explotación del menor en espectáculos o materiales pornográficos (inciso "c") como así también 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 (arts. 2 y 3).

Asimismo, la protección de la integridad de los menores frente al crecimiento de los casos de pornografía infantil, también fue abarcada por la el Convenio de Ciberdelito de Budapest, que mas adelante se analizará.

En otro orden de ideas, corresponde mencionar que, además de las conductas descriptas hasta aquí, el párrafo segundo estipula la tenencia de las representaciones sexuales de menores, con el agregado de que aquella debe tener como fin unívoco la distribución o comercialización.

Así, la simple tenencia de representaciones pornográficas de menores no constituye un delito, sino conlleva consigo la finalidad inequívoca de distribución o comercio.

Es menester mencionar que dicha ultra intención, si bien no es de simple probanza, se asimila a otros tipos penales; por ejemplo, aquel que surge del artículo 5to inciso "C" de la ley 23.737, en la que la jurisprudencia se ha ocupado de delinear los parámetros para demostrar dicha intención final.

Por su parte, respecto del aspecto subjetivo requerido por el tipo penal, será sólo plausible de aplicación a través del dolo directo. "*Entendemos que la redacción dada al tipo penal no deja lugar a dudas de que se trata de una figura dolosa (requiriendo la presencia de dolo directo), como lo son también el resto de las figuras del capítulo*" (Palazzi, P.A., 2012, pag. 52).

En resumen, el artículo 128 incorporado por la ley 26.388 permitió despejar las

dudas en torno a la penalización de la distribución por medios electrónicos de representaciones pornográficas de menores de edad, como así también la tenencia con fines de comercio o distribución, aunados los terceros participes en los hechos.

- Violación de secretos y de la privacidad:

Artículo 153 C.P.

Para comprender el alcance que pretendió tener la ley 26.388, resulta demostrativa la disposición de su artículo tercero, que modificó el título del Libro II del Título V del III, disponiendo que el mismo se llamara "violación de secretos y de la privacidad" (hasta ese entonces el título era "violación de secretos").

En ese marco, uno de los valores mas importantes frente al avance tecnológico es la información, y en consecuencia, el derecho a que aquella, en todas sus formas, se encuentre protegido y reservado.

Ya desde la reforma constitucional del año 1994, con la introducción del "habeas data", o con la ley 25.326 ya analizada, se demostró aquel interés en los datos existentes en las diversas bases de datos, como así también en el uso que se da a dicha información.

Asimismo, la privacidad de las comunicaciones se encuentra debidamente resguardada no sólo en nuestra constitución nacional (artículos 18 y 19) sino también vigorizada en distintos tratados internacionales, como en el artículo 11 inciso 2do de la Convención Americana de Derechos Humanos, o en el artículo 17 inciso 1ro del Pacto Internacional de Derechos Civiles y Políticos.

En ese marco, la privacidad, como bien jurídico protegido por el tipo penal, puede ser susceptible de diversos ataques que merecen su tutela "*El más antiguo es el ingreso no consentido a la morada, recinto tradicional de la vida privada. La versión más moderna de esta acceso no autorizado es el ilegítimo a sistemas informáticos, que la reforma incluye como art. 153 bis…"* (Palazzi, P.A., 2012, pag. 68).

Es decir, la privacidad, poco a poco se fue trasladando de los lugares físicos e íntimos, a espacios virtuales, donde hoy día "transitamos" y "desarrollamos" gran parte de nuestra vida.

De tal manera, la primer modificación se produjo en el artículo 4rto de la ley, dispuso sustituir el artículo 153 del Código Penal de la Nación, que hasta ese entonces disponía:

Artículo 153: Será reprimido con prisión de quince días a seis meses, el que abriera indebidamente una carta, un pliego cerrado o un despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido; o se apoderare indebidamente de una carta, de un pliego, de un despacho o de otro papel privado, aunque no esté cerrado; o suprimiere o desviare de su destino una correspondencia que no le esté dirigida.

Se le aplicará prisión de un mes a un año, si el culpable comunicare a otro o publicare el contenido de la carta, escrito o despacho.

Ahora bien, luego de la reforma, el artículo quedó redactado del siguiente modo:

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.

De su rápida lectura, se advierte que el centro de la modificación estuvo orientado a incluir, en forma clara y directa, las comunicaciones electrónicas, equiparándolas con las telefónicas y cartas epistolares.

Por otro lado, se incluyó la conducta de quien intercepta o captara las comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado.

Dichos párrafos, completaron el abanico de conductas relacionadas con los nuevos modos de comunicación, permitiendo incluir entre ellas, los mensajes de texto,

las cartas, los llamados, los mensajes de *whatsapp*, *facebook*, mail y cualquier otro modo que, a futuro, se utilizara para comunicarse.

Finalmente, la reforma incorporó una pena especial de inhabilitación en caso de que el delito fuera cometido por un funcionario público.

Como bien señala el Dr. Palazzi, la reforma no innova en cuanto al tipo penal, ni crea una nueva figura, sino que agrega, en forma directa, el término "comunicación electrónica", a los otros modos comisivos preexistentes en el tipo penal.

De tal forma, lo que se hizo fue evitar el continuo debate en torno a si, en la descripción anterior, aquellas se encontraban previstas o, por el contrario, resultaban atípicas por el medio. Al respecto, "*...la garantía constitucional de la correspondencia se aplica también al correo electrónico, a los fines de dotarla de todas las garantías constitucionales que resguardan un medio de comunicación personal. Pero es distinto considerar que resulta delito "abrir" un correo electrónico sin permiso, cuando la norma no fue prevista para medios digitales*" (Palazzi, P.A. 2012, pag. 70).

Abrir, para Creus, es "… remover los obstáculos que impiden la lectura del contenido de la carta, pliego, etc., a raíz de su cerramiento, quebrantando o violando de cualquier modo, pero con significado material que recaiga sobre el obstáculo mismo: romper el sobre que cubre..." (Creus, C. 1998, pag. 351).

En este vaivén discursivo, recordemos, que en el año 1999, a través del fallo "Lanata", la Cámara Nacional de Casación Penal, Sala IV, sostuvo la equiparación "*... a los fines de la protección de los papeles privados y la correspondencia prevista en los arts. 153 y 155 del Cód. Penal- al correo electrónico, -"e-mail"- con el correo tradicional, dado que aquél posee características de protección de la privacidad más acentuadas que la inveterada vía postal, en tanto que para su funcionamiento se requiere un prestador del servicio, el nombre del usuario y un código de acceso que impide a terceros extraños la intromisión en los datos que a través del mismo puedan emitirse o archivarse*".

Ello, desplegó un sinnúmero de críticas por parte de la doctrina, resultando que cuestionaron ese "abrir", orientado a la carta tradicional, no debía ser aplicado a los medios electrónicos (Pont Vergues, F. y Brolese, F., 2009).

Con tales antecedentes, la reforma incorporó, con acierto, el "accediere indebidamente", que conjuntamente con el "abrir", abarcaron las conductas relacionadas ya no solo con la correspondencia epistolar, sino también con las comunicaciones electrónicas.

En este sentido, en torno a las acciones punibles de interés para el presente trabajo, aparecen en primer lugar el abrir o el acceder a una comunicación electrónica, de forma indebida. Así, el acceso a una comunicación se producirá al tener contacto, en forma deliberada, con una comunicación por parte de una persona para quien no estaba dirigida.

De tal manera, dicho acceso o apertura puede producirse tanto en mails, chats, mensajes de texto enviados y recibidos por celular, y en cualquier dispositivo o situación en que, entre dos personas, se esté dando una comunicación de carácter privado.

No privado como sinónimo de secreto, sino como un hecho ajeno a la injerencia de terceros que no son parte. La apertura, será indebida cuando ha sido realizada sin derecho; por el contrario, habrá derecho en caso de mediar orden judicial o medida que así lo disponga (Palazzi, P.A., 2012).

Para Creus (1998), en consonancia con lo sostenido por Palazzi, tiene que tratarse de una apertura indebida, o sea de la realizada sin derecho.

La siguiente conducta que aparece en el artículo bajo análisis es el "apoderamiento indebido de una comunicación electrónica"; dicho verbo típico, también presenta una situación digna de ser analizada.

En ese marco, el apoderamiento, sobre elementos físicos, trae aparejada un desapoderamiento en el otro, una pérdida de ese objeto en la víctima, como consecuencia de las características de los objetos de existencia real (por llamarlos de algún modo).

Sin embargo, ello no se presenta en el mundo de las comunicaciones electrónicas, en las que, el apoderamiento de uno, no significa el desapoderamiento en el otro; existe una posibilidad infinita de replicar un archivo informático, sin afectar las cualidades de ninguno de ellos.

De este modo, al haber el legislador conjugado el término "apoderarse" con la "comunicación electrónica", se sobrentiende que la acción ya no requiere que se produzca un desapoderamiento en la víctima, sino que la simple apertura o copia del documento electrónico que se traté, en forma indebida, transformará la conducta en típica frente al derecho penal.

Como bien aclara Palazzi (2012), se incurrirá en el tipo penal en caso de apoderarse de un archivo que forma parte de una comunicación electrónica, en caso de tratarse de otro tipo de archivos, podría encuadrar la conducta en el artículo 153 bis y, si se destruyese a su vez el original, podría haber un concurso con el daño informático.

Finalmente, el primer párrafo del artículo bajo análisis penaliza al que indebidamente suprimiere o desviare de su destino una comunicación electrónica.

De tal formal, el tipo delictivo consiste en impedir que una comunicación electrónica llegue a su destino, por sacarla de su curso o por desviarla a un destino distinto al que tenía.

Es importante aclarar, que el sujeto activo en el delito, debe ser una persona distinta que aquella para quien estaba destinada la comunicación.

Asimismo, por las características propias de la tecnología, es válido remarcar que el desvío o la supresión del correo electrónico puede darse tanto cuando aquel se encuentra "en curso", como así también una vez recibido por el destinatario, en tanto y en cuanto este no lo haya advertido.

Una vez que el destinatario recibe la misiva y se hace carne de su contenido, la conducta en caso de suprimir la manda podría constituir otro tipo de delito, como aquellos analizados previamente, o daño informático, como se verá mas adelante, pero ya no el presente.

El párrafo segundo del artículo 153 dispone "*En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido".*

Este nuevo agregado, suplió el vacío legal que existía, en la anterior redacción del artículo, con las intervenciones telefónicas que fueran realizadas indebidamente.

En efecto, como explicáramos previamente, la penalización de las intervenciones telefónicas indebidas se hallaba sólo prevista en la ley de inteligencia (25.520), y la norma era sólo aplicable a los miembros de los servicios de inteligencia.

Recordemos que la ley de comunicaciones nro. 19.789, disponía que las comunicaciones eran inviolables, y que aquellas podían ser sólo interceptadas mediante la orden de un juez; sin embargo, no se establecieron penas en la norma que dieran lugar al surgimiento de delitos.

Por tal motivo, la ausencia de normas penales permitía que cualquier persona, con los conocimientos y herramientas necesarias, pudiera producir una intervención de una comunicación sin que ello tuviera una consecuencia penal, por resultar la conducta atípica.

Por otra parte, corresponde mencionar que, a partir de la redacción del párrafo segundo del artículo 153 del Código Penal, se previó no sólo la escucha telefónica tradicional, sino también aquellas que se dan por los nuevos medios digitales, al incorporar, una vez más, en la descripción del tipo penal las "*comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido".*

Para finalizar, el último párrafo del artículo dispone que "*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".*

En comparación con la redacción anterior, se agregó, una vez mas, la frase "comunicación electrónica", para comprender los delitos tecnológicos en el tipo penal.

Puede aclarase, si, que quien divulga debe ser la misma persona que realiza las acciones descriptas ya que, en caso de tratarse de una persona distinta aquella, la conducta podría resultar constitutiva de aquella establecida en el artículo 155 del Código Penal de la Nación

Palazzi (2012) sostiene que si "*...el que publica es un tercero, en ese caso resultará aplicable el art. 155, CPen, y si la publicación fue hecha con el propósito de defender un interés publico, encontrará protección en el segundo párrafo de dicha norma*".

El aspecto subjetivo

Común a todas las conductas aquí tratadas, es el aspecto objetivo requerido por el tipo penal.

Ha sido "insistente" el legislador, al aclarar, en cada uno de los casos que los comportamientos debían ser "indebidos", carentes de una autorización de derecho, que habilite la conducta.

De tal modo, el delito requiere una conducta dirigida a realizar el tipo penal, no permitiendo la realización culposa del mismo, sino que siempre requerirá del dolo en el autor.

En su anterior redacción, al analizar cada una de las conductas, Creus sostiene la necesidad del dolo en el autor para tener por configurado el tipo; "*...se requiere en el autor el conocimiento del carácter del objeto y de lo indebido del apoderamiento que perpetra (el error en estos aspectos podría excluir la culpabilidad), y sería sólo admisible el dolo directo*" (Creus, C. 1998, pag. 353).

Vale mencionar, que reconoce el dolo eventual en la supresión o desvío de correspondencia, pero ello no resulta aplicable al ámbito tecnológico, ya que Creus considera que quien puede cometer el hecho es el cartero, aquí inexistente.

Donna, por su parte, al referirse al primer supuesto del artículo, sostiene que el tipo penal, exige el dolo directo, de manera que no sólo se exige que el autor conozca que se trata de una carta, pliego cerrado, de un despacho telegráfico o telefónico, sino, además, que se encuentre cerrado y que se lo abra, de manera indebida. Además debe ser consciente de que la carta no estaba dirigida a su persona (Donna, E., 2001).

- Acceso ilegítimo a sistemas informático

Artículo 153 bis C.P.

Uno de las conductas que precisaba mayor atención, era el acceso ilegítimo a sistemas informáticos, que hasta el momento se encontraba huérfana de sanción penal, al no estar prevista en el ordenamiento positivo.

De tal manera, se incorporó el artículo 153 bis, en el que se dispuso lo siguiente:

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

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

Así, es dable mencionar que la conducta aquí penalizada es la del hacker. La expresión, conforme explican los Dres. Tobares y Castro (2009), hace referencia a un conjunto de comportamientos de acceso o interferencia subrepticios, a un sistema informático o red de comunicación electrónica de datos y a su utilización, sin autorización o mas allá de lo debido.

De dicha descripción, puede colegirse que, por un lado, la ultra intención no está relacionada con la destrucción ni con el producir un daño, sino con la finalidad de burlar un sistema con ciertas medidas de seguridad, dispuestas para impedirlo. Por otro lado, se diferencias de los "crackers", quienes no sólo se encargan de violar sistemas como los antes mencionados, sino que además tienen como finalidad destruir, borrar, o robar información de los sistemas que atacan.

En pos de lo expuesto, se desprende que el bien jurídico protegido por el artículo 153 bis es el derecho a la privacidad. Como bien sostiene el Dr. Palazzi (2012), se amparan la reserva, la confidencialidad y el derecho a la privacidad del titular del sistema y del dato informático.

Respecto del tipo penal, el aspecto objetivo se conforma por el acceso por cualquier medio a un sistema o dato informático de ingreso restringido, sin la debida autorización.

En primer lugar, es dable remarcar que el sistema al que se ingresa debe tener algún tipo de protección , y no hallarse con libre acceso, ya que caso contrario, caeríamos en el absurdo de que navegar por internet se convertiría en delito.

En ese marco, el ingreso sin autorización debe sortear las barreras o trabas dispuestas para que el ingreso no sea público; no simplemente desde un punto de vista fáctico, como explica Palazzi (2012) sino desde el punto de vista normativo.

Así, ejemplifica el autor que el ingreso indebido a un ordenador en forma remota puede realizarse, sin embargo, no debe hacerse, y eso clasifica el acceso como restringido.

Por otro lado, el acceso "por cualquier medio" permite englobar una serie de conductas: por una parte, puede darse por el acceso remoto desde una computadora y por internet; pero también puede darse al sentarse frente a un computadora y acceder a los archivos almacenados en ella, o al tomar un celular ajeno, y mediante el "hack" de su clave de acceso, se tomara contacto con archivos almacenados en el mismo.

De igual forma, el acceso puede producirse mediante la utilización de programas destinados a tal fin, como por ejemplo los de "spyware", que se instalan sin autorización del usuario en los ordenadores y a partir de allí, tienen acceso a datos personales.

Respecto del acceso sin autorización a redes sociales -en su sector privado-, o a sistemas de almacenamiento en la nube, entiendo que la violación de dichos sistemas, deberán ser encuadrados en la norma analizada, en caso de no encuadrar en un delito mas severamente penado.

De tal manera, sistema informático es aquel que permite almacenar y procesar información, y en el que interactúan hardware, software y personal informático o usuario. El "sistema informático" fue definido, a su vez, en el convenio sobre la ciberdelincuencia suscripto en Budapest, en el año 2001, como todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

En ese norte, se verifica que tanto las redes sociales como los servidores para almacenamiento de datos en la nube o en la red, reúnen todos los requisitos descriptos. Respecto del "almacenamiento en la nube" es válido recordar que aquello es una ficción, por cuanto el almacenamiento se produce, en realidad, en servidores que, aunque lejanos, son de existencia real.

Por su lado, ambos sistemas poseen sistemas de prevención de ingresos no deseados, dotándose así de todos los elementos requeridos por el tipo penal.

Sobre el particular, vale mencionar que, en ambos casos, no se requiere que el atacante interactúe con la información allí almacenada ni tome conocimiento, por ejemplo, con conversaciones privadas, sino que lo que se requiere es el simple acceso.

Finalmente, en torno al elemento subjetivo requerido por el tipo penal, una vez mas nos hallamos frente a un tipo de carácter doloso, que no deja posibilidad de que su comisión sea imputable por ninguna de las formas culposas.

- Publicación indebida de una comunicación electrónica

Artículo 155 C.P.

El artículo 6to de la reforma introducida por la ley 26.388 modificó el artículo 155 del Código Penal, que quedó a partir de ese entonces redactado del siguiente modo:

> "*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.*"

La introducción que se hizo al artículo, más relevante, fue el reemplazo de la fórmula "correspondencia" por "una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza*"*, volviéndose de este modo, absolutamente abarcativa de los diversos modos de comunicación modernos, al ampliar el objeto del delito.

Al igual que en el artículo 153, la norma requiere que la publicación se produzca de forma indebida, sin derecho, circunstancia que fue debidamente analizada en su oportunidad.

En torno al bien jurídico protegido por la norma, Creus C. (1998) sostiene que la correspondencia dirigida a otro por cualquier persona no sale de la esfera de reserva del remitente más que con referencia al destinatario; y que la publicación elimina

dicha reserva, por lo que se viola su libertad, aunque no contenga secretos, y eso ocurre hasta en las hipótesis en que el ataque provenga del mismo destinatario.

Por su lado, los elementos que hacen a la consumación desde el punto de vista objetivos son tres: que la correspondencia no sea destinada a la publicidad; que aquel que la posea la haga pública indebidamente y que el hecho de la publicación pueda ocasionar perjuicio (Donna E. 2001).

Hoy día, la interpretación de la doctrina, que data de fecha previa a la sanción de la norma bajo estudio, perfectamente encuadra en las previsiones de la nueva redacción, que principalmente amplió los objetos del delito, expresándolos de forma clara y precisa, para volverlos objeto de protección del derecho penal.

Ello no quiere decir que antes no estuvieran cubiertos, sino que lo que se cercenó es el continuo cuestionamiento de los ámbitos de previsión del tipo penal.

Por otro lado, es válido mencionar que el único conflicto que puede presentar la normativa, es la determinación de cuando una comunicación está destinada a la publicidad, lo cual a su vez permite comprobar que la publicación es indebida.

Así, entiendo que en una comunicación existe un pacto implícito en torno a la privacidad de la misma, entre los interlocutores existe un acuerdo tácito respecto de que sus expresiones quedarán en el ámbito de su privacidad (Donna, E 2001).

De tal forma, la publicación sin la autorización expresa o tácita de los hablado, la volverá indebida, en tanto no se esté frente al supuesto que surge del último párrafo del artículo, y la publicación tenga la finalidad unívoca de proteger un interés público.

Por su parte, en torno al perjuicio, aquel puede ser de cualquier naturaleza (moral, material, patrimonial, etc). Asimismo, aquel puede recaer sobre el remitente, el destinatario o sobre terceros extraños a la comunicación de que se trate.

Lo importantes, y necesario, es que el perjuicio recaiga o pueda recaer sobre persona distinta del agente que hace publicar la correspondencia, sin perjuicio de que, a la par, se afecte al autor del delito (Creus, C.1998).

Para finalizar, no es ocioso mencionar que nos encontramos ante un delito doloso. Al respecto, a sostenido la doctrina que el autor debe conocer que está frente a una correspondencia, que ésta no puede ser dada a publicidad, que la publicación es

indebida y que puede u ocasiona un perjuicio; "…*sólo es admisible el dolo directo, y la segunda, que el perjuicio es un elemento del tipo que integra el dolo.."* (Donna, E. 2001).

- Revelación de secretos

Artículo 157 C.P.

La reforma introdujo una modificación en el artículo 157 del Código Penal, que actualmente se encuentra redactado de la siguiente forma:

> "*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*".

Así, en comparación con su redacción anterior, la norma incorporó el término "datos" como objeto del delito. Ello, aunado a la equiparación realizada por el artículo 1ro de la ley, en tanto dispone que a la palabra documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión, amplió el ámbito de protección del derecho penal, abarcando aquellos presentes en sistemas informáticos.

Por su lado, en torno al sujeto activo sobre el que recae la norma penal, conforme estipula el artículo 77 del Código Penal de la Nación, es todo aquel que participa accidental o permanentemente del ejercicio de funciones públicas, sea por elección popular o por nombramiento de autoridad competente.

De tal manera, la incorporación del término dato, si bien resulta extremadamente impreciso, permite que el ámbito de protección de la norma penetre hasta en los más mínimos detalles, e impida la revelación de cuestiones que, por sus características deban ser secretas.

La acción típica consiste en revelar el secreto, para lo cual es suficiente con que se lo comunique a cualquier persona, en tanto y en cuento no sea una de las que, como el agente, están obligadas a guardar el secreto (Creus, C. 2008). La acción no consiste en "divulgar", sino en "revelar" que, si bien va más allá de comunicar, no implica publicar (Donna, E. 2001)

Por su lado, el carácter de secreto, desde el punto de vista de la norma penal, estará dado por otra norma que especifique que determinado dato o documento debe ser secreto.

En ese sentido, esa disposición de la ley puede ser directa (indicando determinados documentos como secretos o reservados) o indirecta, esto es, delegando en determinados funcionarios la facultad de determinar lo que es secreto por medio de reglamentos, resoluciones u órdenes (Creus, C. 2008)

Respecto del aspecto subjetivo creado por el tipo penal, aquel requiere del dolo, pero en este caso permite el dolo eventual. Tal es el caso del funcionario público que deja en manos de un tercero un documento que debe ser secreto, sabiendo que aquel puede enterarse de su contenido, y acepta la consecuencia de su acción (Palazzi, P.A. 2012).

- Protección de datos personales

Artículo 157 bis C.P.

Una de las modificaciones más importantes que realizó la ley 26.388 fue la del artículo 157 bis del Código Penal de la Nación a través de su artículo 8vo.

El mismo, actualmente dispone:

> *"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."*

Es importante señalar que, a su vez, relacionado con el presente, que mediante el artículo 14 de la ley 26.388 se derogó el inciso 1ro del artículo 117 bis -oportunamente

incorporado por la ley 25.326-, cuyo contenido pasó a formar parte del nuevo artículo 157 bis, inciso 3ro, con algunas modificaciones.

Dicha decisión, tuvo su fundamento, principalmente, en las críticas que produjo que se incorporara, por la ley 25.326, la protección respecto de la inserción de datos falsos en bancos de datos personales, dentro del título "Delitos contra el honor" del Código Penal (Palazzi, 2012).

Ello, por cuanto dicha decisión resultó confusa en torno al bien jurídico protegido por la norma, que como bien se corrigió a través de la ley aquí bajo estudio, es la privacidad.

Ahora, con la nueva redacción, se incluyen y reprimen en el artículo 3 conductas relacionadas con la privacidad de los bancos de datos personales, en las distintas aristas que pueden hacer a su afectación.

El primero de ellos, reprime el simple acceso no autorizado a un banco de datos personales.

Al respecto, Riquert sostiene que la acción típica de acceder a la base de datos, puede ser realizada por cualquier medio, si bien el tenor de la ley indica que el legislador quiso hacer énfasis o señalar los medios informáticos. La acción típica de acceder puede concretarse por cualquier medio.

Por su lado, enseña que "*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. La lesión al bien jurídico protegido se concreta con el mero acceso*" (Riquert, M.A., 2014).

Por su parte, es válido mencionar que los bancos de datos personales, deben poseer medidas de confidencialidad y seguridad, adoptadas por el responsable del banco de datos, y serán dichas barreras las que el autos debe violar para lograr acceder a la información.

Sobre el tipo penal, también debe hacerse mención a que el acceso al banco de datos personales, debe realizarse "*a sabiendas e ilegítimamente"*, o *"violando sistemas de confidencialidad y seguridad de datos"*. Dicha redacción ha recibido críticas por parte de la doctrina, con gran atino.

En ese norte, Palazzi refiere que la conjunción alternativa "o", carece de sentido, ya que no son alternativas, ya que ambos requisitos deberían estar presentes "*...a menos que se interprete que el recaudo de burlar medidas de seguridad es solo una opción...*". Sin embargo, no es una alternativa a cuando no se actúe con dolo e ilegítimamente (porque estos elementos siempre deberán estar presentes para que se cometa el delito) (Palazzi, P.A. 2012).

El segundo de los supuestos, esta dado por quién ilegítimamente proporcione o brinde información registrada en un archivo o en un banco de datos personales.

La reforma incorporó el término "archivo" como objeto del delito, y como parte de la acción la formula "ilegítimamente proporcionara", no previstas en la redacción original incorporada por la ley 25.326.

De tal manera, lo que se hizo, en primer lugar, es ampliar el marco de protección de la norma, que no requiere ya la existencia efectiva de un banco de datos, sino que la información revelada puede pertenecer a un simple archivo que contenga datos.

Por su parte, la acción punible se compone por proporcionar en forma ilegítima; proporcionar en tanto dar a una persona o una cosa algo que necesita para un fin determinado o que le conviene y que no puede obtener por sí misma, o dejar que disponga de ello.

Ilegítimo, por su lado, será en los términos de la norma regulatoria de los datos personales, ley 25.326, que establece un deber de secreto o confidencialidad en su artículo 10, sobre los responsables de las bases de datos como así también sobre todos aquellos que intervengan en el tratamiento, incluso luego de terminada la relación con el titular del servicio.

La mención del término "ilegítimamente" es un elemento muy importante: requiere analizar si la revelación de los datos es legal o no, de conformidad con el ordenamiento jurídico vigente. Ello se resume básicamente en el cumplimiento de la ley 25.326 y sus reglamentaciones (Palazzi, P.A. 2012).

La última de las tres conductas establecidas en el tipo penal es la de insertar o hacer insertar, ilegítimamente, datos en una base de datos.

Así, como dijera al comienzo de este punto, la conducta se hallaba, con un tenor

similar, prevista en el artículo 117 bis del Código Penal de la Nación -inciso 1ro-, que penaba a quién insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

De tal manera, se eliminó el requisito de que los datos sean falsos, ya que el bien jurídico protegido es la privacidad, y la afectación de dicho bien puede será lesionado por la inserción de datos, independientemente de su relación con la veracidad.

Ya no se pretende, como otrora, proteger el honor y la lesión de aquel mediante datos falaces, sino la integridad de los datos de una persona.

> 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 este 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".
>
> Riquert, M.A. (2014)

Finalmente, la acción aquí analizada consiste en insertar o hacer insertar, permitiendo la acción por terceros.

Respecto del verbo típico, definido como "introducir algo en otra cosa" (Real Academia Española), se entiende por la agregación de un dato sin destruir ni dañar los preexistentes (ya que si no nos hallaríamos frente a otras conductas).

Finalmente, como dato relevante resulta importante mencionar que Palazzi (2012), refiere que esta figura es candidata al concurso con el daño informático, en

tanto uno tiene la finalidad de dañar o destruir la información (delito de daño), distinta a la de perjudicar al sujeto referenciado en el banco de datos personales (delito de inserción de datos).

Como colofón, en torno al aspecto subjetivo de los tipos penales analizados, es válido remarcar que todos ellos son de carácter doloso, ya que los verbos típicos estudiados no admiten, de ninguna forma, un tipo comisivo distinto, por lo que sus formas culposas serán obsoletas.

- Fraude informático

Artículo 173 inciso 16 C.P.

Otra de las conductas que requería una atención inmediata era el fraude mediante la utilización de computadoras o fraude informático. Al respecto, recordemos que sólo se hallaba estipulado el fraude mediante la utilización de tarjetas de crédito, pero no aquellas defraudaciones que, sin la intervención de las mismas se dieran por medios informáticos.

Como situación novel, la incorporación del artículo permite, por primera vez en nuestro derecho, que la defraudación, se aparte por primera vez de la tríada constitutiva del tipo penal, compuesta por el ardid, el error y la disposición patrimonial.

En efecto, las discusiones doctrinarias y jurisprudenciales suscitadas a partir de la aparición de las defraudaciones informáticas, previas a la sanción reparadora de la ley 26.388, giraban en torno a la ausencia de dichos elementos en algunas estafas informáticas.

Al respecto, existen numerosos modos comisivos, que ahora han quedado subsanados, pero que históricamente se hallaban huérfanos, en un vaivén discursivo que los corría de la estafa al hurto y viceversa. Como sostienen los Dres. Tobares Catalá y Castro Argüello (2009), la imposibilidad de hacer caer en error a una máquina había provocado lagunas de punibilidad, en casos que claramente merecían la pena de la estafa.

Por tal motivo, el nuevo inciso incorporado al artículo 173 eliminó dichas

barreras, y clarificó el panorama para la correcta adecuación de las conductas disvaliosas relacionadas con las estafas informáticas. De este modo, el trinomio requerido por la estafa es ahora reemplazado, en el supuesto analizado por la acción de realizar cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

En torno al bien jurídico protegido por el tipo penal, es dable destacar que su inclusión dentro de los supuestos de defraudación especiales del artículo 173, permite corroborar que lo que se intenta proteger es el patrimonio de la víctima.

El Dr. Palazzi (2012) destaca una serie de fraudes informáticos:

> 1. Alteración de registros informáticos: es la alteración mediante la cual se modifica un registro informático relacionado con decisiones de pago o con la disposición de fondos (art. 173 inc. 16 CP)
>
> 2. Uso no autorizado de tarjetas y claves falsas o sustraídas o de sus datos: denominado "carding", es la modalidad prevista en el artículo 173 inciso 15. Dicha modalidad se produce tanto con la creación de tarjetas falsas como con la obtención de sus números de registro.
>
> 3. *Mise en scene* en cajeros automáticos: se trata del copiado de datos de tarjetas a través de dispositivos unidos a una computadora. Con dichos elementos, se copian los para luego duplicar las tarjetas.
>
> 4. *Phishing* y robo de identidad: el significado de "phishing" es suplantación de identidad. La maniobra consiste en el envío correos
>
> electrónicos engañosos, con la finalidad de que, a través de páginas web visualmente similares a la de las entidades que presuntamente representan, el usuario ingrese sus datos y claves personales. Luego de ello, "haciéndose pasar" por el verdadero titular, se obtienen

datos bancarios, personales, se realizan operaciones comerciales, bancarias, etc.

5. Estafas en mercados virtuales o con medios de pago: es la estafa a través de portales de ventas, mediante la cual se ofrecen productos a la venta, con la finalidad de nunca entregarlos.

Ahora bien, en torno al tipo penal, la acción penal consiste en defraudar mediante una manipulación en un ordenador o en los datos transmitidos por estos. Palazzi (2012) afirma que con la incorporación de esta nueva norma no solo se pena a los procesos informáticos que son modificados, sino cualquier supuesto de defraudación mediante ordenadores, como accesos ilegítimos mediante claves falsas o phishing o falsos montajes a cajeros automáticos, que quedan cubiertos por esta figura y, con anterioridad a la reforma, estaban incluidos en la figura general del 172 o del art. 173, inc. 15 el Código Penal.

Sine embargo, la norma establecida por el inciso 16, abarcará sólo las maniobras que utilicen cualquier técnica de manipulación informática, quedando por ejemplo el *phishing* abarcado por la estafa (artículo 172 CP), ya que allí no habrá manipulación informática, sino un accionar destinado a inducir a error al usuario.

Para finalizar, respecto del elemento subjetivo requerido por el tipo penal, es claro que nos hallamos ante un delito de neto corto doloso, que requiere del dolo directo para constituirse, signado por el ánimo de lucro (Tobares Catala, G.H. y Castro Argüello, M.J. 2009).

- Daños informático y virus

Artículo 183 segundo párrafo

El agregado como segundo párrafo del artículo 183 del Código Peal de la Nación, incorporó el siguiente texto: "*En la misma pena* (quince días a un año) *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*".

De tal manera, el artículo vino a suplir, como varios de los de la ley analizada, un vacío de punibilidad que existía en razón de la no adecuación típica en el daño o destrucción de archivos o programas informáticos, provocados en forma directa o mediante la utilización de virus informáticos.

Así, la acción típica de la primera parte del artículo es alterar, destruir o inutilizar. Se altera cuando se modifica la esencia o forma de algo. Destruir, por su lado, implica en la jerga informática borrar definitivamente, sin la posibilidad de que pueda ser recuperado.

Finalmente, inutilizar es realizar un cambio en el archivo que no pueda ser reconocido por el ordenador, o no pueda ser abierto, o no pueda ejecutarse; cualquier acción que sin destruirlo impida su funcionamiento.

Así, el objeto del delito pueden ser los *datos, documentos, programas o sistemas informáticos;* este es en realidad el agregado que precisaba el artículo 183 en su anterior redacción, para poder subsumir bajo su marco de protección los daños informáticos.

Sin embargo, la legislación fue más allá, y el ámbito de protección actualmente excede a las computadoras, sino que por la forma utilizada, se hallan protegidos los datos en cualquier soporte en que se encuentren (teléfonos, tarjetas de memoria, etc).

La segunda parte del párrafo segundo del artículo 183, penalizó la distribución de virus informáticos, hasta el momento también huérfanos de punición.

De tal manera, la acción típica es la de vender, distribuir, hacer circular o introducir; no así la simple tenencia de los programas o su creación. El objeto del delito, por su lado, serán los sistemas informáticos en su totalidad.

Ahora bien, resulta relevante mencionar que un programa destinado a causar daños, es lo que comúnmente llamamos virus informático, y debe tener el potencial de producir daños en el hardware o en el software.

También es importante mencionar que no cualquier programa que provoque o pueda provocar daños en un sistema informático podrá ser considerado en los términos del artículo, sino sólo aquellos cuyo fin unívoco sea la causación dañina.

Así, la descripción del tipo penal nos permite verificar que se trata de un delito

de peligro abstracto; es un paso previo respecto del daños que analizáramos párrafos atrás.

En efecto, el artículo 183 segundo párrafo cubre dos etapas distintas del iter criminis, por un lado, si es detectado el potencial dañino de un software al momento de su distribución, se aplicará la norma que surge *in fine*; si se produce el daño, será plausible de aplicación de la primera parte del artículo bajo estudio.

Por su parte, es válido remarcar que la peligrosidad de los daños informáticas fue también receptada por el artículo 184, que en su inciso 6to, agravó las penas en caso de darse sobre 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, aumentando el mínimo de la pena a 3 meses y el máximo a 4 años de prisión.

- Interrupción de las comunicaciones

Artículo 197 C.P.

> "*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*".

La nueva redacción del artículo 197 del Código Penal, agregado a través del artículo 12 de la ley 26.388, incorporó como objeto del delito la comunicación "de otra naturaleza" para así englobar a las nuevas tecnologías.

Como bien señala el Dr. Palazzi (2012) la redacción anterior, a su vez, se hallaba teñida de una protección "de lo público", y con la modificación se incluye cualquier clase de comunicación, como el correo electrónico, llamadas IP, mensajes de chat, de texto por celular o de servicios como *whatsapp* o *messenger*.

Dicho problema, ya lo resaltaba también el Dr. Donna (2002) y el Dr. Creus (1998), que sostenía que resultaba fundamental determinar si se alcanzaban los servicios privados, más aún cuando el decreto-ley 21.338 había agregado la exigencia de que sean públicos o puestas al servicio público

Las primeras tres definiciones que da la Real Academia Española de la palabra "comunicación" es "1. f. Acción y efecto de comunicar o comunicarse, 2. Trato, correspondencia entre dos o más personas.3. f. Transmisión de señales mediante un código común al emisor y al receptor".

En tal entendimiento, resulta válido entender que cualquier ataque o privación de los servicios de internet, o de accesos a una página web, también se hallan amparados por la norma, en tanto se interrumpe la conexión entre el emisor y el receptor.

De esta manera, y a modo de ejemplo, los ataques de "crackers", para indisponer la conexión de los sitios web que atacan, mientras dura el mismo, se hallarían también insertos en la temática bajo estudio.

En torno a la acción típica, la primera parte del artículo sindica la interrupción o el entorpecimiento; interrumpir es introducir una solución de continuidad en el curso de la comunicación. En cambio entorpecer es dificultar la comunicación (Donna, E. 2002).

Por otro lado, la segunda parte del artículo penaliza a quien resista en forma violenta el restablecimiento de la comunicación interrumpida. Para que esta se dé, en primer lugar, debe darse la interrupción de la comunicación, y además, ser resistida en forma violenta, entendiendo esta última como un ataque a una persona.

Finalmente, el aspecto subjetivo de ambos supuestos delictivos, requiere de dolo, y dada la forma de la redacción es difícil pensar el dolo eventual, aunque ello es posible.

- Alteración de pruebas

Artículo 255 C.P.

Finalmente, a través del artículo 13 de la ley 26.388, se modificó el artículo 255 del Código Penal de la Nación, quedando redactado actualmente de la siguiente forma:

> "*Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo*

depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500)".

El único agregado que se realizó, en comparación con su anterior redacción, fue la de "…en todo o en parte…", modificación que no luce en clara sintonía con la necesidad de contemplar las nuevas tecnologías. Se trata de una figura que procura la conservación o preservación de aquellos objetos que estén destinados a servir de prueba cuya custodia hubiere sido confiada a un funcionaria u otra persona en el interés del servicio público (Riquert, M.A. 2014).

Las acciones típicas son la sustracción, alteración, ocultación destrucción o inutilización de cualquier objeto destinado a servir de prueba, documento y registros confiados a la custodia.

Sobre el particular, corresponde mencionar que la redacción del artículo, tal como ha sido sancionado, se presta a confusión toda vez que aparecerían dos modos comisivos independientes; por un lado la sustracción, alteración, ocultación destrucción o inutilización de cualquier objeto destinado a servir de prueba; por el otro, la sustracción, alteración, ocultación, destrucción o inutilización de registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés d l servicio público.

Sin embargo, su ubicación sistémica dentro del Código Penal, y la doctrina actual y relacionada con las versiones anteriores del artículo, plantean que en todas las acciones que surgen del artículo, se requiere la vigencia de una custodia sobre el objeto.

Así lo sostiene Creus C. (1998), al referir que la custodia oficial es un requisito común a todos los objetos típicos, o Donna E. (2002), en tanto afirma que objeto material de la acción son los objetos custodiados con la finalidad de utilizarlos como medios de prueba, de registros o de documentos.

Así, las acciones típicas enunciadas requieren, desde el punto de vista del subjetivo, el conocimiento de su existencia como elemento de prueba, y la finalidad de

quebrantar tal custodia; el autor no persigue dañar el objeto sino su valor probatorio.

Es válido mencionar, para finalizar este punto, que la equiparación realizada a través del artículo 1ro de la ley 26.388 de la palabra “documento", en tanto dispone que comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión, permite englobar en la nueva previsión, la prueba digital o informática.

En ese sentido, el objeto del delito será cualquier elemento destinado a servir de prueba, incluidos los documentos y archivos informáticos; cualquier elemento destinado a servir de prueba, independientemente de su soporte.

3.2 Su relación con el Convenio de Ciberdelito del Consejo de Europa.

En el año 2001, 7 años antes de la sanción de la ley 26.388, el Consejo de Europa (entidad formada luego de la segunda guerra mundial con la finalidad de crear textos relacionados con los derechos humanos), suscribió el “Convenio sobre la Ciberdelincuencia”, firmado en Budapest el 23 de noviembre de 2001. Su entrada en vigencia, se produjo en el año 2004.

Nuestro país, si bien no ha suscripto el convenio, aquel claramente sirvió de base para la redacción de la ley 26.388; más aún, al momento del debate de la ley se reconoció su importancia (exposición de motivos, sesión del 4 de junio de 2008), y refleja muchas de las ideas del mismo.

El convenio se compone por 4 capítulos: el primero aporta terminología específica, como las definiciones para sistema informático, datos informáticos, proveedor de servicios, y datos relativos al tráfico.

El segundo capítulo, denominado “medidas que deberán adoptarse a nivel nacional”, se integra por las normas penales de fondo y de forma, disponiendo en algunos casos normas específicas que deben ser adoptadas y en otros casos, recomendando la protección se ciertos bienes jurídicos o penando determinadas conductas.

Un tercer capítulo sienta las bases de los principios generales de cooperación internacional en la materia, y finalmente el capítulo cuatro es de forma, estableciendo

los modos para la suscripción del convenio.

Pero volviendo al nudo del Convenio, del capítulo 2do del convenio surgen los tipos penales que deben ser adoptados por los firmantes del convenio.

De tal manera, las conductas que, conforme el convenio, deben ser penadas, fueron las siguientes:

A. **Artículo 2, Acceso ilícito.**

Dicha conducta fue recogida por nuestra legislación, en el artículo 153 y 153 bis del Código Penal de la Nación, que prevé la apertura o el acceso ilegítima a un sistema informático (artículo 4rto y 5to de la ley 26.388).

Asimismo, el acceso ilegítimo a bases de datos, como un tipo especial, se encuentra previsto en el artículo 157 bis del código de fondo (art. 8 de la ley 26.388).

B. Artículo 3, Interceptación ilícita

También se halla prevista en el artículo 153 del Código Penal de la Nación, segundo párrafo.

C. Artículo 4, Ataques a la integridad de los datos

Tal supuesto, fue receptado en el artículo 10 de la ley 26.388, que contempló el delito de daño informático, incluido en el ordenamiento de fondo como segundo párrafo del artículo 183 y agravado en el artículo 184 del mismo cuerpo normativo.

D. Artículo 5, Ataques a la integridad del sistema

Al igual que en el punto anterior, la conducta fue receptada en el artículo 10 de la ley 26.388, que contempló el delito de daño a sistemas informáticos, incluido en el ordenamiento de fondo como segundo párrafo del artículo 183 y agravado en el artículo 184 del mismo cuerpo normativo.

E. Artículo 6, Abuso de los dispositivos

El abuso de los dispositivos, como tal, si bien no fue previsto en un artículo

específico, se halla cubierto en los distintos tipos penales relacionados con la temática. En efecto, el convenio dispone que en el abuso de dispositivos, entran los programas informáticos creados para acceder o producir daños, que en nuestro derecho positivo se haya previsto en el artículo 183 segundo párrafo.

Por su lado, también se hallan previstos en el artículo 15 del artículo 173, incorporado por la ley 25.930, tanto en el *carding* como en la *misse en scene* en cajeros automáticos.

F. Artículo 7, Falsificación informática

En este caso, la falsedad documental informática, no fue prevista expresamente, pero aquella se encuentra alcanzada por la modificación realizada en la definición de documento, que incluye toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

G. Artículo 8, Fraude informático

El fraude a través de medios informáticos, fue también recogido por nuestro ordenamiento positivo, en el inciso 16 del artículo 173 del Código Penal, agregado por intermedio del artículo 9no de la ley 26.388.

H. Artículo 9, Delitos relacionados con la pornografía infantil

Gran parte de las conductas previstas en el artículo 9 del convenio de Budapest, fueron previstas a través del artículo 2do de la ley 26.388, que modificó el artículo 128 del Código Penal de la Nación.

Es válido mencionar que, si bien nuestro derecho positivo utiliza la palabra "representación de un menor", no resultaría penalmente imputable la participación de una persona que "parezca" menor, tal como establece el convenio en su punto "2" inciso "b", en tanto no fuera un deliberado intento por representarlo.

I. Y artículo 10, Delitos relacionados con la propiedad intelectual

Los delitos relacionados con la propiedad intelectual, conforme fuera analizado al comienzo del presente trabajo, se hayan previstos en la ley 11.723, y particularmente su modificación a través de la ley 25.036.

En resumen, en comparación con nuestra legislación, si bien el tratado redunda en aclaraciones y deberían realizarse algunas modificaciones, se han cubierto la gran mayoría de las conductas estipuladas en el mismo, habilitando que, en algún momento, nuestro país solicite su incorporación al convenio.

Sobre ello, resulta importante mencionar, que cuantos mas países adhieran a los convenios internacionales sobre ciberdelito, mayor será la efectividad en la persecución delictual; y las mismas barreras que derribó el delito a través de la la tecnología informática, podrán ser salteadas por el derecho penal a través de los acuerdos multilaterales.

4. El "delito de *Grooming*"

4.1 Análisis de la figura.

El último gran hito en la legislación argentina, frente a los delitos informáticos, fue la sanción de la ley 26.904, del 11 de diciembre de 2013, por medio de la que se penó el "*grooming*".

A través de dicha norma, se incorporó como artículo 131 al Código Penal de la Nación, el siguiente texto: "*Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma*".

El *grooming* es cualquier acción que tenga por objeto minar y socavar moral y psicológicamente a una persona, con el fin de conseguir su control a nivel emocional. Aunque puede producirse en cualquier instancia, es particularmente grave cuando una persona realiza estas coacciones y presiones emocionales contra un niño o niña con el objetivo de obtener algún tipo de favor sexual (Gamba S., 2010).

Por su lado, Lo Giudice, M.E. (2013) y Migliorisi D. (2014) describen el *iter criminis* del tipo penal, en tres etapas:

1.- Una inicial, donde se produce el acercamiento por parte del mayor al menor.

2.- Una intermedia, donde ganada ya la confianza, se va obteniendo datos personales de la víctima, de la familia, relaciones sociales. Comienza un intercambio de confidencias, secretos.

3.- La etapa final o de actuación, ya hay una intención sexual, implícita o explícita, puede ser lograr mediante engaño una cita real destinada a lograr, un fin sexual.

De tal manera, la acción penal consiste en contactar a un menor de edad, con la finalidad de cometer cualquier delito contra la integridad sexual. Contactar es, conforme la definición dada por la Real Academia Española, establecer contacto o comunicación con alguien.

En torno a la finalidad, por la redacción del artículo, habrá de estarse a las conductas previstas y reprimidas en el Título III (del Libro II) del Código Penal de la Nación.

Es decir, el mayor debe entablar una comunicación para con el menor, signada por la finalidad de cometer alguno de los delitos establecidos en nuestro ordenamiento positivo, bajo el título delitos contra la identidad sexual.

Por ello, no caben dudas que nos hallamos frente a un tipo penal de neto corte doloso, que no admite otra forma comisiva mas que el dolo directo. Resultaría inapropiado entender que existe otro modo de tipificar la conducta.

4.2 La complejidad de su estructura y de su aplicación

Sin embargo, se ha señalado que no es del todo correcta la etiqueta de "grooming" para designar las acciones tipificadas por resultar extremadamente difícil discernir "ex ante", qué conductas están siendo dirigidas a un abuso y cuáles son, simplemente, conductas de atenciones sinceras respecto de menores (Pescelvi, S.M., 2015).

Por su lado, parte de la doctrina ha criticado, con razón, las complejas

características del tipo penal, que inevitablemente requieren conocer la ultra intención del autor. En ese sentido, en las etapas iniciales de la comisión del delito, no será posible asegurar en forma unívoca cual es esa finalidad, ese fin ulterior que persigue el adulto en la comunicación con el menor.

Por otro lado, si la víctima ya quedó bajo la influencia de un depravado sexual o un sujeto que se entrometió en su normal desarrollo, la conducta quedaría atrapada en el tipo penal de corrupción.

Más aún, si hubiera obtenido fotografías o representaciones del menor de tono sexual, resultaría mas apropiado encuadrar la conducta del mayor en la figura del art. 128 del C.P. verificándose hasta posibles superposiciones de conductas reprimidas.

La Dra. Pescelvi, S.M., (2015) afirma que la aplicación del artículo importa adelantar la barrera punitiva a un acto preparatorio de otro preparatorio, por lo que el delito se convierte en un uno de sospecha que quiebra el principio de lesividad vigente en nuestro sistema constitucional.

En efecto, ni siquiera la intención –muy difícil de probar, por cierto- otorga un plus de lesividad a la conducta sino que, quizás será tranquilizador para aquellos que quieren penar intenciones, algo para lo que no está el derecho penal sino la moral o la religión, en todo caso.

Como se mencionara anteriormente, existen distintos momentos en los que las conductas que intenta prevenir el tipo penal se cruzan con otros tipos penales. En ese entender, en atención a que la parte del contacto, sería aquella que no resulta encuadrable en otros tópicos, hubiera resultado de mayor efectividad, penar la sustitución y/o usurpación virtual de identidad, con lo cual se habría entorpecido la creación de falsos perfiles en redes sociales.

En comparación, por ejemplo, el Código Penal español exige en su artículo 183 ter primer párrafo que el contactado tenga menos de dieciséis años y, que el autor proponga concretar un encuentro, signado ese último por actos materiales encaminados al acercamiento.

De tal manera, se advierte que, si bien es importante la creación de legislación específica en la materia, hubiera resultado más efectiva la creación de un tipo penal al

menos de peligro concreto, que requiriera un acto efectivo para su delimitación, ya que su actual redacción es extremadamente complejo de aplicación.

5. Conclusiones parciales

En base a todo lo expuesto, se verifica que nuestro país ha avanzado, con aciertos y desaciertos, en la penalización de conductas relacionadas con la tecnología, y de conformidad con los estándares mundiales.

No es ocioso mencionar que algunas de las normas analizadas presentan sendas falencias, y otras, han sido desarrolladas con una técnica legislativa implacable.

Asimismo, resulta importante reconocer que el proceso legislativo, si bien ha sido largo y lento, poco a poco fue acercando posiciones con los estándares mundiales, los que deberán unificarse a través de un proceso necesario y sin precedente. Ello, si existe la voluntad política de combatir el fenómeno delictivo de los delitos informáticos en forma suficiente.

UNIVERSIDAD SIGLO 21

CAPITULO 3
LA SITUACIÓN ACTUAL EN MATERIA DE CRIMINALIDAD INFORMÁTICA

1. Introducción

En este capítulo final, y luego del análisis de las cuestiones de derecho fondo, se estudiarán brevemente algunas cuestiones relacionadas con los delitos tecnológicos y el derecho procesal, la recolección de la prueba en el ámbito internacional, como así también se verificarán cuáles son las conductas delictuales que, si bien resultan disvaliosas para la sociedad, se hallan carentes de punibilidad a la fecha del presente trabajo.

2. Problemática en materia procesal

2.1 Determinación de competencia

Una de las características más relevantes que posee la ciberdelincuencia, es la transnacionalidad que presenta en todas sus facetas, y ella es una de las principales barreras que dificultan su persecución.

La gran mayoría de los derechos positivos, se apoyan sobre la idea del principio de territorialidad de la ley penal, y la Argentina no es una excepción, ya que se signa por la aplicación del poder punitivo por los hechos cometidos dentro de las fronteras físicas del país -o que los efectos del mismo se den dentro de las fronteras-, y, en forma subsidiaria, por el principio real o de defensa (artículo 1 del Código Penal de la Nación).

Sin embargo, en el plano del ciberdelito, donde no existe esta delimitación física tan clara, las conductas disvaliosas pueden realizarse en un país, desarrollarse en otro, y tener sus efectos en un tercer lugar. Tal sería el caso, de una intrusión informática desde el país “A”, que retire dinero resguardado en un banco del país “B”, y que afecte a un ciudadano que vive en el país “C”.

Esas situaciones, no suelen darse en los delitos “tradicionales” sino que son propias de esta nueva era de la comunicación, donde las TIC`S acercan los lugares

mas recónditos del mundo a una pantalla.

En el caso de nuestro país, de conformidad con las previsiones del artículo 1ro del Código Penal de la Nación, se halla habilitada la persecución de conductas delictivas, cuando los efectos de un delito se produzcan o deban producirse en el territorio Argentino, o en los lugares sometidos a su jurisdicción.

Dicha habilitación -denominada teoría de la ubicuidad-, resulta esencial al momento de facultar la persecución de delitos cometidos en cualquier parte del mundo, pero cuyos efectos se produzcan dentro de nuestro territorio. En efecto, la teoría de la ubicuidad entiende que el delito se comete tanto donde se produce la manifestación de la voluntad como así también en el sitio en donde se ha producido el resultado.

Sobre el particular, ha sido sostenido por el Ministerio Público Fiscal, ante la Corte Suprema de Justicia, Procurador Luis González Warcalder, que "*En los llamados "delitos a distancia", es decir, en todos aquellos hechos en que los diferentes pasos del iter criminis no se producen en el mismo lugar, la adopción del criterio de ubicuidad para establecer el lugar de comisión de los hechos supone como consecuencia, para los supuestos de tentativa -como en este caso-, que el delito deba reputarse cometido tanto en el lugar donde comenzó la ejecución como en el lugar donde se hubiera consumado (Fallos: 313: 823 y 321:1226)*" (Competencia N° 1497. XL. "Moralejo, Christian Néstor s/ tentativa de extorsión", 2004).

De tal modo, se verifica que nuestro país presenta un derecho positivo que facilita la persecución de los delitos informáticos, en tanto y en cuanto los efectos o las conductas disvaliosas se produzcan dentro del territorio nacional.

2.2 La recolección de la prueba

Como se ha repetido hasta el cansancio en el marco del presente trabajo, la tecnología avanza a pasos agigantados y veloces, y con él lo hacen las conductas disvaliosas que requieren la pronta atención legislativa.

No es distinto el curso que siguen a su vez las técnicas para la obtención de pruebas y la complejidad que presenta tal designio.

En ese sentido, la mayor complejidad se presenta en materia de cooperación internacional para la recolección de la prueba y el desarrollo de diligencias tendientes al esclarecimiento de los hechos respecto de los delitos informáticos.

Sobre ello, resulta importante mencionar que la transnacionalidad que caracteriza a los delitos informáticos, hace necesaria la progresiva adopción de convenios internacionales que agilicen la conservación y disposición de los elementos de prueba, y ello será factible, a su vez, a partir de la consolidación de un derecho penal sobre delitos informáticos unificado o, al menos, de características similares.

Por ello, el Convenio sobre ciberdelincuencia de Budapest resulta un instrumento de derecho penal internacional invaluable, ya que no sólo se halla orientado a unificar las conductas delictivas en los códigos de fondo, sino que presenta una serie de obligaciones para las partes en la obtención y conservación de la prueba.

Así, el convenio dispone que las partes, deben adecuar sus digestos de forma, a los efectos de disponer de mecanismos para la "conservación rápida de datos informáticos" (art. 16), "conservación y revelación parcial rápidas de los datos relativos al tráfico" (art. 17), libramiento de "ordenes de presentación" (art. 18) y orden de "registro y confiscación de datos informáticos" (art. 19), "obtención en tiempo real de datos relativos al tráfico" (art. 20), e "interceptación de datos relativos al contenido" (art. 21).

Por otra parte, el Convenio a su vez posee una serie de disposiciones relativas a la cooperación internacional y asistencia mutua, intentando crear mecanismos suficientes que permitan combatir los delitos informáticos de forma eficiente.

3. Desafíos actuales en materia de criminalidad informática

En base a todo lo expuesto, resulta evidente que en materia legislativa, el derecho penal argentino se ha nutrido de una serie de normas que resultaban necesarias para combatir la ciberdelincuencia.

Sin embargo, el proceso de desarrollo de la tecnología va permitiendo la aparición de nuevas y disvaliosas conductas que merecen la atención, una vez mas, del aparato legislativo para la sanción de normas que protejan a la sociedad toda de los las

mismas.

En ese marco, durante el desarrollo del trabajo se marcaron una serie de modificaciones que, a juicio del autor, debían ser consideradas próximamente, como la modificación de la ley 25.891 -de telefonía celular- o de la ley 26.904 -que incorpora la figura del *grooming*.

Aunado a ellas, una de las conductas que fue desdeñada al momento de sancionarse la ley 26.388 y que resultaría de necesaria atención, es la suplantación de identidad en los medios electrónicos.

En ese marco, es creciente la cantidad de perfiles falsos que día a día se registran en la red social, violando no sólo las normas de adhesión, sino también produciendo un uso de imágenes, nombres, y otros datos de personas de existencia real, que ven afectada, cuanto menos, su vida social.

Como dato de interés, en el año 2012 la misma red social reconoció que aproximadamente un 6 por ciento de las cuentas eran falsas, por lo que, toda vez que en aquel momento la cantidad de usuarios ascendía a 845 millones, daba una cifra nada despreciable de cincuenta millones setecientas mil cuentas falsas.

De tal forma, y más allá de la finalidad para la cuál es creada, la suplantación de identidad de personas de existencia real o jurídica, es un problema de creciente evolución.

En efecto, ya no es extraño que famosos tengan que aclarar, continuamente, que no poseen cuentas en determinadas redes sociales, ya que mediante la utilización de su imagen, su nombre y sus datos, consiguen realmente engañar al público consumidor, y en algunos casos, pueden provocarles molestias, perjuicios o simplemente, y con total derecho, no desean que otro se haga pasar por ellos.

Ante tales situaciones, las víctimas tienen la opción de recurrir ante la plataforma en la cuál se utilizan sus datos para solicitar el cese de dicha utilización, pero ante la negativa o falta de respuesta de aquellas, no existe una norma penal que ampare y penalice a su autor, si bien tendrá a la mano reclamos civiles.

Otra de las modalidades disvaliosas relacionadas con el mundo informático es el “ciberacoso” o “ciberbullyng”, del cual son víctimas tanto menores de edad como

mayores.

En ese sentido, la conducta de acoso a una persona determinada, trasciende las fronteras personales, hasta llegar a los medios electrónicos, en los que utilizando plataformas sociales como el medio para que se desarrolle el delito, se desata una creciente violencia hacia la víctima.

Ello, al trascender la esfera de "intimidad", permite que cientos, miles o millones de personas pasen a formar parte del acoso, con el trágico resultado de, en algunos casos, el suicidio del acosado.

Sin lugar a dudas, las conductas aquí descriptas son sólo algunas de las que nuestro sistema legal precisa estudiar a los efectos de dar una pronta respuesta a las necesidades sociales, tanto desde el punto de vista de fondo como procesal, a los efectos de que estas nuevas herramientas tecnológicas, que nos acompañan día a día no se transformen en elementos o medios para el despliegue de conductas perjudiciales para la sociedad

4. Conclusiones parciales

Las características mencionadas en el presente capítulo, son sólo algunas de las aristas que caracterizan a los "delitos en tecnologías", y que permiten comprender la complejidad que representa su estudio, y persecución penal.

Asimismo, la velocidad en el desarrollo de las tecnologías hace necesaria una estricta supervisión sobre los comportamientos sociales que se presentan como consecuencia de dicho avance, y en particular requieren que el estado, desde el aparato legislativo, se halle siempre alerta para prevenir, a través de la sanción de normas penales, las conductas negativas que surgen en consecuencia.

Por su lado, se hace necesaria la sanción de normas para adaptar el derecho interno a los estándares internacionales, como así también la firma de instrumentos y convenios con otros países, ya que sólo a través de una ágil colaboración internacional se podrá controlar, en forma eficiente, el fenómeno delictivo bajo estudio.

CONCLUSIÓN FINAL

A casi 80 años desde la aparición de la primer computadora y a casi 70 años desde la aparición del primer virus, la tecnología, la informática, la computación, los celulares, han crecido exponencialmente, más allá del pensamiento de cualquier analista, creador o inventor.

Tal desarrollo, trajo aparejado un sinnúmero de conductas disvaliosas, algunas de ellas quedarán como una situación negativa; otras, parte de reclamos civiles y, las mas negativas, poco a poco previstas y reprimidas por el derecho penal.

Nuestro derecho, como hemos visto, comenzó un proceso de incorporación de los medio tecnológicos al derecho penal a partir del año 1996, con la sanción de la ley 24.766.

Desde dicho hito, nuca se detuvo el análisis y desarrollo legislativo relacionado con las conductas más reprochables que aparecieron en el seno de la sociedad, relacionadas con la proliferación de las tecnologías de la información y la comunicación. Sin embargo, una deuda pendiente es que dichas modificaciones sean más espontáneas, inmediatas; mientras el poder legislativo no sancione ciertas conductas, inevitablemente habrá víctimas de este creciente fenómeno, que no tendrán la protección del derecho.

En ese sentido, nótese que la ley pilar de nuestro sistema jurídico para el combate de los delitos relacionados con las TIC´s fue sancionada siete años después de que se realizara el Convenio de Ciberdelincuencia o Ciberdelito de Budapest, en el seno del Consejo de Europa.

Asimismo, una mayor previsión permitiría evitar la sanción de normas “apuradas” (como el caso de la ley 25.891) y así evitar la continua modificación de normas penales, que dificultan la concreción del valor justicia.

Por otra parte, resulta innegable que las Tecnologías de la Información y la Comunicación continuarán desarrollándose y ampliándose, invadiendo cada uno de los aspectos de nuestras vidas.

Así como hace unos años, muchas empresas no poseían computadoras, hoy es impensable montar cualquier tipo de actividad comercial sin contar con la compañía y apoyo de la informática.

La globalización informática, así como acerca los mercados y los negocios, las personas y las familias, también acerca al delincuente con su objeto de deseo, y le facilita, en muchos casos, el medio para cometer los delitos.

En otro orden de ideas, no resulta ocioso mencionar que, así como se ha comenzado en la técnica legislativa respecto de las normas de fondo, debe ponerse atención en los modos de recolección de los medios de prueba, como así también en la responsabilidad empresarial de los entes que intervienen en el proceso de brindar servicio de internet, telefonía, etcétera.

Asimismo, a nivel mundial existen una serie de problemáticas que, en breve, deben tener la atención de los aparatos legislativos.

A modo de ejemplo, en la investigación penal cada vez más se presentan inconvenientes en la imposibilidad de intervenir los modernos medios de comunicación, como los llamados por Whatsapp, Messenger, y otros medios de comunicación, cuya intrusión estatal resulta, por el momento, imposible.

Dicho panorama, no es sólo conocido por abogados e investigadores, sino también por aquellos dedicados a la actividad delictual, que utilizan dichas falencias en su favor, complejizando la tareas de descubrir la verdad real y acercar el valor justicia.

Tales situaciones requieren de la participación de la comunidad mundial del derecho, para el establecimiento de normas internacionales que permitan el desarrollo de las tecnologías para el mejoramiento de la vida toda, minimizando los riesgos que conlleva cada una de las apariciones de nuevos modos de contacto, de la comunicación y de la información.

Bibliografía

- Azuara C. (2012) Combate a la ciberdelincuencia. Editorial: Xalapa (México).
- Belloni A. (2011) Ponencia en el marco del XI Encuentro de la Asociación Argentina de Profesores de Derecho Penal Facultad de Derecho de la Universidad Nacional de Rosario – Provincia de Santa Fé**.** *"Auspicios y concreciones de la internet. Algunas reflexiones en torno a los delitos informáticos, con especial referencia al `odio cibernético´ "*. Publicado por la Asociación Argentina de Profesores de Derecho Penal. http://www.aapdp.com.ar/intponencias.html.
- C. A. Ferraro y C. Lerch (2011). Que es que en tecnología. Buenos Aires. Ediciones Granica. Version online en google books.
- Creus, C. (1998). Derecho Penal, Parte Especial (6ta edición actualizada y ampliada). Buenos Aires, Editorial Astrea.
- Del Pino S. Delitos informáticos: generalidades. Extraido de la pagina web http://www.oas.org/juridico/spanish/ cyb_ecu_delitos_inform.pdf.
- Díaz Gómez A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", *REDUR* 8, diciembre 2010, págs. 169-203. ISSN 1695-078X. Visitado en http://www.unirioja.es/dptos/dd/redur/numero8/ diaz.pdf.
- Donna, E. (2001) Derecho Penal, Parte Especial. Buenos Aires, Rubinzal - Culzoni Editores, Tomos I a IV.
- Figari, R.E. (2009). "Daño informático arts. 183, 2º párr. y 184 incs. 5º y 6º del C.P. Ley 26.388". Publicado en Infojus: http://www.infojus.gob.ar/doctrina/dacf100072-figari-dano_informatico_arts_183.
- Gamba S., (2010) *No groomiarás - Otro entusiasta aporte al expansionismo penal*. ElDial.com-DC150D.
- Garibaldi, G.E.L. (2010) Las modernas tecnologías de contro de

investigación del delito. Buenos Aires, editorial: Ad Hoc.

- Lo Giudice, M.E. (2013) *Con motivo de la sanción de la ley que introduce el "delito de grooming" en el Código Penal*. elDial.com - DC1C0B.

- Martino, Antonio A., "*E-commerce* y derecho hoy. La experiencia de la Comunidad Europea", Ecomder 2000, I Congreso Internacional por Internet sobre Aspectos Jurídicos del Comercio Electrónico, Facultad de Derecho, UBA.

- Migliorisi, D.F. (2014) Crimenes en la web- los delitos del siglo XXI, Editorial: Del nuevo extremo.

- Molina Q., Eduardo (2014) Responsabilidad de los buscadores de internet. ABELEDO PERROT Nº: AP/DOC/4240/2012.

- Oficina de las Naciones Unidas contra la Droga y el Delito (2010) *Evaluación de la amenaza de la delincuencia organizada transnacional.* extraído de https://www.unodc.org/documents/data-and-analysis/tocta/ Globalization _ of_Crime-ExSum-Spanish.pdf.

- Palacios M. (2011) Ponencia en el marco del XI Encuentro de la Asociación Argentina de Profesores de Derecho Penal Facultad de Derecho de la Universidad Nacional de Rosario – Provincia de Santa Fé**.** "El derecho a la intimidad ante la expansion de las redes sociales en internet: un desafio juridico*"*. Publicado por la Asociación Argentina de Profesores de Derecho Penal. http://www.aapdp.com.ar/ intponencias.html.

- Palazzi, P.A. (2012) Los delitos informáticos en el Código Penal (segunda edición). Buenos Aires, editorial: Abeledo Perrot.

- Palazzi P.A. (2000) Delitos Informáticos. Buenos Aires, editorial: Ad Hoc.

- Palazzi P. (2004) Internet: su problemática jurídica. SJA 15/12/2004 ; JA 2004-IV-1466.

- Pescelvi, S.M. (2015) Grooming - Una figura a modificar en el código penal. elDial.com - DC1F41.

- Pont Vergues, F. y Brolese, F., (2009). *Delitos informáticos, principio*

de legalidad y sucesión de leyes (comentario al fallo "Ventura" de la Cámara Nacional de Casación Penal Sala I). Publicado elDial.com - DC103D.

- Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP) (2014). "Informática y delito".
- Riquert M. Transcripción de la conferencia "*Informática y derecho penal: ¿entre el control social y el delito?"* Publicado por la Asociación Argentina de Profesores de Derecho Penal.
- Riquert M. (2014) *Algo más sobre la legislación contra la delincuencia informática en MERCOSUR a propósito de la modificación al Código penal argentino por ley 26388*. Centro de Investigación Interdisciplinaria en Derecho Penal Económico.
- Riquert M. (2012) *"Apostillas al texto de la ley 26735"*. Publicación en su blog personal http://riquert-penaltributario.blogspot.com.ar/2012/02/apostillas-al-texto-de-la-ley-26735.html.
- Riquert M. (2008) "Delito de alteración dolosa de registros (art. 12 ley penal tributaria). Publicado en su blog personal http://riquert-penaltributario.blogspot.com.ar/2008/07/delito-de-alteracin-dolosa-de- registros.html.
- Rosende, E. (2008). Derecho Penal e Informática. Buenos Aires, editorial: Fabián Di Placido.
- Rosende, E. El intrusismo informático. Reflexiones sobre su inclusión al código penal. Publicado por la Asociación Argentina de Profesores de Derecho Penal (http://www.aapdp.com.ar/archivosparabajar/03 Rosende.pdf).
- Saez Capel, J (2001) Informática y delito, editorial Proa XXI
- Sueiro C. (2011) Ponencia en el marco del XI Encuentro de la Asociación Argentina de Profesores de Derecho Penal Facultad de Derecho de la Universidad Nacional de Rosario – Provincia de Santa Fé**.** "*La eficiencia de la ley 26.388 de reforma en materia de criminalidad informática al código penal de la nación"*. Publicado por la Asociación Argentina de Profesores de Derecho Penal. http://www.aapdp.com.ar/intponencias.html.

• Tobares Catalá, G.H. y Castro Argüello, M.J. (2009) *Delitos Informáticos*.

• Ulrich Sieber (1998) "Legal Aspects of Computer-Related Crime in the Information Society". Extraído de la pagina web de la Unión Europea http://www.echo.lu/legal/en/comcrime/sieber.html

• Vanossi, Jorge Reinaldo (2004) "Régimen legal aplicable a la telefonía celular. Comentarios a la sanción y al texto de la ley 25891". La Ley. AR/DOCO1592/2004.

Jurisprudencia

• Dictamen del Procurador General de la Nación y resolución de la Corte Suprema de Justicia de la Nación, Competencia N° 351. XLVIII. "Jutton, Juan Carlos si denuncia delito del la seguridad pública".

• Cámara Nacional de Casación Penal, "Autodesk Inc. s/recurso de casación". Voto de los Dres. Catucci, Madueño, Bisordi. Sala I, Resolución del: 19/07/1995.

• Cámara Nacional de Casación Penal, "Roitman s/ recurso de casación", Sala IV.

• Cámara Nacional en lo Criminal y Correccional Federal, Sala 2, 12/7/2011, "Dragonetti, Hugo Alberto v. Google Inc. s/medidas cautelares", elDial AF5E7A.

• Cámara Nacional en lo Criminal y Correccional Federal, sala 1a, 13/3/2002, "Vita, Leonardo G. y González Eggers, Matías s/procesamiento", elDial AA1B16.

• Causa n° 46.744 "Fiscal s/ apela declaración de nulidad de informe pericial", Jdo. Fed. N°7, Sec. N°14, Reg. N° 458.

• Cámara de Apelaciones en lo Penal, Contravencional y de Faltas, Causa Nro. 16056-00-00/2012 "N.N. s/inf. art. 183 CP".

Legislación Nacional

- Código Penal de la Nación. Ley 11179 (1921).
- Código Penal, su modificación, Ley 25.930 (2004).
- Código Penal, modificación, Ley 26.388 (2008).
- Código Penal, modificación, Ley 26.904 (2013).
- Código Procesal Penal de la Nación. Ley 23.984 (1991).
- Ley de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente, Ley 24.766 (1996).
- Ley de firma digital, ley 25.506 (2001).
- Ley de inteligencia, 25.520 (2001).
- Propiedad Intelectual, ley 25.036 (1998).
- Protección de datos personales, ley 25.326 (2000).
- Régimen penal tributario, ley 24.769 (1997).

Legislación internacional

- Alemania: Segunda Ley contra la Criminalidad Económica, 1986
- Chile: Ley de delitos informáticos. (1993)
- Convenio de Budapest sobre la Ciberdelincuencia
- España: Ley Orgánica de Protección de Datos de Carácter Personal (1999) España
- Estados Unidos: ley Federal de Protección de Sistemas de 1985.
- Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030).

UNIVERSIDAD SIGLO 21

ANEXO E – FORMULARIO DESCRIPTIVO DEL TRABAJO FINAL DE GRADUACIÓN

AUTORIZACIÓN PARA PUBLICAR Y DIFUNDIR TESIS DE POSGRADO O GRADO A LA UNIVERIDAD SIGLO 21

Por la presente, autorizo a la Universidad Siglo21 a difundir en su página web o bien a través de su campus virtual mi trabajo de Tesis según los datos que detallo a continuación, a los fines que la misma pueda ser leída por los visitantes de dicha página web y/o el cuerpo docente y/o alumnos de la Institución:

Autor-tesista *(apellido/s y nombre/s completos)*	Yair Turnes
DNI *(del autor-tesista)*	30494716
Título y subtítulo *(completos de la Tesis)*	Delitos Informáticos. Especial atención a las leyes 26.388 y 26.904.
Correo electrónico *(del autor-tesista)*	yayo.turnes@gmail.com
Unidad Académica *(donde se presentó la obra)*	Universidad Siglo 21
Datos de edición: *Lugar, editor, fecha e ISBN (para el caso de tesis ya publicadas), depósito en el Registro Nacional de Propiedad Intelectual y autorización de la Editorial (en el caso que corresponda).*	

Otorgo expreso consentimiento para que la copia electrónica de mi Tesis sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21 según el siguiente detalle:

Texto completo de la Tesis *(Marcar SI/NO)*[1]	Si
Publicación parcial *(Informar que capítulos se publicarán)*	

Otorgo expreso consentimiento para que la versión electrónica de este libro sea publicada en la en la página web y/o el campus virtual de la Universidad Siglo 21.

Lugar y fecha: _____

Firma autor-tesista **Aclaración autor-tesista**

Esta Secretaría/Departamento de Grado/Posgrado de la Unidad Académica: _____certifica que la tesis adjunta es la aprobada y registrada en esta dependencia.

Firma Autoridad Aclaración Autoridad

Sello de la Secretaría/Departamento de Posgrado

[1] Advertencia: Se informa al autor/tesista que es conveniente publicar en la Biblioteca Digital las obras intelectuales editadas e inscriptas en el INPI para asegurar la plena protección de sus derechos intelectuales (Ley 11.723) y propiedad industrial (Ley 22.362 y Dec. 6673/63. Se recomienda la NO publicación de aquellas tesis que desarrollan un invento patentable, modelo de utilidad y diseño industrial que no ha sido registrado en el INPI, a los fines de preservar la novedad de la creación.