DELITOS INFORMÁTICOS

ÍNDICE GENERAL

arielceresole@gmail.com
sergiooyarzabal@gmail.com

PRÓLOGO

El tema fue seleccionado en virtud de la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones; sumado al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica "Delitos Informáticos".

También nos interesó saber que tan bien preparada está nuestra justicia ante el novedoso fenómeno y con que medios cuenta a la hora de hacerle frente.

Agradecemos a quienes de una u otra manera contribuyeron a este trabajo de investigación: a los jueces de primera y segunda instancia e integrantes del Ministerio Publico de la Acusación y Defensa, fiscales entrevistados y en especial al Dr. Hugo Degiovanni quien, amén del tiempo cedido para la entrevista, tuvo la amabilidad de facilitarnos material que nos ha sido de suma utilidad.

Por último, antes de comenzar a desarrollar la investigación quiero, con aprobación de mi compañero, dedicar la misma a Julio Ceresole:
Mi padre, mi mentor, mi maestro, mi consejero, mi ídolo, el líder de mi familia, el mejor amigo de mi madre y por mucho el hombre más increíble que he conocido.
Te extrañamos todos los días, pero mientras recorremos el camino siempre intentaremos que te sientas orgulloso de cada paso que demos.

INTRODUCCIÓN

A modo introductorio al tema podemos decir que a lo largo de la historia el hombre, ante la necesidad de comunicarse, transmitir y tratar información, ha elaborado diferentes sistemas a tales fines que van desde las señales de humo, código morse, teléfono hasta llegar a la informática que es la ciencia encargada del estudio y desarrollo de máquinas para, al menos inicialmente ayudar al hombre con trabajos rutinarios y repetitivos; con el tiempo se fue diversificando su uso.
Luego nace Internet como tecnología que pondría cultura, ciencia e información al alcance de millones de personas en todo el mundo. Si bien este adelanto tiene innumerables ventajas de las que muchos usuarios y empresas han logrado extraer importantes beneficios, también abre las puertas a conductas antisociales y delictivas ofreciendo oportunidades nuevas y complejas de infringir la ley. Un cambio social ha operado en las últimas décadas, que resulta íntimamente vinculado a la evolución tecnológica operada en ese transcurso de tiempo, generándose problemas para la protección de intereses sociales no convencionales y para la represión de las conductas delictivas realizadas a través de medios no convencionales, en este contexto debe de tenerse en cuenta que el impacto de la explosión tecnológica es un problema de política criminal que se conoce sobradamente. La técnica siempre es un arma y cada avance fue explotado criminalmente, en forma tal que siempre el criminal está más tecnificado que la prevención del crimen, lo que resulta más dramático en las sociedades informatizadas, en la medida que éstas resulten tecnológicamente vulnerables.[1] En base a esto surge la pregunta en la que se centra nuestro trabajo:

¿Cuáles son los medios jurídicos usados por el fuero penal del distrito Judicial Nº 10 (Rafaela) 5ta Circunscripción de la Provincia de Santa Fe para esclarecer el delito informático?

El **objetivo** de esta investigación es determinar de qué manera la problemática del delito informático se afronta en el distrito judicial de Rafaela. Esto nos permitirá comprender si la justicia local cuenta con herramientas suficientes para hacer frente a una actividad delictiva que en principio podría suponerse es de compleja investigación. En nuestro sistema jurídico denominado continental romanista, que tiene como antecedente directo el sistema jurídico de los códigos napoleónicos, la principal fuente del derecho es la ley, no la jurisprudencia o la costumbre jurídica como es en el sistema anglosajón. Si bien esto se puede interpretar como una ventaja al momento de resolver conflictos pues la norma solo se modifica con otra norma, presenta dificultad en cuanto a la adaptación del derecho a la dinámica de la realidad cotidiana cuyos cambios están siempre varios pasos por delante del derecho.

[1] REYNA ALFARO, LUIS MIGUEL. "Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal", JURISTA Editores E.I.R.L. Lima, 2002. pág.125

CAPÍTULO I: MARCO TEÓRICO

Para llevar adelante esta investigación es necesario definir los siguientes constructos teóricos:
En primer término hemos de especificar que es un delito: toda acción típica, antijurídica y culpable[2]. Hablamos de acción haciendo referencia a toda conducta humana exteriorizada evitable[3]; el carácter de típico se lo da el hecho de estar descripta en una norma[4]; será antijurídica cuando sea contraria al derecho en su totalidad[5] y se entenderá culpable cuando el sujeto que realizo la conducta pudo comprender la criminalidad del acto y dirigir sus acciones al momento del hecho[6].

Establecido que es delito, pasamos a decir que, a grandes rasgos, el delito informático es aquel que se vale de medios informáticos para vulnerar algún bien jurídico tutelado, pudiendo hacerlo mediante:

Acciones que inciden sobre el software y hardware de una pc.
Acciones en que la pc es usada como instrumento para perpetrar un delito.
Acciones en que se utiliza hardware o software sin autorización debida.[7]

El Dr. Terragni ha definido al delito informático como "toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y esté sancionado con una pena".[8]

Siguiendo estudios realizados en base al libro de Derecho Informático de Julio Tellez[9] podemos sostener que los delitos infomáticos poseen las siguientes características:

- Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

[2] MONSERRAT A., Guía de estudio de derecho pena,l parte general, Capitulo VI, Ed. Estudio S.A, Buenos Aires, año 2011, pp. 99-101.
[3] BACIGALUPO, ENRIQUE, Teoría de los lineamientos del delito, ed. Hammurabi, Buenos Aires, año 1994, p. 15.
[4] LASCANO, CARLOS, Derecho penal parte general, CapituloVIII , ed. Advocatus, Córdoba, año 2002, p. 453
[5] MONSERRAT, op. cit. p. 129.
[6] LASCANO, op. Cit p. 200.
[7] GAMBOA, WALTER, Power Point sobre Cibercriminalidad
[8] http://www.terragnijurista.com.ar/doctrina/informaticos.htm fecha de ingreso 05/08/2014
[9] www.terragnijurista.com.ar/doctrina/informaticos.htm fecha de ingreso 05/08/2014

- Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

.

- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

- Ofrecen facilidades para su comisión a los menores de edad.

- Tienden a proliferar cada vez más.

A la hora de hablar de los sujetos, en primer término tenemos que distinguir que el sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos", mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.
Ha sido imposible conocer la verdadera magnitud de los "Delitos Informáticos" ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables; que sumado al temor de las empresas de denunciar este tipo de ilícitos por el desprestigio y su consecuente pérdida económica que esto pudiera ocasionar, hace que éste tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".[10]

En cuanto al sujeto activo podemos afirmar que las personas que cometen delitos informáticos difieren de los delincuentes comunes, ya que requieren habilidades para el manejo de sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible o son hábiles en el uso de sistemas informatizados. Los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, por ello estudiosos en la materia han catalogado a este tipo de delito como “delito de cuello blanco”, término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año 1943.[11]

[10] http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml fecha de ingreso 10/08/2014
[11] http://www.terragnijurista.com.ar/doctrina/informaticos.htm fecha de ingreso 12/08/2014

A modo de clasificación podríamos dividir a los delítos informáticos en los siguientes grandes grupos:

- ***Fraudes cometidos mediante manipulación de computadoras:*** Estos pueden suceder en el interior de Instituciones Bancarias o cualquier empresa en su nómina, ya que la gente de sistemas puede acceder a variados tipos de registros y programas.

- ***Reproducción no autorizada de programas informáticos de protección Legal:*** Es la copia indiscriminada de programas con licencias de uso para copias de una sola persona, se le conoce también como piratería.

- ***La manipulación de programas:*** Mediante el uso de programas auxiliares que pemitan estar manejando los distintos programas que se tiene en los departamentos de cualquier organización.

- ***Manipulación de los datos de salida:*** Cuando se alteran los datos que salieron como resultado de la ejecución de una operación establecida en un equipo de cómputo.

- ***Fraude efectuado por manipulación informática:*** Accesando a los programas establecidos en un sistema de información, y manipulandolos para obtener una ganancia monetaria.

- ***Falsificaciones Informáticas:*** Manipulando información arrojada por una operación de consulta en una base de datos.

- ***Sabotaje informático:*** Cuando se establece una operación nociva tanto de programas de cómputo, como un suministro de electricidad o cortar lineas telefónicas intencionalmente.

- ***Virus:*** Pequeños programas de computadora que tienen la capacidad de autoduplicarse y parasitar otros programas. Una vez difundidos, los virus se activan bajo determinadas circunstancias y en general, provocan algún daño o molestia.
  El virus informático tiene tres características principales: produce daño, es autorreproductor y es subrepticio u oculto.[12]

- ***Gusanos***: Es un programa similar al virus, pero que a diferencia de éste no requiere infectar a otro programa, ya que se difunde en forma autónoma de computadora a computadora.

[12] http://www.delitosinformaticos.com/delitos/delitosinformaticos3.shtml fecha de ingreso 01/09/2014

- ***Bomba lógica o cronológica:*** Su funcionamiento es muy simple, es una especie de virus que se programa para que explote en un día deterrminado causando daños a el equipo de cómputo afectado.

- ***Piratas Informáticos:*** Hackers y Crackers dispuestos a conseguir todo lo que se les ofrezca en la red, tienen gran conocimiento de las técnicas de cómputo y pueden causar graves daños a las empresas.

- ***Acceso no autorizado a Sistemas o Servicios:*** Penetrar indiscriminadamente en todo lugar sin tener acceso a ese sitio.

- ***Reproducción de material inapropiado o contrario a las buenas costumbres:*** Conducta que abarca tanto la pornografía, pedofilia, discriminación, violencia explícita, odio racial, etc. por vías informáticas.

REGULACIÓN LEGAL INTERNACIONAL

En cuanto a la regulación legal del fenómento en estudio, existe un convenio a nivel internacional: Convenio de Ciberdelincuencia del Consejo de Europa.

El **Convenio sobre Cibercriminalidad**, también conocido como el Convenio de Budapest sobre el Cibercrimen o simplemente como Convenio de Budapest, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Japón y China.

El 1 de marzo de 2006, el Protocolo Adicional a la Convención sobre Cibercriminal entró en vigor. Los estados que han ratificado el Protocolo Adicional consideran necesario penalizar la difusión de propaganda así como de las amenazas racistas y xenófobas e insultos a través de los sistemas informáticos.

El Convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. También contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la interceptación ilegal.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercriminal, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Los principales objetivos de este tratado son los siguientes:

1. La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones, conectados al área de los delitos informáticos.

2. La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.

3. Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

Los siguientes delitos están definidos por el Convenio: acceso ilícito, interceptación ilegal, la interferencia de datos, la interferencia del sistema, mal uso de los dispositivos, la falsificación informática, el fraude relacionado con la informática, los delitos relacionados con la pornografía infantil y los delitos relacionados con los derechos de autor y derechos conexos.

El Convenio es el resultado de cuatro años de trabajo de expertos europeos e internacionales. Se complementa con un Protocolo Adicional que repudia cualquier publicación de la propaganda racista y xenófoba a través de redes informáticas como una ofensa criminal. En la actualidad, el terrorismo cibernético también se estudia en el marco del Convenio.

El Convenio de Budapest y el Mercosur.

Luego de que, en noviembre de 1996, el Comité Europeo sobre problemas penales creó un comité de expertos para trabajar el fenómeno de la delincuencia asociada a la tecnología; el Consejo de Europa impulso y abrió la firma del conocido Convenio sobre Cibercriminalidad, en su reunión celebrada en la ciudad de Budapest el 23 de noviembre de 2001.

Dicho convenio está en vigor desde el 1º de julio de 2004, con un protocolo adicional del 28 de enero de 2003 sobre la lucha contra el racismo y la xenofobia por Internet.

Para Oscar Morales García, fue el proyecto legislativo más ambicioso en la materia. Además, afirma que, por atemperar alguna de sus propuestas originales durante la revisión de los borradores, han terminado plasmando "una Convención político criminalmente aceptable"[13]

[13] MORALES GARCIA, OSCAR, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre Cibercrimen", en AAVV, Delincuencia Informática. problemas de responsabilidad, Cuadernos de Derecho Judicial IX-2002 Consejo General del Poder Judicial, Madrid, 2002, p.195

Justamente por la búsqueda de consensos entre los Estados que participaron en su confección, Rovira del Canto dijo que se trataba de una "Convención de mínimos".[14] Si bien es una iniciativa de la Unión Europea ha sido firmado por numerosos países extracomunitarios, como Estados Unidos o Japón. Argentina adhirió en 2010.[15] Además, dentro del margen latinoamericano se encuentran Costa Rica, República Dominicana, México y Chile.

Compartimos la concepción sobre el Consejo de Europa hecha por Walter Perrón en tanto organización de derecho internacional que, claramente, tiene un alcance que va más allá de los Estados miembros de la Unión Europea, cuyo núcleo está expuesto en la Convención Europea sobre derechos humanos. El Consejo no tiene facultades soberanas propias sino que su objeto es influir en el desarrollo de los Estados miembros a través de recomendaciones y tratados. Su instrumento más importante es el Tribunal Europeo de Derechos Humanos (TEDH), cuya jurisprudencia es de superlativa importancia y ante el que todo ciudadano de un estado miembro puede comparecer en el marco de una petición individual. El nombrado individualiza precisamente como el segundo sector más importante las numerosas convenciones respecto de distintos aspectos del derecho penal y procesal penal; tales como las relativas a extradición, asistencia jurídica recíproca, lucha contra el terrorismo o un variado conjunto de delitos conglomerados bajo la designación de "criminalidad organizada" -lavado, tráfico de drogas, financiamiento del terrorismo- y otros que sólo pueden ser protegidos a nivel transnacional -corrupción pública y privada, protección del medio ambiente, tráfico ilegal de personas, explotación sexual de niños, insider trading, manipulaciones del mercado y delitos informáticos-.[16]

Por eso en su trabajo "Delincuencia informática y control social: ¿excusa o consecuencia?" Riquert Marcelo señala que el citado Convenio se ha constituido en una referencia insoslayable en términos de armonización legislativa en la materia[17] y que la normativa Argentina no tiene al presente mayor problema de compatibilidad con los estándares mínimos que aquel reclama en lo referente al derecho penal sustancial. Mientras que en lo adjetivo o formal es donde puede advertirse algún déficit de mayor significación. No se trata de un problema exclusivo de nuestro país, sino que, como advierte Marcos Salt se trata de un rasgo extendido a toda la legislación latinoamericana. Pues sus previsiones procesales han sido diseñadas pensando en la evidencia física y no en la digital. En muchos casos los problemas que se presentan terminan siendo solucionados por vía

[14] ROVIRA CANTO, ENRIQUE, ciberdelincuencia intrusiva hacking y grooming en línea http://www.iaitg.eu/mediapool/67/67026/data/Ciberdelincuencia_intrusivas_hacking_y_grooming_Enrique_Rovira.pdf
[15] CHERÑASKY, NORA, "El delito Informatico" en XI Encuentro de Profesores de Derecho Penal de la República Argentina. Buenos Aires, La Ley/UBA/AAPDP, 2013, p. 288
[16] PERRON, WALTER, "Perspectivas de la unificación del derecho penal y del derecho procesal en el marco de la Unión Europea", en AAVV, Estudios sobre la Justicia Penal. Homenaje al profesor Julio b.j Maier, Buenos Aires, Editores del Puerto, 2005, pp. 734/735 y 737/738.
[17] RIQUERT, MARCELO, "Delincuencia informática y control social: excusa y consecuencia?" en Revista Jurídica Facultad de Derecho de la UNMDP, nº6, 2011 pp.67/99

jurisprudencial aplicando analógicamente criterios y reglas de las pruebas físicas. El retraso en la adopción de reformas procesales respecto de las modificaciones en el derecho penal material se verifica también en otras regiones -Alemania Portugal y España-.[18]

La situación de nuestra región es curiosa. Con la adopción de modernos códigos de corte acusatorio, se ha producido una masiva transformación de los sistemas procesales en los últimos quince años. Sin embargo, ha dejado sin mayores variaciones los artículos dedicados a la prueba, que permanecen con una semejanza notable a los viejos digestos inquisitivo o mixtos.

Hecha la aclaración recordamos que, para fundar la necesidad de provocar aquella armonización, desde hace tiempo se hace hincapié en que las fronteras nacionales constituyen un obstáculo evidente para la detección, investigación, persecución y castigo de los autores de delitos perpetrados mediante el uso de nuevas tecnologías de información y comunicación (TIC). En cambio, Internet está configurada como un espacio sin fronteras para aquellos. Hay una ineludible dimensión supranacional y para afrontarla es claro que la vía más conveniente no es la antigua cooperación bilateral; sino el impulso de esfuerzos de armonización regional mediante convenios multilaterales, como el que ahora nos ocupa.[19]

Además, como resalta Lezertua, la armonización sustantiva es un elemento indispensable pero no suficiente para llevar a cabo un combate eficaz contra la ciberdelincuencia. Debe ser acompañada por otro relativo a los instrumentos apropiados para detectar, investigar, procesar y castigar a los autores estas infracciones.[20]

Jasky y Lombaert destacan que la Comisión Europea en su comunicación "Hacia una estrategia general en la lucha contra la ciberdelincuencia", distingue una tercer área de actividades principales en la elaboración de una estrategia europea coherente para luchar contra la ciberdelincuencia en cooperación con los Estados miembros de la Unión Europea; tanto con las instituciones de la región como las internacionales. Señalan además que la legislación y la ejecución de la ley a nivel transfronterizo debe articularse con la colaboración de los sectores público y privado.[21] Cherñavsky ha destacado la experiencia adquirida por Europol en la coordinación de programas sobre cibercrimen, de respuesta y estrategias, incluso respecto de la lucha contra el terrorismo. A su vez destacó la necesidad de que Argentina desarrolle esa experticia en

[18] SALT, MARCOS, "disposiciones Código de Procedimiento Penal sobre el delito cibernético en América Latina en cuanto a su cumplimiento de la Convención de Budapest (Argentina, Chile, Colombia, Costa Rica, México, Paraguay y Perú)", Estamburgo, Consejo de Europa, 12 de abril de 2011, p.4
[19] GOMEZ DIAZ, ANDRES, "El delito informático su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest" en Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR), p. 183
[20] LEZERTUA, MANUEL, "el proyecto de Convenio sobre el Cibercrimen del Consejo de Europa" Cuadernos de Derecho Judicial X-2001. Consejo General del Poder Judicial, Madrid, 2001, p.25
[21] RADOMIR JASKY Y RUBEN LOMBAERT "Hacia una estrategia europea unificada para combatir la ciberdelincuencia", E) NAC. E-newsletter. En la lucha contra el cibercrimen n* 4 octubre de 2009, p. 39

cooperación internacional y con el intercambio de información tanto en contra del cibercrimen, como de los delitos financieros, del lavado de dinero y el terrorismo.[22]

Debe tenerse presente que en el convenio no se proporciona una definición general de "Delito Informático", "Ciberdelito" o de "Cibercrimen".

En los cuatro primeros títulos se enumera una serie de comportamientos -en total nueve, que tienen una o varias conductas, siempre "intencionales" para la tradición anglosajona, o "dolosas" para el modelo dogmático europeo-continental- a la que los estados son exhortados a considerar como infracciones penales de su legislación interna.

No se trata, entonces, de la provisión de una redacción tipo de delitos, cual suerte de receta inalterable, sino de una formulación genérica, abierta y, en algunos casos, con alternativas y los signatarios puedan adaptar conforme a su propio diseño de derecho local. Esta característica, lógica y apropiada para una suerte de convenio-marco, dificulta el cotejo con la normativa nacional; ya que dentro del universo de casos en consideración hay legislación pre convenio y post convenio de países que lo han firmado y otros que no, que han realizado una tipificación más amplia o más estricta y, a la vez, que lo hicieron en forma más concentrada o más dispersa en un doble sentido:

a) en cuanto a la adopción de una ley especial o un capítulo específico en su Código Penal, o en alternadas modificaciones en leyes especiales y el propio Código, o difuminada o sectorizada dentro del último;

b) en cuanto el Convenio, brinda en algún artículo una serie de verbos típicos para los que no hay una sola norma nacional que los reciba juntos, sino que puede hacerlo desperdigados entre diferentes tipicidades o, incluso sólo parcialmente.

Es esencial no perder de vista este factor; porque, al concretar la comparación tendiente a establecer asertiva o negativamente en la recepción de una propuesta en nivel nacional, en ocasiones, se improvisa una respuesta que sería aproximada. Es decir, puede darse el caso de que, sin haber correspondencia precisa, aún con algún déficit menor de tipicidad; no pueda sostenerse la absoluta laguna de punibilidad local y, por eso, se entienda que existe cumplimiento con el requerimiento externo, aunque sea parcial.

Tampoco en el convenio se indica o sugiere en cada caso algún tipo de sanción concreta. En el artículo 13, en forma general, se habla de la respuesta penal de personas físicas y jurídicas. Esta debe ser efectiva proporcionada y disuasoria. En el caso de las personas jurídicas, puede tratarse tanto de sanciones penales como civiles o administrativas; dentro de las penas pueden incluirse las pecuniarias, en cambio, en el caso de las personas físicas, pueden incluirse las penas privativas de libertad.

[22] CHERÑASKY, op. cit., p.288

Sin ahondar demasiado, a continuación, daremos un pantallazo de como tratan la temática los países que componen el mercosur en particular[23]:

BOLIVIA

La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". Dentro de este capítulo, se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos.

BRASIL

La Ley 12.737 es una ley reciente (año 2012), en la cuál se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet.

CHILE

La Ley 19.223 es una ley “Relativa a Delitos Informáticos” de acuerdo a su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos. La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación.

COLOMBIA

La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos”. Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cuál regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general “si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos”.

[23] http://www.asegurarte.com.ar/material/CONAIISI_Temperini_Camera_Ready.pdf fecha de ingreso 04/09/2014

ECUADOR

La Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "DE LAS INFRACCIONES INFORMÁTICAS", el art. 57 afirma que "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley." En artículo siguiente, agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos.

PARAGUAY

No se ha encontrado legislación especial referida a la materia. Sin embargo, a partir de distintas reformas al Código Penal Paraguayo, se han adaptado algunos delitos para la posibilidad de comisión a través de las nuevas tecnologías y en otros casos se ha incorporado tipos penales específicos (como el caso del art. 175 de Sabotaje de Computadoras). Los artículos son 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249.

PERU

La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos 207 – A – B y C y 208. En otro orden, la Ley 28.251 actualizó e incorporó distintos delitos contra la integridad sexual, entre ellos, tipificando la pornografía infantil, a través de la modificación del art 183-A. Además Perú posee la Ley 28.493 (2005) que regula el uso del correo electrónico no solicitado (spam), sin embargo en la misma no incluye ningún tipo de sanción penal.

URUGUAY

Si bien no se ha encontrado legislación especial en la materia, se han encontrado diferentes normativas parcialmente aplicables a la materia. El art. 7 de la Ley 17.815, afirma que “constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales.”, permitiendo así la aplicación de los tipos clásicos del CP. La Ley N° 17.520, penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados. La Ley Nº 17.815 regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación.

VENEZUELA

Posee una ley especial sobre Delitos Informáticos. Contiene 33 artículos y están clasificados en 5 Capítulos a saber: Contra sistemas
que utilizan TI; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico.

En principio, puede decirse que Argentina, Paraguay y Venezuela no ofrecerían déficit de tipificación alguno en confronte con las demandas de Budapest. En otro extremo Bolivia y Uruguay serían los estados que necesitarían una urgente actualización para entrar en sintonía armónica con los restantes. Aunque en ambos hay proyectos de reforma, en consideración actualmente.

Como primera observación, es dable concluir que la región del Mercosur no ofrece mayores problemas para su integración con los restantes signatarios del Convenio Europeo en materia de derecho penal material.

CONVENIO DE BUDAPEST Y MERCOSUR: LEGISLACIÓN COMPARADA[24]

Budapest	Art. 2	Art. 3	Art. 4	Art. 5	Art. 6	Art. 7	Art. 8	Art. 9	Art. 10
Argentina	sí	sí	sí	sí	sí	sí	sí	sí	sí
Bolivia	sí	no	sí	no	no	no	sí	no	sí
Brasil	no	sí	sí	sí	sí	sí	no	sí	sí
Chile	no	sí	sí	no	no	sí	sí	sí	sí
Colombia	sí	sí	sí	sí	sí	no	sí	sí	sí
Ecuador	sí	sí	sí	sí	no	no	sí	sí	sí
Paraguay	sí	sí	sí	sí	sí	sí	sí	sí	sí
Perú	sí	sí	sí	sí	sí	no	sí	sí	sí
Uruguay	no	sí	no	no	no	sí	no	sí	sí
Venezuela	sí	sí	sí	sí	sí	sí	sí	sí	sí

Referencias: Art. 2: Acceso ilícito; Art. 3: Interceptación Ilícita; Art. 4: Atentados contra la integridad de los datos; Art. 5: Atentados contra la integridad del sistema; Art. 6: Abuso de equipos e instrumentos técnicos; Art. 7: Falsedad informática; Art. 8: Estafa Informática; Art. 9: Infracciones relativas a pornografía infantil; Art. 10: Infracciones vinculadas a atentados contra la propiedad intelectual y derechos afines.

Con relación a la forma en que se penan las infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos -Título 1-, si bien resulta clara la uniformidad en cuanto al uso de la pena privativa de la libertad como principal modo de respuesta; puede advertirse rápidamente la diversidad con que en general se recibe el genérico mandato del artículo 13: las sanciones han de ser "efectivas proporcionadas y disuasorias" habida cuenta las disímiles escalas combinadas en abstracto, así como las variantes en alternatividad o conjunción con otras modalidades de penas. Como observaciones particulares podríamos expresar:

[24] ALAGIA, ALEJANDRO; DE LUCA, JAVIER y SLOKAR, ALEJANDRO, Revista de Derecho Penal Nº7, Ministerio de Justicia y Derechos Humanos de la Nación, Editorial Infojus, Buenos Aires, 2014, p.174

1) Acceso ilícito (art. 2): Bolivia es el único que no admite pena privativa de libertad. En cambio, prevé penas de prestación de trabajo común. Todos los demás contemplan pena privativa de libertad. Argentina es el único que la prevé en forma exclusiva. Paraguay admite la posibilidad alternativa de multa. Perú admitía la alternativa de prestación de servicios comunitarios, pero con la Ley 30.096 de octubre de 2013 ahora mantiene la pena privativa de libertad y días multa como sanción conjunta. Finalmente; Colombia, Ecuador y Venezuela prevén aplicación conjunta de prisión y multa.

2) Interceptación ilícita (art 3): en este caso todos contemplan pena privativa de libertad. Argentina, Chile, Colombia, Perú y Uruguay de forma exclusiva. Paraguay admite la posibilidad alternativa de multa. En cambio Brasil, Ecuador y Venezuela preveen aplicación conjunta de prisión y multa.

3) Atentados contra la integridad de los datos (art 4): nuevamente Bolivia es el único que no admite pena privativa de libertad sino que prevé las de prestación de trabajo o multa. Los demás contemplan la pena privativa de libertad. Argentina y Chile de forma exclusiva. Paraguay admite la posibilidad alternativa de multa. Brasil, en algunos tipos, admite la multa conjunta y, en otros, alternativa. Por último, Colombia, Ecuador Perú y Venezuela prevén la aplicación conjunta de prisión y multa.

4) Atentados contra la integridad del sistema (art 5): respecto de esta conducta, todos contemplan pena privativa de libertad. Argentina lo hace de forma exclusiva, mientras que Paraguay admite la posibilidad alternativa de multa. Por su lado, Brasil, Colombia, Ecuador, Perú y Venezuela prevén aplicación conjunta de multa y prisión.

5) Abuso de equipos e instrumentos técnicos (art 6): nuevamente todos prevén como sanción la pena privativa de libertad, Argentina es el único que lo hace en forma exclusiva y Paraguay admite la posibilidad alternativa de multa. Brasil, Colombia, Perú y Venezuela prevén la aplicación conjunta de prisión y multa.

Lo expuesto se sintetiza gráficamente en el cuadro que sigue:

PENASCONTRAINFRACCIONES.ARTS.2a6[25]

Budapest	Art. 2	Art.3	Art.4	Art.5	Art.6
Argentina	P 15D a 2A	P 15D a 1A	P 15D a 6A	P 15D a 2A	P 15D a 1A
Bolivia	PT hasta 1A o M hasta 200D	no	PT hasta1A o M hasta 200D	no	no
Brasil	no	P 2 a 4A y M	P 1 a 12A y/o M	P 1Me a 3A y M	P 3 Me a 4A y M
Chile	no	P menor grado min. a medio	P menor grado min. a máximo	no	no
Colombia	P 48 a 96 Me y M 100 a 1000S	P 36 a 72Me	P 48 a 96 Me y M 100 a 1000S	P 48 a 96 Me y M 100 a 1000S	P 48 a 96 Me y M 100 a 1000S
Ecuador	P 1 a 3A y M 1000 a 1500 u$s	P 2Me a 9A y M 1000 a 10000 u$s	P 6Me a 6A y M 60 a 600 u$s	P 8Me a 4A y M 200 a 600 u$s	no
Paraguay	P hasta 3A o M	P hasta 3A o M	P hasta 5A o M	P hasta 5A o M	P hasta 1A o M
Peru	P 1 a 4A y 30 a 90 DM	P 3A hasta 10A	P3 a 6A y 80 a 120 DM	P3 a 6A y 80 a 120 DM	P 1 a 4A y 20 a 60 DM
Uruguay	no	P 3M a3A	no	no	no
Venezuela	P 1 a 5A y M 10 a 15 UT	P 3 a 6A y M 300 a 600UT	P 2 a 10A y M 200 a 1000 UT	P 2 a 10A y M 200 a 1000 UT	P 3 a 6A y M 300 a 600 UT

Aclaración: en el caso de países en los que concurren varios tipos a cubrir el pertinente artículo del Convenio de Budapest, la escala se formó con el mínimo menor y el máximo mayor posibles considerando tipos básicos y especiales y sin incluir agravantes genéricos. Tampoco se incorporaron ni considerado las muy comunes sanciones de inhabilitación cuando el hecho es cometido por un funcionario o persona encargada de custodia, o el decomiso de elementos del delito.

Referencias: Art. 2: Acceso ilícito; Art. 3: Interceptación ilícita; Art. 4: Atentados contra la integridad de datos; Art. 5: Atentados contra la integridad del sistema; Art. 6: Abusa de equipo e instrumentos técnicos.

[25] ALAGIA, ALEJANDRO; DE LUCA, JAVIER y SLOKAR, ALEJANDRO, Revista de Derecho Penal Nº7, Ministerio de Justicia y Derechos Humanos de la Nación, Editorial Infojus, Buenos Aires, 2014, p.176

Abreviaturas: P: prisión de libertad (prisión, reclusión, detención, presidio, penitenciaria); D: cantidad de días; Me: cantidad de meses; A: cantidad de años; PT: prestación de trabajo; M: multa; DM: días-multa; S: cantidad de salarios; UT: unidades tributarias.

En relación a la forma en que se penan las infracciones informáticas, de contenido o contra la propiedad intelectual y derechos afines (Títulos 2 3 y 4), se mantiene idéntica observación en cuanto a la uniformidad en el uso de la pena privativa de libertad como principal modo de respuesta y diversidad para recibir el genérico mandato del art. 13, en orden a que las sanciones han de ser "efectivas, proporcionadas y disuasorias". Sentado eso pueden destacarse las siguientes particularidades:

1) Falsedad informática (art 7) todos los países contemplan penas con prisión de libertad. Argentina, Chile y Uruguay lo prevén en forma exclusiva. Paraguay admite la posibilidad alternativa de multa. Finalmente Brasil y Venezuela prevén la aplicación conjunta de prisión y multa.

2) Estafa informática (art 8): nuevamente todos contemplan la pena privativa de libertad. Argentina y Chile en forma exclusiva; Paraguay admite la posibilidad alternativa de multa. Por último, Bolivia, Colombia, Ecuador y Venezuela prevén la aplicación conjunta de prisión y multa.

3) Infracciones relativas a la pornografía infantil (art. 9): se mantiene la nota de uso por todos de la pena privativa de libertad que, en este caso, es prevista en forma exclusiva por Argentina, Chile, Ecuador y Uruguay. Paraguay admite la posibilidad alternativa de multa. Brasil, Colombia, Perú y Venezuela prevén aplicar en conjunto prisión y multa.

4) Infracciones vinculadas a los atentados a la propiedad intelectual y derechos afines (art. 10): todos prevén la forma privativa de libertad. Argentina y Uruguay en forma exclusiva, en tanto Paraguay admite la posibilidad alternativa de multa. En cambio la aplicación conjunta de prisión y multa es la opción de Bolivia, Brasil, Chile, Colombia, Ecuador y Venezuela.

PENASCONTRAINFRACCIONES.ARTS.7a10[26]

Budapest	Art. 7	Art. 8	Art. 9	Art. 10
Argentina	P 1 a 6A	P 1Me a 6A	P 1Me a 6A	P 1Me a 6A
Bolivia	no	P 1 a 5A y M 60 a 200D	no	P 3Me a 2A y M 60 a 200D
Brasil	P 1 a 5A y M	no	P 3 a 8A y M	P 6Me a 4A y M
Chile	P menor en cualquier grado	P menor en cualquier grado	P menor en grado med. a max.	P menor grado min. y M 5 a 50 UT
Colombia	no	P 48 a 120Me y M 200 a 1500 S	P 10 a 20A y M 150 a 1500S	P 32 a 90 Me y M 26.66 a 300 S
Ecuador	no	P 6M a 5A y M de 500 a 2000 u$s	P 6 a 9A	P 3Me a 3A y M 500 a 5000 UVC
Paraguay	P hasta 5 A y M	P hasta 5 A y M	P hasta 5 A y M	P hasta 3 A y M
Peru	no	P 3 a 10A y M 60 a 140 DM	P 6 a 12A y M 120 a 365 DM	P hasta 6A y M 10 a 120 DM
Uruguay	P 3Me a 10A	no	P 6Me a 12A	P 3Me a 3A
Venezuela	P 3 a 6A y M 300 a 600 UT	P 1 a 7A y M 10 a 700 UT	P 2 a 8A y M 200 a 800 UT	P 1 a 5 años y M 100 a 500 UT

Aclaración: en el caso de países en los que concurren varios tipos a cubrir el pertinente artículo del Convenio de Budapest, la escala se formó con el mínimo menor y el máximo mayor posibles considerando tipos básicos y especiales y sin incluir agravantes genéricos. Tampoco se incorporaron ni considerado las muy comunes sanciones de inhabilitación cuando el hecho es cometido por un funcionario o persona encargada de custodia, o el decomiso de elementos del delito.

[26] ALAGIA, ALEJANDRO; DE LUCA, JAVIER y SLOKAR, ALEJANDRO, Revista de Derecho Penal Nº7, Ministerio de Justicia y Derechos Humanos de la Nación, Editorial Infojus, Buenos Aires, 2014, p.177/8

Referencias: Art. 7: Falsedad informática; Art. 8: Estafa Informática; Art. 9: Infracciones relativas a pornografía infantil; Art. 10: Infracciones vinculadas a atentados contra la propiedad intelectual y derechos afines.

Abreviaturas: P: prisión de libertad (prisión, reclusión, detención, presidio, penitenciaria); D: cantidad de días; Me: cantidad de meses; A: cantidad de años; PT: prestación de trabajo; M: multa; DM: días-multa; S: cantidad de salarios; UT: unidades tributarias UVC: unidades de valor constante.

Poco más de una década después del convenio de Budapest, comienza a surgir el interés en que las legislaciones nacionales incorporen nuevas tipicidades o refuerzen las anteriores. Por caso, en la Unión Europea la "Directiva 2013/40/UE del Parlamento y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información" respecto del robo o suplantación de identidad digital. También se propulsa la incomparación de figuras que capten con más precisión entre otras conductas disvaliosas el grooming, el ciber talking y el ciber bullying. Sería un tema para seguir pensando el fenómeno expansivo del derecho penal. Del otro lado queda sobre todo la necesidad de reflexionar acerca de la racionalidad de seguir usándolo para conductas que tienen un alto grado de aceptación y son muy extendidas socialmente, cuya dañocidad básicamente es de orden patrimonial y que, por tanto, bien pudieran ser devueltas al ámbito civil, comercial y, si se quiere mantener una cierta cuota de poder punitivo, al derecho sancionador administrativo o contravencional. Nos referimos a la actividad cuasi bagatelar de agentes como los "manteros" -como se les llama Latinoamérica- o top manta/top mochila -en España- así como el tan frecuente de intercambio de archivos online.

REGULACION LEGAL NACIONAL

Antecedentes nacionales y leyes de reforma en materia de criminalidad informática al Código Penal de la Nación.

La comunidad jurídica Argentina se interrogó tempranamente por el dictado y sanción de una ley que previera la protección de bienes intangibles y la posible comisión de conductas típicas a través del empleo de medios informáticos o tecnologías digitales.

Fue así como desde el año 1996 hasta el año 2008 se presentaron numerosos proyectos de ley destinados a reformar el Código Penal de la Nación mediante una ley integral y concordada para adaptar cada tipo penal a esta nueva modalidad comisiva o bien a través de la sanción de una ley complementaria con idénticas finalidades.

Así podemos mencionar como proyectos de ley presentados durante el periodo 1996-2008 los siguientes:

1. Proyecto de Ley de Leonor Esther Tolomeo de 1996;

2. Proyecto de Ley de Carlos “Chacho” Álvarez (1996);
3. Proyecto de Ley de José A. Romero Feris (1996);
4. Proyecto de Ley de Antonio Tomás Berhongaray (1997);
5. Proyecto de Ley de Anteproyecto de Ley de 2001;
6. Proyecto de Ley de Marta Osorio (1225-D-05);
7. Proyecto de Ley de Silvia Virginia Martinez (1798-D-05);
8. Proyecto de Ley de Andrés L. Sotos (985-D-05);
9. Delia Beatriz Bisutti (2032-D-06);
10. Dante Omar Canevarolo (3001-D-06);
11. Diana Conti y Agustín Rossi (2291-D-06);
12. Proyecto de Ley de Reforma y Actualización Integral del Código Penal de la Nación (resoluciones MJyDH 303/2004 y 136/2005) hasta culminar en el Proyecto de Ley (CD-109/06;S-1751-1875 y 4417/06 y expediente 5864-D-2006) que dio origen a la presente ley 26.388

Este último surgió del tratamiento de un gran número de expedientes legislativos y se presenta como una versión por demás mejorada y refinada de todos los anteriores proyectos desde 1996 hasta 2008.

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

La ley 26.388 partió de una ley de reforma integral y concordada al Código Penal de la Nación, basándose en el modelo de proyecto de la Ley de la diputada, Leonor Esther de Tolomeo (1996) y llevó adelante la modificación de tipos penales tradicionales que la doctrina venía debatiendo durante más de dos décadas (1996-2008) y que se hacían presentes en cada uno de los proyectos de ley antes enunciados.

Es así como la ley 26.388 a alcanzado con su reforma a un número muy limitado y específico de tipos penales como lo son:

1. El ofrecimiento y distribución de imágenes relacionadas con pornografía infantil, artículo 128 del Código Penal.
2. Violación de correspondencia electrónica, artículo 153 del Código Penal.
3. Acceso ilegítimo a un sistema informático, artículo 153 bis del Código Penal.
4. Publicación abusiva de correspondencia, artículo 155 del Código Penal.
5. Revelación de secretos, artículo 157 del Código Penal.
6. Delitos relacionados con la protección de datos personales, artículo 157 bis del Código Penal.
7. Defraudación informática, artículo 173 inciso 3 del Código Penal.
8. Daño, artículo 183 y 184 del Código Penal.
9. Interrupción o Entorpecimiento de las comunicaciones, artículo 197 del Código Penal.
10. El tipo penal de la alteración, sustracción, ocultación, destrucción e inútilización de medios de prueba, artículo 255 Código Penal a lo cual

debe agregarse las modificaciones terminológicas realizadas en el artículo 77 del Código Penal.

Es así como contamos con una reforma que ha llevado 12 años de elaboración y que ha tomado como sustento otros 13 proyectos legislativos, modificando y adaptando tipos penales tradicionales para que puedan ser perpetrados o realizados a través de medios informáticos o dispositivos electrónicos.

Asimismo debe destacarse que el dictado de la ley 26.388 de reforma al Código Penal de la Nación en materia de criminalidad informática cobra mayor significado y relevancia tras la sanción en el año 2011 de la Ley que buscaba la despapelización y digitalización de la Administración de Justicia; nos referimos más precisamente a la ley 26.685.

El jueves 7 de julio de 2011 se publicó la Ley 26.685[27] que otorga a los "expedientes electrónicos, documentos electrónicos, firmas digitales y electrónicas, comunicaciones electrónicas, y domicilios constituidos -la misma- eficacia jurídica y valor probatorio" que en el soporte papel.

Como bien alude de Horacio R. Granero, la ley 26.685 es producto del "Plan Estratégico de modernización de la justicia que ha encarado la Corte Suprema de Justicia de la Nación que es sin dudas una proyección ambiciosa pero a la vez realista, encaminada a transformar en los próximos años el servicio público de Justicia".[28]

La ley 26.685 que introduce el domicilio electrónico y el expediente digital cuenta con dos (2) artículos de fondo y uno de forma.

El artículo 1º de la Ley 26.685 dispone: "Autoriza la utilización de expedientes electrónicos, documentos electrónicos, firmas electrónicas, firmas digitales, comunicaciones electrónicas y domicilios electrónicos constituidos, en todos los procesos judiciales y administrativos que se tramitan en el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales".

Mientras que el artículo 2 establece "que la Corte Suprema de Justicia de la Nación y el Consejo de la Magistratura de la Nación, de manera conjunta, reglamentan su utilización y dispondrán su gradual implementación"

Es así como la Corte Suprema de Justicia de la Nación desde la sanción de la ley 26.685, ha profundizado sus esfuerzos a fin de materializar la aplicación del expediente digital y que no se transforme en una mera declaración de buenas intenciones por parte de la ley.

Pueden destacarse como actos tendientes por su parte de la Corte Suprema de Justicia de la Nación, orientados a la compresión y materialización del empleo del expediente digital:

[27] Boletín Oficial 07/07/2011

[28] GRANERO, HORACIO R., "La sanción de la ley 26.685 de Expedientes Digitales. El principio de la Equivalencia funcional y la firma digital", Revista de Derecho Penal Nº 7, Ministerio de Justicia y Derechos Humanos de la Nación, Buenos Aires, 2014. p. 202

1. Creación de la biblioteca jurídica digital de la Corte Suprema de Justicia de la Nación doctor Rodolfo G. Valenzuela el 31/10/2011.[29]

2. La reglamentación desde el 13/12/2011 del "Sistema de Notificación Electrónica (SNE)"[30]

3. La puesta en funcionamiento del "Sistema de Notificación Electrónica (SNE)" de aplicación obligatoria desde el 7/5/2012, para la interposición de recurso de queja por denegación del recurso extraordinario federal.[31]

4. El establecimiento a partir del 1/6/2012 del "Libro de Asistencia de Letrados (Libro de Notas) dentro del programa informático" de seguimiento de causas de la Corte Suprema de Justicia Nacional, que actualmente se realiza, en lugar del soporte papel.[32]

5. La extensión de la aplicación obligatoria del sistema de notificación electrónica a todos los fueros y diversas materias. [33]

La Corte Suprema de Justicia de la Nación no ha sido la única que ha dado grandes avances en materia de digitalización del servicio brindado por la administración de justicia, como bien menciona Gisela Cardarle, "la justicia de la Ciudad de Buenos Aires ha dado pasos significativos en la formulación de sistemas de gestión bajo el soporte digital".[34]

Además de la sanción de la ley 26.388 de reforma del Código Penal de la Nación en materia de criminalidad informática y de la ley 26.685 de implementación del expediente digital y la notificación electrónica, en el último

[29] Corte Suprema de Justicia de la Nación Acordada 28/2011
[30] Corte Suprema de Justicia de la Nación Acordada 31/2011
[31] Corte Suprema de Justicia de la Nación Acordada 3/2012
[32] Corte Suprema de Justicia de la Nación Acordada 8/2012
[33] Corte Suprema de Justicia de la Nación Acordada 29/2012 "Aplicación obligatoria del sistema de notificación electrónica para los tribunales provinciales en los trámites de un recurso extraordinario federal un recurso de queja extraordinario por denegado" CSJN Acordada 14/2013 "Se dispone la aplicación obligatoria del sistema informático de gestión judicial para todos los Fueros" CSJN Acordada 35/2013 "Aplicación del sistema de notificación electrónica a las presentaciones por retardo de justicia y presentaciones varias ante la Corte Suprema de Justicia" CSJN Acordada 36/2013 "Ampliación del sistema de notificación electrónica a las presentaciones efectuadas en causas originarias ante la Corte Suprema de Justicia" CSJN Acordada 38/2013 "Amplicación de sistema de notificación electrónica a todos los Fueros implementandose a través de las Cámara de Nacionales y Federales" CSJN Acordada 43/2013 "Ampliación de la SNE a todos los superiores tribunales de provincia y a la Ciudad Autónoma de Buenos Aires".
[34] CANDALARE, GISELA "Hacia la justicia digital en la ciudad de Buenos Aires", Revista de Derecho Penal Nº 7, Ministerio de Justicia y Derechos Humanos de la Nación, Buenos Aires, 2014

año se ha realizado una reforma específica y puntual que amplía el catálogo de delitos por medio de la ley 26.904.

La ley 26.904 introduce la figura del grooming al Código Penal de la Nación a través de la nueva redacción del artículo 131, el cual establece que "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, contactaré a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

Como refiere Hugo Vaninetti, el grooming "engloba básicamente la realización de actos preparatorios a través de las modernas tecnologías de la comunicación e información para perpetrar posteriormente delitos contra la integridad sexual. Importaría decir que es una etapa virtual previa al abuso sexual en el mundo real".[35]

Con esta última ley 26.904 tenemos una visión panorámica del marco de lo Legislativo de la República Argentina en materia de criminalidad informática conformada así por la ley 26.338 de reforma en materia de criminalidad informática al Código Penal de la Nación, la ley 26.685 de implementación del expediente digital y la notificación electrónica y la reciente Ley 26.904 que incorpore la figura de grooming al catálogo de delitos ya preestablecido por la ley 26.338 al Código Penal de la Nación.

CAPITULO II: MARCO METODOLÓGICO

Tipodeinvestigación

El **paradigma** que elegimos fue el **interpretativo**, que surgió como una reacción contradictoria al positivismo ya que toma a la persona como sujeto dejando de lado la concepción meramente objetiva.

En cuanto a la **forma** utilizada, se utilizó la **pura** dado que partimos de un marco teórico y permanecimos en él; se ha logrado incrementar los conocimientos, pero sin contrastarlos con ningún aspecto práctico de manera inmediata. No obstante lo antes expuesto, esta forma de investigación buscó el progreso científico con miras a formulaciones hipotéticas de posible aplicación posterior.

[35] VANINETTI, HUGO A., " Inclusión del grooming en el Código Penal", Buenos Aires, La Ley, 2013.

Debido que nuestro propósito era describir cómo se hace frente al fenómeno del cibercriminal en Rafaela podemos decir que nuestro trabajo fue realizado en base al **nivel descriptivo de conocimiento**.

Hemos seguido el **Método Cualitativo** dado que nuestro objetivo fue recoger discursos completos de los sujetos que componen el universo de nuestro campo de estudio y tras la correspondiente interpretación logramos analizar los recursos que posee Rafaela para hacer frente al cibercrimen.

Tomando en cuenta que el eje de nuestra investigación se basó en las entrevistas a los miembros del poder judicial del distrito Judicial Nº 10 (Rafaela) 5ta Circunscripción de la Provincia de Santa Fe, es sencillo dilucidar que el **tipo de dato** que hemos utilizado es **De campo**.
Estudiamos una **dimensión temporal sincrónica**, es decir, transversal, dependiente de un período de tiempo determinado; no su evolución y lo que ello conlleva.

Universoymuestra:

Teniendo en cuenta los objetivos propuestos definimos como universo a los miembros del poder judicial del distrito Judicial Nº 10 (Rafaela) 5ta Circunscripción de la Provincia de Santa Fe que gestionan la actividad en materia penal con competencia en ilícitos relacionados a ciberdelitos. Consideramos que la **muestra** es **sumamente representativa** porque sobre un total de 22 operadores se han podido entrevistar 14, lo que representa el 63.63 por ciento del total.

Técnicaderecolecciónde datos:

Recogimos los datos a través de **entrevistas semiestructuradas** realizadas a jueces (de primera y segunda instancia) e integrantes del ministerio público (de la acusación y de la defensa) y fiscales del distrito Judicial Nº 10 (Rafaela) 5ta Circunscripción de la Provincia de Santa Fe. De lo manifestado por los

entrevistados, hemos decidido citar con nombre y apellido dado el carácter público de las funciones que ocupan y por ende de las opiniones que expresan.

Plandetratamientodelosdatos:

Los datos que se recolectaron han sido verbales y se conservaron de esta manera para el análisis realizado.

CAPITULO II: ANÁLISIS Y CONCLUSIONES

ANÁLISIS

De las entrevistas realizadas extraemos los siguientes datos para analizar, los cuales en gran medida serán objeto de la posterior conclusión.

De lo expuesto por el Dr. Marco Antonio Terragni, Abogado, Doctrinario, Escritor, Doctor en Ciencias Jurídicas y Sociales, Doctor en Derecho, Profesor de Derecho Penal y de Derecho Constitucional, podemos deducir que el tema abordado -léase delitos informáticos- no es algo sencillo, sobre todo, dado que establecer un concepto de Delito Informático no es tarea fácil, aún así tomando una concepción amplia del mismo, Terragni, recordó al menos un caso del cual tuvo conocimiento y fue de mucha trascendencia en la ciudad. En cuanto a la cantidad de casos que llegan a los estrados judiciales, afirmó que no hay diferencia con delitos de otra índole ya que la gran mayoría de los delitos no son denunciados a menos que sus consecuencias sean de importancia significativa; consideró también que la justicia, tanto Nacional como de la Provincia de Santa Fe, están bien dotadas para hacer frente a la problemática en cuestión, en caso de tener problemas un juez de Rafaela podría acudir a los recursos que las antes mencionadas poseen,

pero también destacó que pedir la opinión de un experto local cada día se vuelve menos complejo dado el establecimiento creciente, en la ciudad, de universidades que dictan carreras relacionadas con la informática.

Fernando Gentile Juez de Sentencia de San Cristóbal por medio de su entrevista manifiesta que han arribado aproximadamente 10 casos sobre delitos informáticos.

Considera que esa cantidad de casos no reflejan la realidad de lo que realmente ocurre (hay mayor cantidad de delitos informáticos). El en base a su experiencia como abogado nos cuenta que en reiteradas ocasiones llegaban personas y le realizaban consultas pero estas no se concretaban en actuaciones judiciales y algunos en los que se radicaba las denuncias no tenían respuestas satisfactorias.

En lo que respecta a la ciudad de San Cristóbal no se cuenta con ningún medio en especial, en caso de ser necesario se recurre a peritos generalmente de Gendarmería Nacional (de Paraná) o bien a personal policial de la ciudad de Rosario para que secuestren y/o periten los equipos tecnológicos, tampoco se cuentan con los elementos tecnológicos para asegurar la cadena de custodia del elemento que eventualmente sea incautado dado el elevado costo que implican estos elementos tengo entendido que solo existen un par en la provincia (en nuestra zona no se usan por no contar con los mismos y se asegura como toda prueba pero este tipo de material requiere un cuidado especial por su fragilidad o facilidad de alteración, no hace falta encender un equipo para alterarlo o dañar la información del disco), con lo cual cualquier prueba informática es pasible de nulidad.

Liliana Cattaneo de Serruya, Fiscal Nº2 Cámara Civil y Comercial expresó que esa cantidad de causas no refleja la realidad ya que muchas que ocurren no son denunciadas. Además en lo referente a las estafas a veces los engañados por pudor o vergüenza no denuncian.

Para afrontar la temática nos comentó que realizan oficios, los cuales envían a Facebook, en lo referente a abusos se trabaja con policía federal que son quienes tienen un buscador a tal fin. También a través de pericias con ingenieros y asesoramiento de lo que se conoce como "hackers". En el poder judicial, expresó que no cuentan con elementos y hay que buscarlos fuera.

Como conclusión nos mencionó debiera contarse con mayores recursos tecnológicos, legislarse mejor y específicamente sobre delitos informáticos.

El Dr. Enrique Raúl Klusacek cuyo cargo es Defensor General Nº 1, manifestó que no han arribado delitos informáticos a el, desde que está en el cargo, pero expresó que debiera investigarse en el nuevo sistema de acusación en donde la investigación está a cargo de los fiscales. Además considera que esta cuestión no refleja la realidad, es decir la problemática del delito informático es una realidad creciente, y aún cuando no sea elevada la cantidad de casos que llegan a los estrados, consideró que lo es en la cotidianidad. Por su parte enunció que se debe contar con capacitación para afrontar esta temática delictiva como así también con medios materiales y humanos, los cuales parecen no tenerse; manifestó que se requiere de profesionales, así como en los casos referidos a delitos sexuales, delitos de menores donde se requiere de psicólogos y psiquiatras para conocer su perfil; también es importante contar para el cibercrimen con profesionales capacitados en la materia.

Por último, en cuanto a los medios jurídicos para hacer frente a estos delitos, considera que es importante recurrir a peritos como en muchos otros delitos donde se recurre a la pericia (perito contable, perito calígrafo, etc.). Nos expresó que es posible que el CERIDE ubicado en Santa Fe tenga un Departamento encargado de estos delitos, sin embargo nos comentaba que también el nivel de importancia que se le dé esta supeditado a la cantidad de causas, lo que es bastante bajo; ante esto se le da prioridad a otras necesidades, por ejemplo habiendo muchos delitos sexuales, genera mayor requerimiento de contar con medios materiales y humanos a fin de hacer frente a ellos. “Tal vez no se cuente con los medios necesarios debido a que hay pocas causas a pesar de la gran cantidad de delitos informáticos existentes”, cerró la entrevista Klusacek.

En la entrevista realizada a Javier Carlos Vottero, Juez de Sentencia en lo Penal, él nos manifestó que no llego ninguna causa de delitos informáticos ni vinculada con delitos informáticos.

Expresó que si bien a su estrado no llegaron causas, seguramente deben existir, ya que se da gran cantidad de delitos informáticos, lo cual demuestra la no adecuación entre los delitos denunciados y los efectivamente cometidos.

Consideró que hay escasez de medios por ser un delito, como muchos otros, que está rodeado de un tecnicismo que hace necesaria la colaboración de peritos avezados en el tema en cuestión.

Magdalena Santa Cruz, Defensora General Nº2 de Rafaela con 13 años en el cargo, expresó que no tiene registro de haber tratado con delitos informáticos.

En cuanto a los medios con los que se cuenta considera que mínimamente los jueces tienen dichos medios para investigar, agrega que quizás esos medios tengan que mejorarse, ampliarse, profundizarse, etc, pero sirven para realizar la investigación.

Hugo Alberto Degiovanni, Juez de Segunda Instancia en lo Penal, cuyo cargo desempeña desde Mayo de 2009; en base a su experiencia nos comenta que no recibió causas sobre delitos informáticos en su actual cargo, pero si cuando era fiscal; en dicha función había recibido una denuncia sobre injurias realizadas por medio de Facebook pero que no prosperó debido a que es un delito de instancia privada, por ende, el Ministerio Fiscal no puede actuar.

Nos mencionó que se dan dos factores, primero que es muy difícil identificar al autor en estos temas y por otro lado que, siempre refiriéndose a calumnias e injurias, son delitos de índole privada y ya se hizo tan habitual, lamentablemente, la agresión verbal, que hoy se contestan, y se vuelven agresiones recíprocas por lo que no llegan a tribunales. También expresó tener presente causas, en que no intervino pero tuvo conocimiento, en las que se profirieron insultos, agresiones y descalificaciones a través de una computadora del consejo municipal, causa que estaba catalogada como injuria por un lado y por el otro había algún tipo de amenaza. La amenaza es de orden público, la injuria de orden privado por este motivo no intervino el fiscal.

Esa causa es la que dio origen al caso Fardin de la Corte Suprema de Justicia que implicó adaptar el procedimiento también conforme al caso

Dieser Fratichelli donde se desdoblaron los juzgados correccionales, en el sentido de que el juzgado correccional que instruía no podía a su vez emitir sentencia, entonces las causas pasaban a San Cristóbal. Esa causa se instruyó en Rafaela, paso a San Cristóbal, el entrevistado tiene entendido, no la certeza, que dicha causa prescribió. Mencionó otra causa, pero en base a lo conocido por los medios de comunicación: la causa era de justicia federal por trata de personas y pornografía infantil, la había iniciado la justicia federal y el imputado principal estaba radicado en la localidad de Santo Tome; como en Rafaela una persona recibía esas imágenes en una pc de acceso al público, sin perjuicio de esa causa que es competencia de la justicia federal, se instruyó otra por exhibiciones obscenas mediante la propagación de imágenes pornográficas pero no por el delito de corrupción porque ellos consumían y no las propagaban intencionalmente.

Consideró que con el cambio al Código Procesal Penal se logró un cambio muy positivo: ahora la investigación la realiza el fiscal, el conflicto es que no se cuenta con los medios necesarios, el problema no es solo que no lleguen denuncias sino, que aun llegando no se puede hacer frente debido a dicha carencia. Lo ideal sería que por ejemplo la unidad de investigación tenga un personal estable un perito fijo en delitos informáticos, otro en pericias mecánicas, otro en electrónicas pero eso no se da, hay que apelar a las pericias privadas y todo eso tiene su costo, pero ello no solo ocurre en delito informático sino también en otras figuras delictivas sucede lo mismo.

Como propuesta superadora consideró que, amén de apelar a la pericia privada, una posibilidad sería: al contar con una universidad que tiene ingeniería en informática y el tener un centro, una unidad académica con esa carrera facilita un poco las cosas, como sucede en el tema de la psicología, gracias a que hay dos facultades en psicología que

pertenecen a distintas universidades, una de esas universidades creó una Cámara Gesell y firmo un convenio con el poder judicial, esto no tiene nada que ver con delitos informáticos, pero se podría dar un tipo de colaboración en donde a los alumnos les permite hacer prácticas en tribunales y a su vez nosotros (Poder Judicial) nos nutrimos de la Cámara Gesell de ellos, que sino se tendría que hacer en Santa Fe con el trastorno de trasladar allí a la víctima, recargando la función judicial de la capital provincial. Ese tipo de convenios con la actividad privada sería bueno a futuro. Se daría un aprovechamiento de los recursos locales, donde a la facultad le permitiría realizar prácticas con sus alumnos y al Poder Judicial realizar las investigaciones pertinentes.

María, Alejandra Politi Fiscal Nº 1 Cámara Civil y Comercial, quien se encuentra en el cargo desde Marzo de 2014, dijo que han llegado dos causas a sus estrados.

Expresó que esa cantidad de causas no refleja la realidad ya que muchas que ocurren con Facebook (pornografía) no vienen a denunciarlas. Además en lo referente a las Estafas a veces los engañados por pudor o vergüenza no denuncian.

Para afrontar la temática nos comentó que realizan oficios, los cuales envían a Facebook, en lo referente a abusos se trabaja con Policía Federal que son quienes tienen un buscador a tal fin. También a través de pericias con ingenieros y asesoramiento de lo que se conoce como “hackers”. Algunas veces se piden que se cierren las páginas en las cuales se cometió el delito: por ejemplo cuando en Facebook ponen caras de personas en cuerpos desnudos que no son su físico.

En el poder judicial, expresó que no cuentan con elementos y hay que buscarlos fuera, con excepción de Policía Federal para causas de abusos.

Como conclusión nos mencionó debiera contarse con mayores recursos tecnológicos, legislarse de mejor manera y específicamente sobre delitos informáticos.

Fernando Ignacio Ferrer, Juez Penal de faltas de Rafaela con competencia en contravenciones y no en delitos.

De dicha entrevista surge que llegaron a sus estrados un 20 por ciento de causas por medios informáticos.

A diferencia del resto de los entrevistados el piensa que en cuanto a contravenciones se refleja el porcentaje de causas con las faltas que se producen.

En cuanto a los medios: cuando se cometen por celulares por ejemplo se recurre normalmente a través de pedidos de informe a la compañía prestataria de los celulares que están involucrados (al receptor y al emisor), eventualmente también se utiliza la intervención telefónica.

En el caso de la falta hay que tener en cuenta lo siguiente: los medios tecnológicos con los que se cuenta son, lamentablemente escasos.

Otro medio que nos citó el entrevistado es la oficina de Santa Fe sobre Delitos e Informática en la que una repartición que está dentro de las orbitas de asuntos internos que tienen cuatro funcionarios peritos y que tienen que atender a toda la Provincia de Santa Fe, lo cual es fácil darse cuenta, que resulta altamente insuficiente, sobre todo teniendo en cuenta que tiene que investigar delitos, eventualmente contravenciones y que los delitos que ellos están especialmente dirigidos a investigar son

aquellos que se dan dentro de la órbita policial o dentro de la órbita del poder ejecutivo, la colaboración que brindan es muy valiosa y eficaz al poder judicial es de cualquier manera residual, es decir lo hacen a título de colaboración y en el tiempo que les permite su tarea principal que es la que les encomienda el poder ejecutivo, las informaciones a obtener de los servidores como puede ser Google, como puede ser las compañías prestatarias de servicios llamase Arnet y Compañía, se pueden obtener en la medida que sean informaciones; ahora en la medida que tengan que tramitar intervenciones o cosas por el estilo por ese conducto no funcionan, no funcionan porque allí prácticamente sobre todo los grandes servidores (Google, Yahoo! y demás) son celosos en cuanto a custodiar la información y la fuente de información y por otro lado también por la gran cantidad de solicitudes que tienen lo que hemos notado es que tienden a restringirla en los casos graves (casos de terrorismo, casos de secuestro, casos de pedofilia) estimó que incluso hasta retacean un poco donde hay defraudaciones que no alcancen un nivel significativo; y un nivel significativo es un nivel que involucre ya a entes estatales.

El Dr. Carlos Juan Manuel Stegmayer, quien durante cuatro años ejerció como fiscal y hace cuatro años que ejerce como juez de Instrucción Nº1 en la ciudad, recordó haber tenido contacto con cuatro causas relacionadas al delito informático, a su entender la cantidad de delitos cometidos no se ve reflejada en la cuantía de causas que llegan a estrados judiciales, dado que muchas víctimas no denuncian. Según sus palabras "Los avances tecnológicos fueron enormes y la pesquisa para acreditar esos delitos no ha avanzado de la misma forma. El derecho es lento en su evolución. Muchas conductas reprochables no eran típicas porque la ley penal no la había tipificado como delito. El derecho Penal

no permite para su aplicación la analogía. Un hecho repudiable no puede ser sancionado si antes esa conducta no fue tipificada como delito. Si existe un vacío legal la conducta reprochable queda impune. Si no hay un tipo penal que describe la conducta no hay sanción. La gente no denuncia porque descree que quien efectuó la maniobra perjudicante pueda ser detectado. Además nuestra ley es benévola con delitos informáticos. Ej. Se permite tener pornografía infantil en una computadora, solo se sanciona su publicación, divulgación, etc. España por ejemplo, sanciona tener ese material en un equipo informático." Por otro lado, según su criterio, los Fiscales y la Policía están insuficientemente preparados para investigar y detectar delitos informáticos, dado el tecnicismo que rodea a las cuestiones de esta índole.

La Dra. Mónica Fiorillo quien se desempeña como Asesora del Juzgado de Menores, expresó que en su actual labor no se dan este tipo de casos; pero anteriormente, siendo secretaria del Dr. Carlos en el juzgado correccional, llegó un caso relacionado a la Informática y propagación de material obsceno. También recordó el caso de un menor de 16 años que violó la seguridad de la CIA, como la conducta en Argentina no estaba penada y en Estados Unidos si, se tuvo que firmar un acuerdo; tras mucho tiempo se logró descubrir al responsable, quien hoy trabaja para la CIA. Como medios para esclarecer el delito informático, citó el peritaje y al CERIDE.

De lo expuesto por el Dr. Guillermo Loyola podemos estimar que, si bien es un tema en el que se esta avanzando, Rafaela no posee la infraestructura y los recursos necesarios para hacer frente al cybercrimen pero siempre puede recurrirse a Buenos Aires quienes

están debidamente aprovisionados para ello, aunque el entrevistado expresó que debiera apostarse más a la infraestructura en la esfera local para lograr soluciones más rápidas, puesto que el tener que recurrir a Buenos Aires conlleva una lógica demora que repercute en el proceso mismo y su eficacia.

La Dra. Estrella Jorgelina Moreno quien es Defensora Regional desde 2011 en Rafaela, nos expresó que a ella, en ejercicio de sus funciones, no llegaron causas relacionadas a delitos informáticos lo cual estimó podría ser producto del desconocimiento público sobre que, como y donde se debe denunciar; “mayoritariamente la gente desconoce que puede efectuar denuncias en fiscalía y se concibe en la policía como un organismo de prevención en cuanto a otro tipo de delitos, no este.

El Dr. Osvaldo Carlos, Juez de Distrito en lo Penal desde el año 2000, expresó que desde que está en el cargo llegaron diez causas de las cuales la mitad eran de una justificación importante como para investigarse, estimó que los hechos que se realizan a través de la informática, ya sea para preparar y facilitar otros delitos como para consumarlos directamente mediante la informática ya sea Facebook, Tweeter, casilla de correo, etc. serían muchos más de los que llegan a los estrados.

En lo que respecta al esclarecimiento de estos hechos, expuso que, necesariamente deben participar personas expertas en el tema: lo más habitual es recurrir al Personal de Informática de la Corte Suprema o Personal Policial de la Unidad Regional de CERIDE. De todos modos consideró que estas instituciones quizás deban contar con mayores recursos para ampliar su infraestructura ya que no cuentan con rapidez

para dictaminar en relación a los casos en los cuales se le solicita dicha tarea, aunque de todos modos esto no ha impedido el avance en relación de las causas en las que ellos han intervenido.

CONCLUSIÓN

Del análisis de lo investigado en la bibliografía que se cita, pero en particular de las entrevistas realizadas hemos llegado a la conclusión que la temática propuesta se define en un marco de dos propuestas: ambas no son contradictorias sino que se complementan y pivotean en las siguientes apreciaciones, a saber:

a- que los elementos jurídicos probatorios para investigar el cyberdelito es la pericial específica sobre los instrumentos del delito. No obstante ello, es pacífica la opinión de los entrevistados de:

b- que en esta circunscripción judicial y concretamente en este distrito judicial existen insuficiencias de recursos humanos y técnicos para lograrlo.

De todo lo analizado se puede llegar a la síntesis de que la pregunta que originara esta investigación arroja como resultado que la única forma de investigar este tipo de ilícitos es a través de la pericial específica por medio de profesionales en la materia; no podemos obviar en este trabajo lo que dijeron la mayoría de los entrevistados que hemos citado en cuanto a la insuficiencia de estos recursos de investigación lo que nos lleva también a inferir que esta dificultad podría ser suplida en gran parte aprovechando los recursos brindados por las instituciones académicas de esta ciudad. En tal sentido no se puede obviar que existe en la Universidad Católica de Santiago del Estero las carreras Técnicatura, Analista de Sistemas e Ingeniería en Informática; por su parte la Universidad Tecnológica Nacional las carreras de Ingeniería y Administración entre las que destacamos las vinculadas a la industria e inclusive la Universidad de Ciencias Empresariales a través de la carrera de Licenciatura de Recursos Humanos, por lo expuesto y en miras a ese aprovechamiento de los recursos locales consideramos que así como se hicieron otros convenios con las instituciones de altos estudios para investigar otra modalidad delictiva (ejemplo: Delitos Sexuales) como lo representa la utilización de la Cámara Gesell a través del convenio suscripto con la Excma. Corte Suprema de Justicia de la Provincia de Santa Fe por medio de la carrera de Licenciatura de Psicología con la Universidad de Ciencias Empresariales y Sociales delegación Rafaela.

BIBLIOGRAFÍA

PÁGINAS DE INTERNET:

http://www.asegurarte.com.ar/material/CONAIISI_Temperini_Camera_Ready.pdf

http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

http://www.eldial.com/nuevo/resultados_index_p.asp?vd=j&publicdial=1&total=1&buscar=delito%20informatico

http://www.delitosinformaticos.com/delitos/delitosinformaticos3.shtml

www.terragnijurista.com.ar/doctrina/informaticos.htm

http://www.oijj.org/es/news/noticia-justicia-juvenil-en-el-mundo/el-convenio-sobre-la-ciber-criminalidad-del-guion-consejo-de-eur

http://www.csjn.gov.ar/

http://www.infojus.gob.ar/

http://www.delitosinformaticos.com/legislacion/chile.shtml

http://criminalidadinformatica.blogspot.com.ar/

http://www.angelfire.com/la/LegislaDir/Carac.html

DOCUMENTAL:

ALAGIA, ALEJANDRO; DE LUCA, JAVIER y SLOKAR ALEJANDRO, Revista de Derecho Penal Nº 7, Ministerio de Justicia y Derechos Humanos de la Nación, Infojus, Buenos Aires, 2014

BACIGALUPO, ENRIQUE, Teoría de los lineamientos del delito, ed. Hammurabi, Buenos Aires, año 1994

CABRERA DE HAIRABEDÍAN, MARCELA, “Algunas consideraciones sobre Delitos Informáticos”, Foro de Córdoba, nº 66.

CEJA, Reformas Procesales Penales en América Latin: Resultados del Proyecto de seguimiento, Santiago de Chile, CEJA, 2005.

CANDALARE, GISELA "Hacia la justicia digital en la ciudad de Buenos Aires", Revista de Derecho Penal Nº 7, Ministerio de Justicia y Derechos Humanos de la Nación, Infojus, Buenos Aires, 2014

CHERÑASKY, NORA, "El delito Informatico" en Javier A. de Luca (coord.), XI Encuentro de Profesores de Derecho Penal de la República Argentina. Buenos Aires, La Ley/UBA/AAPDP, 2013.

FONTÁN BALESTRA, Derecho Penal. Parte Especial, actualizadopor G.A.C. Ledesma, 16º ed., Buenos Aires, Lexis-Nexis/Abeledo-Perrot, 2002.

GAMBOA, WALTER F Power Point sobre delito informático.

GOMEZ DIAZ, ANDRES, "El delito informático su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest" en Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)

GUARINONI, R. "Derecho, lenguaje y lógica", Buenos Aires, Lexis-Nexis, 2006.

GUIBOURG, RICARDO; ALLENDE, JORGE y CAMPANELLA, ELENA "Manual de Informática Jurídica", Buenos Aires, Astrea, 1996.

GRANERO, HORACIO R., "La sanción de la ley 26.685 de Expedientes Digitales. El principio de la Equivalencia funcional y la firma digital", Revista de Derecho Penal Nº 7, Ministerio de Justicia y Derechos Humanos de la Nación, Infojus, Buenos Aires, 2014

LASCANO, CARLOS, Derecho penal parte general, CapituloVIII , ed. Advocatus, Córdoba, año 2002

LEZERTUA, MANUEL, "el proyecto de Convenio sobre el Cibercrimen del Consejo de Europa" Cuadernos de Derecho Judicial X-2001. Consejo General del Poder Judicial, Madrid, 2001.

MONSERRAT A., Guía de estudio de derecho pena,l parte general, Capitulo VI, Ed. Estudio S.A, Buenos Aires, año 2011.

MORALES GARCIA, OSCAR, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre Cibercrimen", en AAVV, Delincuencia Informática. problemas de responsabilidad, Cuadernos de Derecho Judicial IX-2002 Consejo General del Poder Judicial, Madrid, 2002.

PERRON, WALTER, "Perspectivas de la unificación del derecho penal y del derecho procesal en el marco de la Unión Europea", en AAVV, Estudios sobre la Justicia Penal. Homenaje al profesor Julio b.j Maier, Buenos Aires, Editores del Puerto, 2005

RADOMIR JASKY Y RUBEN LOMBAERT "Hacia una estrategia europea unificada para combatir la ciberdelincuencia", E) NAC. E-newsletter. En la lucha contra el cibercrimen nº 4 octubre de 2009.

REGGIANI, CARLOS, Delitos Informáticos, La Ley, Buenos Aires, 2008.

REYNA ALFARO, LUIS MIGUEL. "Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal", JURISTA Editores E.I.R.L. Lima, 2002.

RIQUERT, MARCELO, "Delincuencia informática y control social: excusa y consecuencia?" en Revista Jurídica Facultad de Derecho de la UNMDP, nº 6, 2011.

RIQUERT,MARCELO, "Delincuencia informática en la Argentina y el Mercosur", EDIAR, Buenos Aires, 2009.

SALT, MARCOS, "disposiciones Código de Procedimiento Penal sobre el delito cibernético en América Latina en cuanto a su cumplimiento de la Convención de Budapest (Argentina, Chile, Colombia, Costa Rica, México, Paraguay y Perú)", Estamburgo, Consejo de Europa, 12 de abril de 2011.

TÉLLEZ VALDÉS, JULIO Derecho Informático, 3 ed., McGrawHill, México D.F., 2004.

TERRAGNI, MARCO ANTONIO, Derecho Penal Parte General y Parte Especial, Buenos Aires, La Ley, 2014.

VANINETTI, HUGO A., "Inclusión del grooming en el Código Penal" Buenos Aires, La Ley, 2013.

ZAFFARONI, RAÚL; ALAGIA, ALEJANDRO y SLOKAR, ALEJANDRO, Derecho Penal. Parte General.; Buenos Aires, Ediar, 2005.

ZAFFARONI, RAÚL, Política Criminal Latinoamericana;
Perspectivas-disyuntivas; Buenos Aires, Hammurabi, 1982.