Las nuevas tecnologías y los delitos informáticos.
Análisis de la ley 26.388
Modificación del Código Penal argentino

CELLI TRIUNFETTI, SEBASTIÁN

Legajo nº VABG45748

ABOGACIA

Año 2019

Agradecimientos.

Agradezco a mis abuelos Roberto Celli y Eva Bullo por ser mi pilar fundamental, por su apoyo incondicional y por estar conmigo en cada momento, gracias a ustedes he logrado llegar hasta aquí.

A mis padres Eber Triunfetti y Analia Celli que con su esfuerzo y dedicación me ayudaron a culminar mi carrera universitaria, por confiar, por su respaldo constante, por el sacrificio en todos estos años, gracias a ustedes he concluido con mi meta.

De igual manera mis agradecimientos a mis padres del corazón Andrés Storti y Mariana Barrionuevo, a mis abuelos del corazón Roberto Barrionuevo y Norma Cendron y a mi tía del corazón Sol Barrionuevo.

A mis hermanas y a mi hermano por llenarme de alegría día tras día.

Quiero expresar mi agradecimiento a Iohana Boiero, que me ha guiado durante todo este proceso, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de este trabajo.

A Brisa y Uma por ser mis compañeras de estudio todos estos años y a mis amigos que de una u otra manera me brindaron su colaboración y han estado presentes en los buenos y en los malos momentos.

Finalmente quiero expresar mi agradecimiento a la Universidad Empresarial Siglo 21, a mis profesores y tutores de tesis que desde el primer momento me han tratado de la mejor manera y me orientaron al correcto desarrollo y culminación con éxito de este trabajo.

Resumen

El desarrollo de las tecnologías vinculadas con la información y los nuevos métodos de comunicación, así como la aplicación y explotación de distintas actividades humanas de manera abarcadora e invasiva han generado a partir de los años sesenta el surgimiento de conductas antijurídicas específicas de avance y gravedad inimaginable (Altmark y Molina Quiroga, 2012).

La sanción de la ley 26.388 ha incluido una serie de delitos en el Código Penal con el propósito de actualizar el sistema penal argentino como consecuencia de los avances que la sociedad argentina ha experimentado en materia tecnológica. Sin embargo, a pesar de reconocer una mejora en la legislación sobre esta materia caben dudas respecto a si estas nuevas normativas han sido las correctas y adecuadas para lograr la protección de los derechos de los ciudadanos y el control delos actos delictivos realizados mediante el uso de las nuevas tecnologías.

Puntualmente en la presente investigación se procurará analizar si el legislador argentino mediante la sanción de esta ley ha logrado adecuar sus normas internas a los parámetros internacionales sobre regulación y control de los delitos informáticos e indagar si el ordenamiento jurídico argentino brinda las herramientas necesarias para controlar estos delitos producidos mediante el uso de nuevas tecnologías.

Palabras claves: Delito informático- Código Penal- Tecnologías- Información.

Abstract

The development of information's technologies and the new methods of communications, together with the use and misuse of different human activities in an invasive way have created since the 60's the emergence of specific anti-legal conducts with unimaginable gravity (Altmark y Molina Quiroga, 2012).

With the approval of the law n°26.388 it has been included several crimes in the Penal Code for updating the Argentinean penal system as a consequence of the progresses that Argentinean society has experimented in technology. Therefore, it is recognized some improvement in the legislation; however, it is still uncertain if these new legal regulations have been correct and appropriate to protect citizens' rights and to control crimes committed by the use of new technologies.

In particular, in this investigation work it will be analyzed if the Argentinean legislator with the approval of this law has fit its internal norms to the international criteria about regulation and control of informatics crimes. Also it will be studied if the judicial system of Argentina has the necessary tool to control this type of crimes.

Key words: Informatics crimes- Penal Code- Technologies- Information.

Índice

Introducción

En los últimos años, el avance que se ha producido en la utilización de medios tecnológicos incorporados a nuestra vida cotidiana ha cambiado nuestra forma de vivir. Poder acceder a tecnologías de la información y comunicación permite disponer de conocimientos científicos, manejar y consultar todo tipo de información, cauces de relación y comunicación, gran cantidad de material para la diversión y el entretenimiento, entre otros amplios beneficios que la evolución de la tecnología ofrece.

En el anteproyecto de Ley de Delitos Informáticos elaborado en el año 2001 se afirmó que:

> (…) la "Tecno-era" o Era Digital y su producto, la Sociedad de la Información, han provocado un cambio de paradigma social y cultural, impactando drásticamente en la estructura socio-económica y provocando un rediseño de la arquitectura de los negocios y la industria. La Informática nos rodea y es un fenómeno irreversible. Se encuentra involucrada en todos los ámbitos de la interacción humana, desde los más importantes a los más triviales, generándose lo que, en la doctrina norteamericana, se denomina "computerdependency" (Altmark y Molina Quiroga, 2012, p.135).

A esto agregan los citados autores que en realidad no es posible imaginar sociedades actuales sin la informática y si esto ocurriera se cree que éstas colapsarían. De hecho, se ha llegado a afirmar que la informática es un “instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva de forma de energía, e inclusive, de poder intelectual” (Altmark y Molina Quiroga, 2012, p.135).

Ahora bien, resulta cierto que esta invasión de nuevas tecnologías y el mal uso de la informática pueden ocasionar conductas merecedoras de reproche penal. De esta manera será necesario crear nuevos tipos penales que se encarguen de regular la comisión de estas conductas que hace cuartos de siglos eran impensadas por el legislador penal (Sáez Capel, 2001).

En este sentido, al considerar que muchos aspectos de las vidas de las personas se ven afectados, dirigidos o controlados por la era de la informática resulta necesario repensar en la incorporación de estos delitos informáticos en nuestra legislación penal. Al respecto:

> A esta altura del desarrollo de la denominada Sociedad de la Información, no solo la mayoría de los códigos penales modernos del mundo han contemplado alguna forma de criminalidad relacionada con la informática, sino que hasta existe una convención internacional sobre la materia –Convenio de Cibercriminalidad de Budapest del 23 de noviembre de 2001- del cual son parte más de 40 países desarrollados, y que se encuentra en vías de ser implementada en varios de los países que la aprobaron, habiendo sido Argentina invitada a integrarlo recientemente. Es que el delito informático

> ya no puede ser ignorado por el legislador: su realidad y presencia es incontrolable y los efectos devastadores que pueden causar son enormes (Tobares Catalá y Castro Arguello, 2010, p.12).

Así, se parte del reconocimiento de que los delitos informáticos han adquirido especial relevancia en las sociedades actuales y consecuentemente deben ser controlados.

Consecuentemente, la pregunta de investigación que se plantea en este trabajo consiste en indagar si mediante la ley 26.388 que modifica el Código Penal argentino, el legislador ha logrado adecuar sus normas internas a los parámetros internacionales respecto a la regulación y control de los delitos informáticos. A lo que se suma el interrogante de si el ordenamiento jurídico argentino brinda las herramientas necesarias que permitan controlar y/o reducir la comisión de delitos producidos mediante el uso de nuevas tecnologías.

De esta manera, resulta posible indicar que el objetivo general de esta investigación consistirá en analizar lo anteriormente descripto. Es decir, se buscará explorar la ley 26.388 en profundidad para conocer si con su incorporación se ha podido adecuar el sistema jurídico penal argentino a las normativas internacionales vinculadas con los delitos informáticos. Asimismo, se pretenderá indagar si el ordenamiento jurídico argentino brinda las herramientas necesarias para controlar estos delitos producidos mediante el uso de nuevas tecnologías.

Sumado a lo dicho, representan objetivos específicos del presente trabajo el brindar un concepto del delito informático, examinar sus características principales, estudiar cuáles son los medios de comisión de estos delitos e identificar y explicar los tipos de delitos informáticos más frecuentes en nuestro país. Se agregan también la intención de estudiar en profundidad su regulación en el ordenamiento jurídico argentino, principalmente la ley 26.388 que modifica el Código Penal, el analizar los delitos informáticos desde un contexto internacional y el enunciar algunos antecedes jurisprudenciales vinculados con la materia.

Ahora bien, como hipótesis de este trabajo se plantea que mediante la ley 26.388 que ha modificado el Código Penal Argentino parecería no haberse logrado adecuar las normas internas a los parámetros internacionales de regulación y control de los delitos informáticos.

De hecho, el ordenamiento jurídico argentino a pesar de haber logrado con la sanción de la citada legislación un avance en materia de delitos informáticos, no logra aun tipificar todas las figuras delictivas que se tornan día a día más frecuentes en nuestra sociedad. Asimismo, no se cuenta con las herramientas necesarias y apropiadas que permitan controlar y/o reducir la comisión de estos delitos.

En cuanto a la estructura del trabajo final de grado, éste se dividirá en cuatro capítulos. En la primera parte (primer capítulo) se hará énfasis en el delito informático, sus características, los sujetos que intervienen en su comisión y los medios electrónicos más frecuentes utilizados para la comisión de estos actos delictivos.

Con posterioridad, en el segundo capítulo, se realizará un análisis sobre la naturaleza jurídica y el bien jurídico protegido de los delitos informáticos y se definirán aquellas figuras más frecuentes en nuestro país, como la estafa informática, el fraude, el sabotaje informático, el ciberterrorismo, las calumnias e injurias, el espionaje informático, entre otros. Asimismo, se desarrollará una clasificación de estos tipos penales en base a dos criterios: como instrumento o medio y como fin u objetivo.

En el tercer capítulo, se estudiará al delito informático desde un contexto internacional, para lo que se analizará la regulación internacional de la Organización de las Naciones Unidas (ONU)- principalmente los Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal - y los instrumentos provenientes de la Unión Europea, sobre todo el Convenio de Budapest. A esto se suma el análisis legislativo de algunos países como Francia, España, Reino Unido, Estados Unidos, etc.; lo que permitirá realizar un análisis de la recepción interna de los delitos informáticos y compararlo con la de Argentina.

Finalmente, en el último capítulo se brindará un análisis legislativo y jurisprudencial del derecho interno argentino respecto a los delitos informáticos. Esto quiere decir que se explorará sobre el Código Penal antes de la vigencia de la ley 26.388, sobre la Ley de propiedad intelectual, la de protección de datos personales, y principalmente sobre la propia ley 26.388 que ha incorporado algunos delitos informáticos en nuestra legislación. Asimismo, se analizará la ley 20.094 del delito de *grooming* y diversos fallos en relación al tema tratado en el presente trabajo.

Ahora bien, respecto a la metodología de la investigación que se aplica resulta posible afirmar que en el presente trabajo se empleará principalmente el método descriptivo, ya que aquí la intención principal radica en analizar si mediante la ley 26.388 el legislador ha logrado adecuar sus normas internas a los parámetros internacionales sobre regulación y control de los delitos informáticos. Asimismo, se pretende describir sus características más frecuentes para lograr interpretar si el ordenamiento jurídico argentino brinda las herramientas necesarias que permitan controlar y/o reducir la comisión de los delitos producidos mediante el uso de las nuevas tecnologías.

Las estrategias metodológicas pueden ser cualitativas o cuantitativas. En este trabajo puntualmente se utilizará la metodológica cualitativa. De esta manera, se busca observar de manera comprensiva e integrada si mediante la ley 26.388 el legislador ha logrado adecuar sus normas internas a los parámetros internacionales en esta materia.

Yuni y Urbano, (2006) expresan que mediante esta estrategia metodológica se busca la captación del sentido de los fenómenos, se compara las propiedades de los fenómenos y se las analiza críticamente. Consecuentemente aquí se intenta comprender los aspectos de la citada legislación y se los comparará con las disposiciones internacionales sobre delitos informáticos. En suma, se analiza de manera crítica si realmente el ordenamiento jurídico argentino brinda las herramientas que se necesitan controlar y/o reducir la comisión de estos tipos delictivos.

Sumado a lo dicho, las fuentes bibliográficas que se utilizan en esta investigación son de carácter primario, secundario y terciarias. En cuanto a las *fuentes primarias*, se afirma que éstas proporcionan información de primera mano. En este trabajo las principales fuentes de este tipo son la Constitución Nacional, el Código Penal y el Procesal Penal de la Nación y sobre todo la ley 26.388 que incorpora nuevas figuras delictivas al Código Penal. Sumado a lo dicho se utilizan algunas fuentes jurisprudenciales que se consideren de importancia para ilustrar la comisión de delitos mediante el uso de las nuevas tecnologías.

Por otro lado, se recurre a *fuentes secundarias* que son aquellas en las que la información proviene de fuentes primarias, ya que comentan o sintetizan lo desarrollado en éstas. Aquí se utilizan libros específicos impresos o digitalizados sobre delitos informáticos y aquellos vinculados al uso de las tecnologías. Puntualmente se busca la opinión de especialistas en la temática (entre ellos, Palazzi, Tobares Catalá y Castro Arguello y otros), así como también se recurre a revistas especializadas de derecho penal. Sumado a lo dicho, se proporciona información extraída de La Ley Online, Revista de Pensamiento penal, InfoDerecho, Sistema Argentino de Información Jurídica entre otros repertorios de doctrina y jurisprudencia que se consideren útiles para la temática en cuestión.

Finalmente, a las *fuentes terciarias* las constituyen aquellas guías físicas o virtuales que contienen información sobre las fuentes secundarias. Dentro de esta categoría que se utilizan en menor medida, se extrae información de páginas de internet de algunas organizaciones o autores que se hayan expedido sobre los delitos informáticos y manuales de estudios que sinteticen y/o explique todo lo vinculado este tipo delictivo.

Para finalizar, la técnica de recolección de datos en este trabajo es la de análisis documental que consiste en el estudio del contenido de las fuentes antes mencionadas, de manera tal que se realiza una lectura profunda de la legislación, jurisprudencia y doctrina vinculada a la ley 26.388 y se analiza si el legislador ha logrado con estas modificaciones adecuar las normas internas del derecho argentino a los parámetros internacionales sobre regulación y control de los delitos informáticos.

Por último, la investigación toma como punto de partida la entrada vigencia del Código Penal Argentino, que rige desde 1921 hasta la actualidad. Principalmente se hace énfasis en la ley 26.388 sancionada en 2008 y se estudian sus agregados y su impacto para el control de los delitos informáticos desde aquella fecha hasta nuestros días.

En cuanto a los niveles de análisis, el trabajo se centra en el estudio de la legislación, doctrina y jurisprudencia nacional, realizando algunas comparaciones con la regulación internacional sobre la materia.

Sólo resta aclarar- antes de comenzar el desarrollo de este trabajo- que el tema seleccionado se considera de interés actual ya que puede afectar a toda la sociedad y de manera imprevista. Todos y cada uno de nosotros utilizamos de manera constante las diversas herramientas tecnológicas para las distintas actividades diarias. Celulares, computadoras, tablets, el uso desmedido de internet y todas las tecnologías vinculadas con la información son característica común en el quehacer diario. En este sentido, la doctrina afirma:

> La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información, para ejecutar tareas que en otros tiempos realizaban manualmente (Acurio Del Pino, 2015, p. 3).

Consecuentemente a cualquiera podría sucederle que de pronto y de manera impensada e inesperada se encuentre afectado por algún tipo de conducta incorrecta (para no afirmar de manera apresurada “delictiva”) que perjudique nuestros derechos.

Por lo tanto, resulta viable enunciar que el estudio y/o conocimiento de la correspondiente legislación que se encarga de tipificar los delitos informáticos servirá para otorgar mayor certeza respecto a qué es correcto y qué no; y respecto a qué es un delito informático, por lo que se podrá sancionar dichas conductas y hasta evitarlas en algunos casos.

CAPÍTULO I

PRIMERAS APROXIMACIONES SOBRE LOS DELITOS INFORMÁTICOS

Introducción

En el presente capítulo se abordarán los contenidos más generales vinculados con el delito informático, entre los que se encuentran su concepto o definición y sus principales características.

Asimismo, se desarrollará el análisis de las partes de estos ilícitos: el sujeto activo o delincuente por un lado y el sujeto pasivo o víctima por el otro. Se destacará aquí la pertenencia de los delitos informáticos dentro del género denominado “delitos de cuello blanco” y se brindarán los aspectos centrales que identifican a este tipo de conductas.

Finalmente se estudiarán los sistemas electrónicos utilizados con mayor frecuencia como medio de comisión de estos delitos: los correos electrónicos, los mensajes de texto y las redes sociales. Se hará hincapié en los principales delitos que pueden cometerse al recurrirse a estos medios.

1. Concepto del delito informático

En cuanto al concepto de delito informático se afirma que actualmente no existe una única definición general aceptada que lo caracterice. Sin embargo, gran cantidad de autores han intentado definirlo y cuando se hace mención sobre este tipo de crímenes, se asocia generalmente con aquellas “conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo” (Sain y Azzolin, 2017, p.8).

Tal como se observa la propia definición expresa que las tecnologías son utilizadas o como medio para cometer el delito o como fin. En la primera situación, una persona- por ejemplo- utiliza un dispositivo informático como medio para ejecutar la acción ilegal: una estafa. En el segundo caso, el dispositivo informático es afectado por un programa maligno con el fin de aprovechar o modificar su funcionamiento. (Sain y Azzolin, 2017)

Asimismo, la doctrinaria Callegari (citada en Estrada, 2001) define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas". (p.2). Mientras que Zarzana (también citada en Estrada, 2001) expresa que este tipo de delitos incluye “cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo" (p.2).

De esta manera, hablar de delitos informáticos conlleva necesariamente a pensar en las tecnologías o más precisamente en los dispositivos informáticos como herramientas para lograr este tipo de crimen.

Por su parte, Estrada (2001) también cita en su obra “Delito informático, virus y legislación” a Lima, quien afirma que el delito electrónico:

> (…) en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en su sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método o como fin (p.2).

En esta misma obra se brindan dos sentidos de la locución delitos informáticos. Desde un concepto restringido se comprende a aquellas situaciones en las que se atacan elementos informáticos; mientras que el concepto amplio abarca toda acción típica, antijurídica y culpable que se realizó mediante el uso de una computadora o de sus accesorios (Estrada, 2001).

Finalmente, el citado autor menciona a Ulrich Sieber -uno de los autores más prestigiosos en Europa sobre este tema- quien define a este tipo de delitos como "todas las lesiones dolosas e ilícitas del patrimonio relacionada con datos procesados automáticamente" (p.3).

Asimismo, respecto a la denominada “delincuencia informática” resulta de utilidad determinar qué conductas cometidas por medio de sistemas de procesamiento de datos o cometidas en éstos pueden llegar a lesionar derechos individuales y luego proceder a tipificar estas conductas. Sumado a lo dicho estudiar la delincuencia informática permite determinar cuándo una conducta se considera antijurídica por haber lesionado bienes jurídicos protegidos o haberlos puesto en peligro (Castro Ospina, 2002).

En síntesis, el delito informático implicaría todo tipo de actividad ilegal que encuadrara en figuras típicas y conocidas como el robo, hurto, fraude, falsificación, perjuicio, estafa, etc., pero que involucra la informática para ocasionar el perjuicio (Diccionario de información y tecnología, s/f).

Finalmente, otra doctrina agrega que el delito informático: “abarca, por una parte, la amenaza a la esfera privada del ciudadano mediante la acumulación, archivo, asociación y divulgación de datos obtenidos mediante computadoras y por otra, delitos patrimoniales por el abuso de datos procesados automáticamente” (Sáez Capel, 2001, p.30).

De esta manera, tal como se puede observar diversos son los autores que han esbozado una definición de lo que se considera como delito informático y todos ellos coinciden en que, para

tipificar una conducta ilegal como delito de tipo informático, por supuesto debe existir como medio o como fin, la utilización de la tecnología.

2. Principales características del delito informático

Con el avance de las nuevas tecnologías, el uso desenfrenado de Internet y el aumento de material dentro del denominado ciberespacio resulta bastante más probable la comisión de conductas antijurídicas en las redes. Consecuentemente será de utilidad brindar las principales características de los delitos informáticos para conocerlos mejor y poder protegerse frente a estas conductas ilegales que menoscaban los derechos de las personas.

Al respecto, la Teoría General del Proceso entiende que este tipo de delitos presentan los mismos aspectos característicos en cuanto a su composición que los demás delitos. En este sentido, se afirma que debe existir una acción u omisión por parte de un sujeto, que sea típica- es decir, prevista en nuestro sistema jurídico penal- que sea antijurídica y no se encuentre amparada por alguna causa de justificación. Asimismo, debe existir culpabilidad en el sujeto (esto es que sea responsable del hecho) y debe ser pasible de una determinada sanción. Por supuesto a esto se suma las particularidades que deben tener este tipo de delitos: que sea cometido con la utilización de medios informáticos (Tognoli, 2016).

Esto quiere decir que los delitos informáticos deben presentar en su estructura las mismas características que todo tipo de delito, sus aspectos básicos que hacen que una conducta sea reprochable y castigable por el ordenamiento penal. Si no existe una acción u omisión típica, antijurídica, culpable y sancionable, no existirá delito alguno.

Puntualmente según la opinión del autor mexicano Téllez Valdés (citado en Estrada Garavilla, s/f) este tipo de acciones cuenta con la presencia de los siguientes elementos característicos:

> a) Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
> b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
> c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

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

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

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

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

i) En su mayoría son imprudenciales y no necesariamente se cometen con intención.

j) Ofrecen facilidades para su comisión a los menores de edad.

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley. (Estrada Garavilla, s/f, p.4 y 5)

En este sentido, resulta esencial destacar el primer aspecto que afirma que en la mayoría de los casos son conductas de cuello blanco. Esto significa que el sujeto activo (quien comete el delito) es una persona respetable de elevada condición social y que en general, el ámbito en donde se desarrolla la actividad delictiva es en el ejercicio de la profesión de este sujeto.

Al respecto, la doctrina específica que:

(…) el delito de “cuello blanco” sería aquel cometido por personas que gozan de un elevado status social, y que abusan del mismo (para quedar exentos de punición, tanto primaria como secundaria), perjudicando por su accionar, de forma directa o indirecta, a un numeroso e indeterminado grupos de personas, por acciones que son presentadas públicamente como actividades propias de los negocios (Piñeiro Bertot, 2007, p.5).

En cuanto a este concepto, se conoce que ha sido utilizado por primera vez por uno de los criminólogos estadounidenses más influyentes del siglo XX: Edwin H. Sutherland (1883-1950) (Melo, 2009).

Sutherland en su estudio sobre este tipo de conductas delictivas cometidas por personas de alto nivel social advirtió que ellos en raras ocasiones eran detenidos, investigados y conducidos a los tribunales. Incluso afirmó que estas personas rara vez eran detenidas y que la vía penal en este tipo de delitos era utilizada como última alternativa (Melo, 2009). Consecuentemente parece ser que para estos sujetos cometer un delito es mucho más simple y posible ya que en realidad no reciben la sanción que merecen. Es decir, estas personas que muchas veces son profesionales o empresarios utilizan los medios informáticos para realizar alguna conducta delictiva que le otorga

grandes ganancias económicas y gozan, increíblemente, de la impunidad que el propio sistema les garantiza.

Ahora bien, respecto al apartado “c” de los mencionados por el autor Estrada Garavilla -vinculado con la oportunidad de comisión de estos delitos- resulta interesante destacar es cierto que en la mayoría de los casos estos actos se encuentran premeditados o han sido creados por los delincuentes de cuello blanco, quienes indudablemente conocen la forma de utilizar el sistema informático para la comisión del acto.

Asimismo, las pérdidas económicas que produce este tipo de conducta delictiva en la víctima se vincula con las ganancias que el sujeto activo premeditó y procuró obtener. Se afirma al respecto que éstas son cifras sorprendentes y lo más destacable es el hecho de que este tipo de conducta delictiva tiene poco riesgo ya que- como se dijo- se produce en un instante sin la exposición de demasiadas personas, la mayoría de las veces con sólo presionar una tecla o hacer un “click”.

Finalmente, la doctrina anuncia entre otras características a la magnitud de los daños y naturaleza global e internacional de esta clase de delitos. Se agrega al respecto que la facilidad para cometer estos delitos y a la vez las dificultades en la investigación de éstos han conducido a la necesidad de cooperación entre las fuerzas de seguridad y el sector privado (Palazzi, 2016).

3. Sujetos intervinientes en los delitos informáticos

Como en todos los otros delitos contemplados en el Código Penal, cada acción delictiva se caracteriza por ser realizada por un sujeto activo – responsable del acto- y ser ocasionada perjudicando a un sujeto pasivo, también conocido como víctima del delito.

Ahora bien, en los delitos informáticos el sujeto activo no es un delincuente común, sino más bien podría ser una persona física o jurídica calificada por conocer sobre informática y muchas veces de alto poder adquisitivo. El mecanismo y medio de acción que utilizan estos sujetos para producir el daño lo convierten en sujetos especiales y consecuentemente, tal como ya se analizó, se los conoce como delitos de cuello blanco. A continuación, se profundizará en análisis de ambas partes que componen el delito informático.

3.1 Sujeto activo: quien comete el delito

En esta oportunidad se analizará el sujeto activo, es decir aquella persona que comete el delito informático. En este sentido la doctrina afirma:

> Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos (Arregoitia López, 2014, p.1).

Tal como se expresó con anterioridad, quien comete un delito de este tipo se caracteriza por ser un sujeto especial que conoce sobre informática y quien posee un lugar estratégico para poder cometer el acto. En caso de que esto último no sea así, de igual manera se requerirá que el sujeto activo tenga conocimientos sobre los sistemas informatizados para lograr consumar el acto delictivo.

3.1.1 Características especiales del delincuente

Ya se ha descripto anteriormente que el sujeto activo de este tipo de delitos es una persona especializada en cuanto a sus conocimientos. Es decir, no cualquier sujeto es capaz de cometer delitos informáticos.

Puntualmente se ha dicho que el sujeto activo (quien comete el delito) es una persona respetable y en la mayoría de los casos, de elevada condición social; y que en general, el ámbito en donde se desarrolla la actividad delictiva es en el ejercicio de la profesión de este sujeto. Imagínese una persona empleada de una institución financiera que desvía fondos de las cuentas de sus clientes. Indudablemente éste tiene que no sólo trabajar en dicha institución e identificar sus clientes (elegir la víctima de antemano) sino que además, conocer en profundidad el sistema informático que le permitirá realizar la acción delictiva.

Así, en cuanto al nivel de profesionalidad y características personales de los sujetos activos, existen quienes consideran que el nivel típico de aptitudes del delincuente informático requiere de inteligencia, decisión, motivación y estar dispuesto a aceptar un desafío tecnológico; todo lo que permite imaginar una persona de especiales conocimientos como lo sería por ejemplo un empleado

del sector de procesamiento de datos (Ramírez Bejerano y Aguilera Rodríguez, 2016). Se destaca aquí consecuentemente la profesionalidad y especialización del sujeto activo; es decir, no cualquier persona puede cometer un delito informático.

Asimismo, se ha mencionado que no es fácil descubrir y sancionar este tipo de conductas delictivas y esto es así debido al poder económico que poseen quienes las cometen. Los daños económicos son elevados y existe un gran desconocimiento de la opinión pública y de la sociedad sobre los daños que ocasionan los delitos informáticos. De hecho, las personas que cometen este tipo de delitos ni siquiera son considerados delincuentes, no reciben trato como tal, no se los desprecia ni se los desvaloriza como sí se lo hace con un delincuente de los delitos más frecuentes o conocidos. Incluso la doctrina ha llegado a afirmar que este tipo de conductas son objeto de medidas o sanciones administrativas y no de sanciones que impliquen condenas privativas de la libertad (Segu.Info, s/f).

En suma, se recuerda que los delitos informáticos son considerados como delitos de cuello blanco. En consecuencia, las características que posee el sujeto activo como delincuente de cuello blanco son las siguientes:

> - Utiliza su condición social para insertarse en el ámbito dentro del cual realizará el hecho delictivo.
> - Se maneja con la credulidad o ignorancia de la víctima, por conocer la forma de realizar el ilícito bajo una apariencia legal.
> - El hecho criminal, no posee una trascendencia importante dentro de la sociedad, como puede ser un asesinato.
> - Existe una confianza natural de la sociedad hacia una persona a causa de su posición política, social o económica. Su respetabilidad genera la confianza que le abre las puertas a datos y lugares que, a otros de diferente condición social, se le negaría.
> - Existe una escasa visibilidad del delito. El delincuente de cuello blanco realiza un golpe indirecto, sin tener contacto con su víctima.
> - Volatilización de la cantidad de víctimas producto de que la mayoría de los crímenes de cuello blanco se ejecutan a través de organizaciones. (Anzit Guerrero, 2008, p.4).

De esta manera, tal como se observa las condiciones especiales que caracterizan a este sujeto activo permiten que el delito en sí sea mucho más fácil de consumarse. La condición social del delincuente, su fácil acceso a los sistemas informáticos, su profesionalidad, su confianza, la ignorancia de la víctima, el escaso tiempo que lleva cometer esta acción, entre otros aspectos, configuran el escenario ideal para este tipo de crímenes.

3.2 Sujeto pasivo: víctima del delito

Así como todo delito se identifica por poseer un responsable quien comete la acción, todo delito también tiene un sujeto que padece los efectos de este accionar: el sujeto pasivo o víctima.

En este orden de ideas la doctrina entiende que el sujeto pasivo es la víctima del delito, el propietario legítimo del bien jurídico protegido, aquella persona sobre quien recae la acción u omisión que realiza el sujeto activo (Arregoitia López, 2014).

La citada autora ha afirmado que, aunque estos ilícitos sean difíciles de investigar y de descubrir y en general lo son debido a la falta de legislación que los contemple, lo que facilita su investigación muchas veces son los propios sujetos pasivos.

Respecto al sujeto pasivo de los delitos de este tipo, se afirma que las víctimas de delitos informáticos puede ser cualquier persona. De hecho, casi la totalidad de la población con su conducta favorece en el 99% de los casos (Maza Correa, 2018).

En este sentido, así como en otros tipos delictivos, la víctima puede adoptar una posición neutral que ni favorece ni perjudica la conducta del sujeto activo. Sin embargo, en los delitos informáticos la posición de la víctima es esencial en cuanto a adoptar una conducta preventiva para evitar ser perjudicada por el agresor. Puntualmente la doctrina expresa:

> El sujeto pasivo, en el caso de los delitos informáticos pueden ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos. Víctima puede ser cualquier persona física o jurídica que haya establecido una conexión a Internet (ya que es la principal ventana de entrada para estas conductas), una conexión entre computadoras, o que en definitiva cuenta con un sistema informático para el tratamiento de sus datos (Maza Correa, 2018, p.1).

De esta manera resulta evidente que la víctima de estos delitos puede ser cualquier persona, ya que todos nosotros nos encontramos en situación de vulnerabilidad en el uso constante y despreocupado de Internet. Más precisamente a través de las propias redes sociales se generan distintas conductas que pueden acabar perjudicando derechos de las personas incluso sin darnos cuenta.

Asimismo, la doctrina consultada especifica que se considera de esencial relevancia el aporte de los perjudicados para cooperar en la determinación del *modus operandi* utilizado por los delincuentes y poder prevenir y sancionar estas conductas. Sin embargo, en la mayoría de los casos los sujetos pasivos no adoptan ningún tipo de precaución ni aportan demasiado a su

investigación. Es decir, no presentan denuncias y a veces ni siquiera son conscientes de haber sido víctima de un delito informático (Maza Correa, 2018).

Consecuentemente las estadísticas de este tipo de delito se mantienen ocultas y se dificulta su prevención efectiva que requeriría un análisis de las necesidades de protección y de las fuentes de peligro, que al no ser denunciados no resulta posible realizar. De hecho, si las víctimas potenciales conocieran las técnicas de manipulación y sus formas de encubrimiento se lograría una protección eficaz.

En igual sentido, si se divulgaran las posibles conductas ilícitas que se pueden generar con la utilización de las computadoras y se alertara a los potenciales sujetos pasivos para que tomen las medidas necesarias para prevenir la delincuencia informática y sobre todo si se contara con una adecuada legislación en la materia, se habría evolucionado en la lucha contra este tipo de delincuencia que día a día se expande más y a velocidades impensadas (Ramírez Bejerano y Aguilera Rodríguez, 2016).

Para ilustrar los alcances en las víctimas, en los Estados Unidos se conoce que los números de tarjetas de créditos sustraídos en los últimos meses se multiplicaron y que los ataques informáticos comenzaron a crecer de manera tal que han encendido una luz de alarma a nivel mundial. Afirman las noticias que UPS, Target, Taples o Ebay son algunos de los comercios que fueron víctimas de este tipo de delitos.[1]

Esta fuente de información citada afirma que, por su parte, en Argentina aún no existen datos precisos sobre este tipo de delitos. Esto coincide con lo afirmado con anterioridad respecto a la falta de denuncias y de registros de este tipo de conductas delictivas. Sin embargo, el hecho de que no existan números que confirmen la existencia de estos ilícitos esto no quiere decir que no sean real.

Ahora bien, tal ha sido el crecimiento del uso de las tecnologías y los delitos cometidos mediante su utilización que se han comenzado a divulgar consejos para la prevención de estos actos. Entre ellos, vinculado con el uso de las tarjetas de créditos se recomienda firmar la tarjeta tan pronto como se reciba el plástico y revisar lo que se firma; denunciar los robos de éstas; revisar cotidianamente los consumos; no brindar claves ni datos personales a desconocidos por mail o teléfono; tener la precaución de chequear los sitios web a la hora de comprar, etc.

[1] Fuente: ¿Cómo evitar ser víctima de delitos informáticos? (09/11/14). *MinutoUno.com*. Recuperado el 27/14/18 de https://www.minutouno.com/notas/343506-como-evitar-ser-victima-delitos-informaticos

En nuestro país el Ministerio Público Fiscal informó en una nota al Diario El Clarín que los delitos informáticos no paran de crecer. "No sólo los que implican un perjuicio económico (como el robo de claves bancarias) sino también la difusión no deseada de imágenes íntimas y otras distintas variantes de acoso sexual en las redes".[2]

En este orden de idea, la Unidad Fiscal Especializada en Ciberdelincuencia informó que el sujeto pasivo- víctima- de estos delitos podría seguir ciertas recomendaciones básicas tales como las enunciadas anteriormente, a las que suman: Utilizar contraseñas fáciles de recordar, pero difíciles de adivinar; no utilizar las mismas claves para todo; configurar opciones de privacidad en las redes sociales; no compartir datos personales o imágenes íntimas por chat; realizar copias de seguridad de los archivos; no utilizar cámaras web con desconocidos, entre otras.[3]

4. Sistemas electrónicos como medios de comisión de los delitos informáticos

Se afirmó con anterioridad que este tipo de delitos son cometidos mediante el uso de las tecnologías como fin o como medio para cometer el ilícito. En esta oportunidad se analizarán aquellos sistemas electrónicos más comunes y frecuentes cuya mala utilización genera el acto delictivo. Afirma la doctrina al respecto:

> Las conductas disvaliosas que utilizan a los sistemas informáticos o teleinformáticos como medio o instrumento para la comisión de delitos, no producen el daño sobre el bien o elemento del sistema, sino que se sirven de éste para causar un perjuicio a otros bienes o a personas (Altmark y Molina Quiroga, 2012, p.140).

En este sentido se hace referencia a la utilización del correo electrónico, del celular, de los mensajes de textos, etc. para cometer un acto delictivo. Es decir, se trata de conductas antijurídicas que no son ordinarias y que requieren de conocimiento y acceso a la tecnología a partir de un sistema; sumado a que se utiliza a éste como instrumento para lograr la finalidad delictiva perseguida. Esto puede realizarse al utilizar ilegítimamente los datos y programas de un sistema o utilizándolo de manera correcta, pero para introducirse en otro y producir un resultado disvalioso en bienes económicos o personales de otros sujetos (Altmark y Molina Quiroga, 2012).

[2] Fuente: Lanzan una guía oficial para no ser víctima de delitos en las redes. (28/04/2016). *El Clarín*. Recuperado el 01/05/18 de https://www.clarin.com/sociedad/lanzan-oficial-victima-delitos-redes_0_N1TzBGsg-.html
[3] Ídem cita anterior

Se analizarán a continuación los medios más frecuentes para la comisión de delitos económicos.

4.1 Correo electrónico

Los correos electrónicos son herramientas utilizadas de manera frecuente por todas las personas, ya sea por trabajo o como medio de comunicación cotidiana. Se considera que enviar un correo electrónico con contenido ilegal es tarea fácil, incluso cuando el remitente y el destinatario se encuentran en distintos países. De hecho, "algunos de los proveedores de servicios gratuitos de correo electrónico más conocidos tienen millones de usuarios en todo el mundo, lo que refuerza la dimensión transnacional del delito cibernético" (12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 2010, p.4).

En cuanto a este medio, se afirma que interceptación del correo electrónico queda asimilada con la violación de correspondencia y forma parte de los denominados delitos contra la intimidad de la persona (Acurio Del Pino, 2015).

De hecho, el citado autor expresa que los adelantos en la tecnología de las comunicaciones han generado nuevas oportunidades para que se cometan este tipo de delitos complejos. "La tecnología de las comunicaciones también confiere más flexibilidad y dinamismo a las organizaciones delictivas; el correo electrónico se ha convertido en un instrumento de comunicación esencial independiente del tiempo y la distancia" (Acurio Del Pino, 2015, p.50).

Asimismo, la ley 26.388 que modifica el Código Penal argentino ha contemplado dentro de su articulado como delito informático a la intercepción o captación de comunicaciones electrónicas o telecomunicaciones en el artículo 153 párrafo segundo (Abogados portaley, 2008). Esto quiere decir que la violación de los e-mails ya ha sido tipificada como delito, de aquellos asociados con el perjuicio a la intimidad de las personas.

Para otorgar mayor precisión, se mencionarán a continuación algunos de los delitos que se cometen vía correo electrónico:

- **Spam**

El spam consiste en el envío masivo de mensajes con contenido generalmente publicitario. Se realiza a través de los foros, la mensajería instantánea, los blogs, el correo electrónico, etc. En este tipo de delitos los spammers o remitentes emplean programas "o software especializados o

robots que rastrean páginas web en busca de direcciones, compran bases de datos, utilizan programas de generación aleatoria de direcciones, copian las direcciones de listas de correo, etc." (RecoveryLabs, s/f).

En este sentido, se considera que aquí el delito se vincula con la obtención de la dirección de correo electrónico de una persona, de manera ilegítima; y la perturbación del orden y de la privacidad de la víctima que se genera con el constante envío de publicidad no solicitada por ésta.

Asimismo, se conoce que últimamente se utiliza el envío masivo de correo electrónico (spam) para generar estafas; es decir que a través del spam se estarían cometiendo delitos de mucha mayor gravedad.

- **Apoderamiento de correo electrónico**

Este tipo de conductas implica que el sujeto activo desplace la cosa o el soporte en el que se encuentra la información de manera secreta, a su propio ámbito de dominio o control. Incluye el apoderarse de algo que no le pertenece, como se lo hace en el hurto (Casanova, s/f).

- **Virus**

Los virus forman parte de aquella información peligrosa que se recibe muchas veces a través de los e-mails. Mediante el envío de virus se propagan códigos maliciosos que infectan las computadoras de quienes lo reciben. Puntualmente se afirma que:

> Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos (Virus y delitos informáticos, 2012, p.1).

De esta manera, quien envía un virus con el propósito de dañar el sistema informático de otra persona, estará cometiendo un delito cuyo medio ha sido la utilización de los correos electrónicos.

- **Interceptación ilícita**

Respecto a este delito la doctrina expresa que ésta puede ocurrir a través de las escuchas, monitoreo, vigilancia del contenido de las comunicaciones para adquirir contenido de datos de manera directa mediante el uso del sistema informático; o de manera indirecta a través de la utilización de dispositivos electrónicos para escuchar de forma secreta o para intervenir conversaciones (Altmark y Molina Quiroga, 2012).

De esta manera, tal como se afirma, el interceptar información privada -más precisamente intervenir conversaciones- mediante el acceso a correos electrónicos constituye un delito y debe ser sancionado.

4.2 Mensajes de texto

Así como se hizo referencia a la utilización del correo electrónico para la comisión de delitos informático resulta necesario destacar que estas conductas delictivas también pueden tener lugar mediante el uso de mensajes de texto de un teléfono celular.

Acceder de manera indebida o apoderarse de una comunicación en un mensaje de texto para ocasionar un perjuicio a una persona es una conducta dentro de las tipificadas por la ley 26.388 en su artículo 4 que modifica los artículos 153 y 153 bis del Código Penal:

> ARTICULO 4º — Sustitúyase el artículo 153 del Código Penal, por el siguiente:
> 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.
> (…)

De hecho, puntualmente dentro de los delitos que pueden ocasionarse mediante el uso de mensajes de texto se encuentra el *grooming*.

Esta terminología implica el contacto o acercamiento virtual con una persona menor de edad con el propósito de intercambiar imágenes o contenidos de índole sexual. Aquí el sujeto activo busca generar confianza en el menor, lograr empatía con éste y luego convencerlo para el intercambio de información con la intención de cometer algún tipo de abuso sexual que lesione la integridad física del menor, más allá de la forma en la que se manifieste la agresión y en este caso, vía mensaje de texto (Tazza, 2014).

Queda aquí comprendidos los mensajes gratuitos de la aplicación whatsapp que en la actualidad han adquirido mucha mayor utilidad que los propios mensajes de texto pagos, sobre todo se conoce que gran cantidad de menores tienen acceso a esta herramienta de comunicación.

Sumado a lo dicho, se pueden ocasionar estafas mediante el uso de mensajes de texto o whatsapp. De hecho, ya es práctica común recibir mensajes en el celular que indican que se debe completar una encuesta y que con ella se ganará un cupón de dinero para gastar en diversas tiendas. La persona que lo recibe ingresa al link y completa las respuestas creyendo que obtendrá dicho beneficio cuando en realidad nunca sucederá. De igual manera "(…) marcas internacionales como H&M, Ikea, McDonald's, Burger King, entre otras, han sido utilizadas por ciberdelincuentes para engañar a la gente que usualmente no tiene un profundo manejo de redes" (AE Tecno, 2018, p.2).

Asimismo, otro delito que se puede cometer mediante el uso de mensajes de texto es el manipular conversaciones electrónicas que implica inventar textos que no son los reales e incluso eliminarlos. Esto muchas veces es utilizado para presentar pruebas falsas en juicios y cotidianamente para hacer bromas entre los distintos usuarios de whatsapp. Al respecto la doctrina destaca lo fácil que resulta descargar programas para manipular mensajes a través de virus troyanos o de forma manual. Se acceden a bases de datos que modifiquen los mensajes recibidos, la hora, la fecha, etc. (Abogados portaley, 2014).

4.3 Redes sociales

Por último, se analizará a las redes sociales como medio de comisión de delitos informáticos.

En la actualidad la utilización de redes sociales como Facebook, Instagram, Twitter, etc. han generado innumerables situaciones que pueden ser aprovechadas por los delincuentes para ejecutar sus conductas delictivas. Son éstas un medio idóneo puesto a disposición de quienes pretenden cometer el acto ilegal.

Ahora bien, respecto al uso de las redes sociales resulta común su utilización indebida para generar pruebas falsas en los tribunales, tal como se mencionó con los mensajes de texto. La jurisprudencia ha demostrado que el acceso ilegítimo a información vertida en las redes sociales constituye prueba ilegal que no puede ser valorada en un proceso judicial. De hecho, Tribunal Supremo de la Ciudad Autónoma de Buenos Aires en una de sus causas afirma:

> La presente causa se sustancia por la denuncia efectuada por la querellante a quien fuera su esposo, el cual —con la ayuda de quien fuera su hermana, también querellada— habría accedido ilegítimamente a la información obrante en el muro de su cuenta de "Facebook" con el propósito de utilizarla como prueba en el juicio de divorcio que la querellada le había promovido. Adecuó dicha

> conducta a las prescripciones contenidas en el art. 153 bis del Código Penal, incorporado por la denominada "Ley de Delitos Informáticos" dentro del nuevo Capítulo III del Título V del Libro II, el cual pasó a denominarse "Violación de secretos y privacidad", conforme al art. 3° de la precitada ley (Cueto, 2015, p.1).

Puntualmente la nueva figura penal expresa: "Será reprimido con prisión de quince [15] días a seis [6] meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido" (Cueto, 2015, p.1).

Este artículo contempla justamente aquellos accesos ilegítimos a información privada de una persona, sin su autorización; lo que frecuentemente sucede con Facebook y las demás redes sociales.

En cifras, las noticias informar que "(…) al menos cuatro de cada diez usuarios de redes sociales han sido víctimas de algún ciberdelito. Sin embargo, muchas veces los propios usuarios de Internet desconocen si fueron víctimas de estos delitos" (Techlandia.com., s/f, p.1)

La utilización de las redes sociales para cometer delitos informáticos comprende ciertas figuras entre las que se pueden mencionar:

- **El phishing**

Esta técnica es empleada por hackers quienes se adueñan de datos y utilizan dicha información en sitios de compras online o similares. Particularmente en Facebook se creaban enlaces falsos en los eventos; esto es, un robot genera un evento apócrifo que se envía a todos los usuarios para que éstos confirmen su asistencia cuando en realidad se trata de un link engañoso que solicita datos personales que luego son utilizados para realizar compras en Internet (Techlandia.com., s/f).

- **Robo de identidad**

Este tipo de conducta en una de las más frecuentes en las redes y han aumentado en los últimos años. Implica la recepción de un correo electrónico de algún conocido que invita a entrar a ver una foto, por ejemplo, el Facebook; mientras que en realidad es un engaño ya que ese link conduce a una página que aparenta ser Facebook pero no lo es. Al ingresar allí los datos personales (usuario y contraseña) se produce el hecho delictivo: se roban dichos datos y se duplica la identidad de la persona(Techlandia.com., s/f).

- **Robots**

Esta denominación se refiere a los programas desarrollados por los hackers con los que crean de manera masiva cuentas en redes sociales con el propósito de lograr ganar miles de seguidores en pocas horas. Estas cuentas falsas envían mensajes con links que conducen a los usuarios hacia virus maliciosos que roban información de las computadoras de las personas (Techlandia.com, s/f).

Estas conductas descriptas son a modo ilustrativo, ya que en realidad se pueden producir cantidad de delitos informáticos a través de las redes sociales. Sin embargo, aquí se pretende simplemente brindar las primeras aproximaciones vinculadas con este tipo de conductas ilegítimas.

Conclusiones parciales

En este primer capítulo se han brindado las primeras aproximaciones sobre los delitos informáticos. Se definió el concepto, se analizaron las principales características y se estudió a sus partes: tanto al sujeto activo como al sujeto pasivo o víctima. Asimismo, se brindaron las principales características de los delincuentes que acostumbran a realizar este tipo de conductas ilegales, los que se conocen como "delincuentes de cuello blanco".

Finalmente se estudiaron los medios más frecuentes de comisión de estos delitos, entre ellos la utilización de correos electrónicos, mensajes de textos y redes sociales. A través de estos sistemas informáticos el sujeto activo realiza la conducta delictiva y ocasiona un perjuicio en la víctima, como contrapartida de su beneficio.

Pues bien, hasta aquí con esta presentación de la temática bajo estudio ya resulta posible destacar la influencia a grandes escalas del uso de la tecnología. Esto permite deducir que su mal uso y su negligencia en controlar las acciones ilícitas que de ella puedan surgir, repercutirá sin límites en la vida de las personas; es decir, podrá perjudicar sus derechos más íntimos y generar daños inimaginables.

De esta manera, con todo lo desarrollado hasta aquí se puede afirmar que resultó necesario en primer lugar definir y conocer en profundidad las características de los delitos informáticos para poder continuar con el análisis que permitirá la comprobación, o no, de la hipótesis planteada al inicio de la investigación.

CAPÍTULO II

ANÁLISIS DOCTRINARIO DE LOS PRINCIPALES DELITOS INFORMÁTICOS

Introducción

En este capítulo se procederá con en análisis de la doctrina que explica los principales delitos informáticos.

En primer lugar, se desarrollará la naturaleza jurídica y el bien protegido de este tipo de delitos para continuar con el análisis específico de cada uno de los tipos delictivos más frecuentes en esta sociedad, cuando de delincuencia informática se trata. Es decir, puntualmente se estudiarán la estafa cometida por medios tecnológicos, el fraude, el sabotaje informático, el denominado ciberterrorismo, las injurias y calumnias que se puede producir en la web, el espionaje informático y otros delitos también conocidos vinculados con la informática y el uso de las nuevas tecnologías.

Por último, se brindará una clasificación, dentro de las tantas que existen, que agrupa a estos delitos según el bien jurídico que menoscaben: delitos contra el patrimonio, contra la intimidad y contra la seguridad pública y las comunicaciones.

1. Naturaleza jurídica y bien jurídico protegido de los delitos informáticos

La realidad demuestra que el uso aplicación de Internet en la vida de las personas y en el quehacer diario en conjunto con el crecimiento de las conexiones a través de la tecnología requieren indudablemente un marco normativo que regule y tipifique las conductas punibles que han utilizado la red ya sea como medio o como fin. Así como la utilización de las tecnologías brinda innumerables ventajas y avances en una sociedad resulta imposible ocultar que en algún momento todo esto generaría acciones reprochables. No obstante, tal como lo afirma la doctrina, no es posible culpar a la tecnología, ya que ésta es simplemente un medio más para expresar las conductas humanas (Martínez Fazzalari, 2008).

Sin embargo, cierta doctrina sostiene que el objetivo principal- el de regular estas conductas reprochables a través de la legislación- se encontraría cumplido. Sin embargo, se torna necesario contar con actualizaciones constantes a nivel técnico como legislativo y jurisprudencial debido justamente a que en esta materia la evolución conlleva a que en cada instante lo de ayer ya sea obsoleto (Tobares Catalá y Castro Arguello, 2010).

Ahora bien, cuando se trata de analizar el bien jurídico de este tipo de delitos, la doctrina afirma que es posible distinguir dos teorías que se hallan vinculadas con la forma que adopta (o debería adoptar) la tipificación de dichos delitos (Mayer Luxl, 2017).

Por un lado, se encuentra aquella tesis que sostiene que los "(…) delitos informáticos tutelan un bien jurídico específico, propiamente informático, diverso del que protegen los delitos tradicionales" (Mayer Luxl, 2017, p.238). De esta manera, la distinción entre un delito de tipo informático y otro delito distinto es de fondo y no de forma. Se afirma que el modelo seguido por la Ley Nº 19.223, de 7 de junio de 1993 fue un ejemplo claro de esta postura ya que, en vez de modificarse las normas existentes, se optó por una regulación independiente de los delitos informáticos por fuera del Código Penal destinada proteger "un nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales" (Mayer Luxl, 2017, p.238).

Sin embargo, por otro lado, la misma doctrina especifica que también se conoce la tesis que afirma que los delitos informáticos no tutelan un bien jurídico específico. De hecho, sostienen que el aspecto de "lo informático" no es más que un "contexto delictivo o un particular medio de afectación de bienes jurídicos tradicionales, como la intimidad o privacidad, el patrimonio o la fe pública" (p.239). Por lo tanto, aquí la diferencia no sería de fondo sino meramente de forma. Consecuentemente los delitos informáticos no se distinguirían de los tipos delictivos comunes por los intereses en juego. De esta manera se entiende necesario "(…) encontrar un acomodo entre los delitos que afectan bienes jurídicos tradicionales, sea directamente o de no ser posible una subsunción inmediata introduciendo ajustes legales para dar cabida al factor informático" (Mayer Luxl, 2017, p.239).

Asimismo, el profesor español Romeo Casabona señala que "En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa" (Acurio Del Pino, 2015, p. 6). Al respecto, este profesor ha afirmado que el bien jurídico protegido no siempre es de la misma naturaleza, así como tampoco lo es la naturaleza; ni la forma de cometer el hecho delictivo presenta características semejantes. Agrega:

> (…) el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información (Acurio Del Pino, 2015, p. 6).

Por su parte, el profesor Francisco Bueno Aruz en un estudio sobre el delito informático y los bienes jurídicos que pueden resultar afectados, afirma que este asunto respecto a si este tipo de delincuencia presupone un nuevo bien jurídico protegido dentro del ámbito penal, resulta relativo. Bueno Aruz explica que si en realidad la delincuencia tecnológica se destaca por los medios utilizados (que de hecho dificultan el descubrimiento de los hechos y la prueba de éstos) entonces el bien jurídico protegido en cada caso en particular será el que corresponde a la naturaleza propia de la infracción. Esto es, por ejemplo, la intimidad, la propiedad, la propiedad intelectual o industrial, la fe pública, el buen funcionamiento de la Administración, la seguridad exterior o interior del Estado (Castro Ospina, 2002).

Pues entonces en este trabajo de investigación se concuerda con esta postura, al igual que con aquella que sostiene que los delitos informáticos no tutelan un bien jurídico específico sino los tradicionales. Los delitos informáticos se destacan por poseer un contexto delictivo o un medio de comisión distinto a los delitos comunes tipificados por el Código Penal argentino; y no así por los bienes jurídicos protegidos, que en realidad coinciden con la naturaleza de la infracción cometida, tal como lo afirma Castro Ospina.

2. Definición de los principales delitos informáticos

> Las características intrínsecas de Internet posibilita múltiples consecuencias positivas (interconexión virtual, eliminación de barreras de espacio y tiempo, económicamente accesible, la posibilidad del anonimato, acceso a contenidos ilimitados de cualquier lugar en el mundo, etc.) pero también acarrea como contracara aspectos negativos entre los que se encuentran los delitos informáticos y los inconvenientes para la persecución de dichas actividades apoyados en algunas de las mencionadas ventajas (Vaninetti, 2017, p.1).

En este apartado se analizarán los principales delitos informáticos que según las estadísticas son más frecuentes en Argentina.

2.1 Estafa informática

La estafa en general se define como un delito que menoscaba la propiedad o el patrimonio de una persona. Adquiere diferentes modalidades ya que se puede producir de un modo activo como de manera pasiva; es decir, a través de una acción o de una omisión. Esta última modalidad

requiere que el engaño sea suficiente como para ser calificado de estafa (Seguridad Informática, 2007).

Las características de este tipo delictivo comprenden ciertos elementos como la existencia de un engaño; el ánimo de lucro de quien comete el engaño; la existencia de un traslado patrimonial no autorizado ni consentido o en error; y la realización de este traslado en perjuicio de otra persona (PeritoIT.com., 2017).

Agrega la doctrina citada que de estos elementos se debe destacar el engaño como requisito esencial y definitivo. Éste debe ser un "(…) engaño antecedente, bastante y causante, es decir, idóneo, relevante y adecuado para producir e inducir al error al engañado (la víctima)." (PeritoIT.com., 2017, p.1).

En este sentido, Carlos Creus describe la secuencia causal en la estafa y menciona que en primer lugar el agente despliega una "(…) actividad engañosa que induce en error a una persona quien, en virtud de ese error, realiza una prestación que resulta perjudicial para su patrimonio" (Vaninetti, 2017, p. 2).

De hecho, la doctrina citada afirma que estos elementos: ardid, engaño, disposición patrimonial forman la trilogía imprescindible para la configuración del delito de estafa.

Sumado a lo dicho, otros autores como Zaffaroni y Baigun definen a la estafa como un delito material y de resultado, lo que implica que para que se consuma requiere de un "resultado", el que será la producción de un perjuicio en el patrimonio de la víctima o de un tercero. Esto no implica, sin embargo, que el autor obtenga algún tipo de lucro (Vaninetti, 2017).

Ahora bien, en relación con la estafa informática se la identifica con "la producción de un daño patrimonial cuantificable mediante un comportamiento externo, impropio de un proceso automatizado informático, que altera los datos gestionados por éste, con ánimo lucro y en perjuicio de tercero" (Abogados portaley, 2013, p.1).

Puntualmente respecto de la estafa en Internet, Vaninetti (2017) afirma que los delitos informáticos son "todas aquellas conductas criminógenas que se realizan valiéndose de herramientas de manejo automático de la información y/o tecnologías de la comunicación" (p.2). A esto agrega que las defraudaciones en el ámbito de la red son una de las formas delictivas más frecuentes en Internet.

Asimismo, según este doctrinario existen dos tipos de "estafadores virtuales":

1. Aquellos cuyas maniobras delictivas son más tradicionales y no requieren demasiados conocimientos de informáticas, quienes quedan comprendidos dentro del artículo 172 del Código Penal. Estos son los casos de subastas on line, oportunidades de negocios e inversiones, ventas piramidales, pedidos de donaciones, promoción de viajes, etc. Este tipo de sujeto activo solamente necesitará saber conceptos básicos como navegar por internet, utilizar el mail, entre otros (Vaninetti, 2017).

2. Aquellos que poseen altos conocimientos (profundos y específicos) de utilización de la red, por lo que sus actos de defraudación quedan comprendidos en el artículo 173 inciso 16 del Código Penal. Estas personas manipulan sistemas de procesamiento de datos a la distancia, despliegan técnicas y procedimientos de distinta complejidad, entre los que se pueden mencionar:

> (…) el phishing, el pharming o creación de una página falsa (por ejemplo, simulando a la web de una entidad bancaria), dispositivos sniffing que capturan los datos en redes wifi sin introducirse a una terminal, mediante keylogger que es un software malicioso que registra todos los logs que un usuario realiza en su teclado, entre otras prácticas (Vaninetti, 2017, p. 2).

Asimismo, el Código Penal regula en su capítulo IV titulado "estafas y otras defraudaciones" estas conductas que menoscaban los bienes e intereses de terceros. Puntualmente en el artículo 172 se contempla:

> ARTICULO 172. - Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.

Este artículo transcripto contiene la disposición general, a lo que se le suman los casos especiales de defraudación cuya pena es aquella dispuesta en el mismo artículo 172. De esta manera, en el artículo 173 del Código Penal se mencionan las distintas estafas, entre ellas se expresa: "(…) 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. (Inciso incorporado por art. 9° de la Ley N° 26.388, B.O. 25/6/2008)".

Tal como se observa la ley 26.388 que agrega los delitos informáticos al Código Penal argentino ha sumado como tipo especial de estafa a la estafa informática y la ha definido como aquella manipulación que altere el funcionamiento normal de un sistema informático o la transmisión de datos.

De esta manera “el engaño o ardid y el error de la figura clásica de la estafa es reemplazada en la figura del 173 inciso 16 por la manipulación informática ante las particularidades del medio que se emplea” (Vaninetti, 2017, p. 3).

Para finalizar debe destacarse que el tipo penal de estafa es un delito que indudablemente afecta la propiedad, ya que lo se penaliza no es el engaño sino el daño patrimonial que se ocasiona, incluso a pesar de que el medio utilizado pueda causar daño a otro bien jurídico (Vaninetti, 2017). En efecto, no en vano el propio Código Penal argentino ha incluido a la estafa en el Título VI denominado "Delitos contra la propiedad".

2.2 Fraude

El fraude queda contemplado dentro del ordenamiento jurídico argentino vigente, más precisamente dentro del Código Penal argentino, en el Capítulo IV del libro II que comprende a los delitos contra la propiedad.

En el artículo 173 del Código Penal se incluye al fraude como una especie dentro del género de la estafa (artículo 172). Al respecto, afirma el Dr. Núñez que:

> (…) el fraude es el medio propio de la estafa, el que consiste en la inducción mantenimiento o reforzamiento de otro en un error sobre un hecho o circunstancia, que lo determina a hacer la disposición patrimonial perjudicial para él o para un tercero respecto de cuyo patrimonio tiene poder legal para disponer. (Tobares Catalá y Castro Arguello, 2010, p.175).

Es decir, a través del fraude electrónico se logra que una persona se vea perjudicada mientras que otra se beneficia de este acto que ha realizado y que incrementa su patrimonio de manera ilegal.

Puntualmente se define al fraude electrónico como aquel acto en el que a través del uso de una computadora se distorsionan datos para inducir a otra persona a que haga o deje de hacer algo que ocasiona una pérdida. Esto puede realizarse de distintas maneras: una de ellas, mediante la alteración –sin la debida autorización- de los datos ingresados en la computadora con el objetivo de malversar fondos, tal como suele suceder en las organizaciones cuando sus empleados utilizar la modificación de datos con este propósito. Otra manera de cometer fraude es mediante la eliminación o alteración de información almacenada. Finalmente, suele ocurrir que los delincuentes realicen compras no autorizadas con tarjetas de crédito. A esto lo logran a través de

los códigos de software que cargan en la computadora central de un banco para que éste les suministre las identidades de los usuarios (Legal Information Institute, s/f).

El fraude puede implicar la manipulación, falsificación o alteración de registros o documentos; la malversación de activos; la supresión u omisión de los efectos de ciertas transacciones en los registros o documentos; el registro de transacciones sin sustancia o respaldo y hasta la mala aplicación de políticas contables (Seguridad informática, 2007).

Ahora bien, en cuanto a su recepción legal, tal como se ha afirmado el artículo 173 del Código Penal expresa:

> ARTÍCULO 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece: (…)
> 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. (Inciso incorporado por art. 9° de la Ley N° 26.388, B.O. 25/6/2008)

En este sentido, la doctrina afirma que este artículo 173 combina tipos especiales de estafa (incisos 1°, 3°, 4°, 5°, 6°, 12° y 13°) con los denominados abusos de confianza (de los incisos 2°, 7°, 11° y 14°). Con el surgimiento de las leyes n° 25.930 y 26.388 se agregaron las defraudaciones con tarjetas de compra, crédito o débito y las defraudaciones con medios informáticos respectivamente. Al respecto se afirma que en todos estos supuestos se torna necesario -tal como en el caso de la estafa del artículo 172- el engaño, el error de la víctima, la disposición patrimonial y el perjuicio económico de la víctima (Rodríguez, 2013).

Este tipo penal, según afirma el autor citado, se ubica dentro de la estafa ya que la acción típica es defraudar a otro mediante un perjuicio patrimonial. Sin embargo, lo que conserva como característica de la estafa del artículo 172 es el desplazamiento patrimonial perjudicial. En este tipo de estafa no existe un engaño o ardid sobre la víctima para obtener la transferencia, sino que el delincuente recurre a la manipulación de sistemas informáticos y altera el normal funcionamiento de éstos o la transmisión de datos y provoca como consecuencia el traslado de bienes en beneficio suyo o de terceros (Rodríguez, 2013).

En este entendimiento se destaca que para configurarse la estafa informática debe necesariamente alterarse el normal funcionamiento del sistema informático o la transmisión de datos; ya que no se tipifica esta acción cuando la transferencia o disposición patrimonial es ejecutada por la propia víctima que se encuentra engañada por el autor a través de medios

informáticos. De hecho, en este último caso se trataría de una estafa del artículo 172 (Rodríguez, 2013). Esto quiere decir que:

> (…) estas figuras se reservan a los casos de desplazamientos patrimoniales efectuados con la ignorancia de su titular, al que, con su desconocimiento se le manipulan los datos o el sistema, no a casos en que la informática es uno de los medios con que se fraguó el ardid o engaño (Rodríguez, 2013, p.31).

Como se observa se destacan aquí aquellos casos en los que la persona víctima realiza alguna operación electrónica que resulta perjudicial para su patrimonio, ya que éstos no constituyen fraudes informáticos, sino que se encuadran dentro de la categoría clásica de la estafa. En realidad, para que la acción sea considerada fraude electrónico debe concretarse el traslado patrimonial con el total desconocimiento del autor y mediante la modificación o alteración de datos en operadores electrónicos.

2.3 Sabotaje informático

En cuanto a la enunciación de los delitos informáticos más frecuentes que se brinda en estos apartados, se destaca que el delito de sabotaje es uno de los que quedan comprendidos dentro de los conocidos delitos de daños informáticos.

Sáez Capel (2001) define al término sabotaje informático como "(…) todas aquellas conductas dirigidas a atacar los sistemas informáticos, ya sea que se dirijan a causar daños en el hardware o en el software" (p.124). A lo que este autor suma que los daños causados pueden ser cometidos por sujetos extraños a la empresa o administración pública de que se trate o por los propios empleados de ésta.

En este sentido, cuando los daños son cometidos por personas ajenas a la propia organización, se brinda como ejemplo el "ataque llevado a cabo con explosivos contra el centro informático de la Wets German MANCompany, en 1983, por terroristas que protestaban contra la participación de esta compañía en la producción de misiles Pershing y Cruis" (Sáez Capel, 2001, p. 125). Mientras que cuando estas conductas son llevadas a cabo por personal de la propia empresa se menciona a modo de ilustración los casos de conflictos laborales o sociales dentro de la misma compañía. De hecho, los estudios sobre la temática afirman que el 60% de los casos de sabotaje son realizados por sujetos dentro de las empresas.

Puntualmente este tipo delictivo consiste en borrar, suprimir o modificar sin autorización funciones o datos de la computadora con intención de obstaculizar el funcionamiento normal del sistema. Algunas modalidades que adquiere son los virus, gusanos, acceso no autorizado a sistemas o servicios, espionaje y reproducción no autorizada de programas informáticos (piratería) (Pullido, 2012).

Este delito queda comprendido dentro del Código Penal argentino en el artículo 183, Capítulo VII- modificado por ley 26.388- que contempla a los daños. Se expresa textualmente:

> Artículo 183. - Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Tal como se observa se ha contemplado en este artículo la alteración o modificación de sistemas informáticos, lo que permitiría afirmar que el sabotaje informático quedará comprendido dentro de esta norma y consecuentemente su pena será de prisión de hasta un año.

De esta manera, al contemplar esta conducta dentro del capítulo de daños vale la aclaración de que aquí el daño se aleja de la tradicional noción de destrucción física permanente de la cosa. De hecho, “Los daños informáticos podrán producirse, entonces, por destrucción de los datos, de su interconexión lógica, de su accesibilidad, etc.” (Van den EyndeAdroer, 2015, p.1).

Al respecto agrega el citado autor que la conducta de sabotaje debe ser grave y esto se deberá evaluar a través de la pérdida de funcionalidad del objeto del delito, para lo que no debe confundirse el daño directo con el perjuicio ocasionado.

2.4 Ciberterrorismo

El Ciberterrorismo es un concepto que se utiliza para hacer referencia a distintos ataques en contra de las comunicaciones, la información y de los sistemas informáticos que la contienen. Más precisamente, se agrega una definición otorgada por Mark Pollit -agente del FBI que se dedicó a estudiar el tema- quien expresa: "El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de

computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos" (Massana, 2002, p.12).

Asimismo, entre los objetivos de este tipo delictivo y con la clara intención de anularlos de manera temporal o definitiva, se mencionan:

> (…) las comunicaciones estratégicas, los sistemas de salud, el control aéreo, la videovigilancia, los transportes con sistema computarizado, las armas controladas por sistemas de cómputo, la georreferenciación de vehículos, los objetos que requieren de conexión a la red, las propias redes sociales, los bancos de datos, los sistemas financieros, la telefonía, los mensajes de texto, internet, etc." (Nava Garcés, 2017, p.1).

Tal como se observa el ciberterrorismo se identifica con actos terroristas -como su nombre lo indica- pero cometidos mediante el uso de la informática; esto implica pues que su propósito al igual que el terrorismo se vincula en la mayoría de los casos con cuestiones políticas.

En este sentido la doctrina expresa que las ventajas del ciberterrorismo si se compara con el terrorismo tradicional, es que el primero no conlleva riesgo físico alguno para quien comete el acto (terrorista) ya que éste se encuentra en un ámbito geográfico de actuación distinto al lugar en donde se halla el objetivo o víctima. Sumado a lo dicho, otra ventaja se asocia con la gran repercusión de las acciones. Esto es así puesto que cualquier actuación sobre Internet tiene un amplio e inmediato eco en los medios y con ello un efecto propagandístico evidente. Mientras que por último se destaca que la relación coste-beneficio resulta óptima (Gil, 2011).

Ahora bien, en cuanto a la legislación de esta conducta delictiva, no existe legislación específica en Argentina que contemple al ciberterrorismo. No obstante, lo dicho el artículo 183 del Código Penal que ha sido trascripto en oportunidad de analizar el sabotaje informático también permite incluir los actos aquí tipificados. De hecho, la doctrina expresa que el ordenamiento penal enuncia ciertas conductas que se agravan cuando afectan los servicios públicos y allí justamente es donde se lo puede ubicar al ciberterrorismo (Ciber derecho, 2015).

En este entendimiento se afirma:

> Así en el artículo 183 se reprime el #craking y el #malware al castigar al 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. No obstante, la pena prevista que es de prisión de quince días a un año, en el artículo siguiente se agrava a prisión de 3 meses a 4 años si el delito es ejecutado en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público (Ciber derecho, 2015, p.1).

Como consecuencia resulta posible destacar la necesidad de contar con leyes que contemplen los ataques ciberterroristas y los delitos informáticos, lo que debería ocurrir en el corto plazo en países como Argentina con el propósito de evitar cualquier inconveniente en los sistemas críticos de información, tal como lo han recomendado especialistas en la temática provenientes de los Estados Unidos.

Justamente las recomendaciones de quienes conocen en profundidad el tema de los delitos informáticos se vinculan con la urgente aplicación de leyes que permitan prevenir y neutralizar los ilícitos cometidos mediante el uso de las tecnologías como Internet o de los sistemas de comunicación informáticos. Al respecto, la Organización de Estados Americanos (OEA), con el objetivo de colaborar con el combate del ciberterrorismo en países latinoamericanos, impulsa acciones conjuntas y de cooperación. Sin embargo, hasta el momento Estados Unidos es uno de los únicos países con la tecnología y los conocimientos más avanzados en materia de ciberterrorismo; no sólo en lo teórico sino también en cuanto a la legislación que permite condenar estos delitos. [4]

Como conclusión se torna necesario encontrar una forma de abordar la dimensión transnacional del delito cibernético y mejorar la cooperación internacional a través del desarrollo y normalización de la legislación pertinente (Altmark y Molina Quiroga, 2012).

2.5 Calumnias e injurias

En busca de una definición de calumnia las fuentes doctrinarias coinciden en afirmar que calumnia es toda "acusación, imputación, carente de verdad que se vierte sobre alguien con la clara misión de provocarle un daño". A lo que se agrega que esta falsa acusación sobre una persona se vincula con un delito que se asegura que ha cometido, aunque realmente esto no sea cierto, ya que puede que no exista ese delito o no haya sido esa persona quien lo cometió (Definición ABC, s/f).

Puntualmente se expresa: "La calumnia es la falsa imputación de un delito que dé lugar a acción pública. Por ejemplo, decir que alguien es un ladrón, maltratador o estafador, etc." (González, 2008, p.1). Asimismo, agrega el autor que esta acción de deshonra -afectación del

[4] Fuente: Especialistas piden leyes contra el ciberterrorismo. (31/07/03). *El Día.com*. Recuperado el 11/07/18 de https://www.eldia.com/nota/2003-7-31-especialistas-piden-leyes-contra-el-ciberterrorismo

honor de la persona que se pretende perjudicar- es realizada con el conocimiento de que lo que se dice es falso.

Por otro lado, la injuria es otro delito que se asocia con el menoscabo hacia el honor de una persona. Es definida como aquella acción de lesionar "(…) la dignidad de una persona perjudicando su reputación, o atentando contra su propia estima, al imputarle un hecho o cualidad en menoscabo de su fama o autoestima" (Legalium, 2016).

Al igual que la calumnia, con la injuria se atribuyen hechos inciertos o se formulan juicios de valor sobre alguien con el propósito de deshonrar o desacreditar a una persona. Sin embargo, la diferencia es que la primera requiere de la imputación falsa de un delito, mientras que la injuria no son conductas tipificadas penalmente.

Ahora bien, en cuanto a estas figuras penales como delitos informáticos, se destaca que Internet es el medio de comisión más frecuente de estas conductas. De hecho, se ofrece allí la posibilidad de que las personas se expresen con gran libertad, de manera fácil, accesible y cómodamente a través de la publicación de contenidos en páginas web, en redes sociales, en foros, en correos, etc.

No obstante lo dicho, esta libertad en conjunto con el anonimato que aporta muchas veces la Red ha contribuido a la comisión de estas conductas ilícitas que perjudican los derechos de otras personas (Abogados porta ley, 2013).

En este entendimiento la doctrina expresa que con el paso de los años y con el surgimiento de las nuevas tecnologías se han originado nuevos modos de injurias, de las más varias e ingeniosas. Se afecta así de manera infrenable a la persona, no sólo en sus relaciones sociales, calidades éticas y morales, sino también en las relaciones profesionales que ella tiene; lo que le dificulta encontrar una forma de evitarlas y de conseguir protección (Tobares Catalá y Castro Arguello, 2010).

2.6 Espionaje informático

El espionaje informático es otra de las figuras comprendidas dentro de los delitos informáticos que consiste en la violación de la reserva o del secreto de la información de un sistema, a través de la obtención sin la debida autorización de datos almacenados en un fichero automatizado. A modo de ejemplo, se menciona la intercepción de la información que circula en

línea a través de las líneas telefónicas, también el acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e incluso la interceptación de correo electrónico (Tobares Catalá y Castro Arguello, 2010).

El cuanto a su regulación normativa podría decirse que este delito se contempla en el artículo 224 del Código Penal, el que textualmente reza:

> Será reprimido con prisión de seis meses a dos años, el que indebidamente levantare planos de fortificaciones, buques, establecimientos, y vías u otras obras militares o se introdujere con tal fin, clandestina o engañosamente en dichos lugares, cuando su acceso estuviere prohibido al público.

Sin embargo, a pesar de que exista esta regulación, queda en evidencia el vacío normativo respecto de los sucesos en los que se encuentren involucrados sistemas informáticos a nivel gubernamental o comercial e industrial. De hecho, se debe tener en cuenta que en la actualidad las alternativas mencionadas por el citado artículo pueden estar registradas en soportes magnéticos o digitales, interconectados a la Internet, lo que permite su vulneración incluso sin hallarse físicamente en los establecimientos mencionados por dicha norma, ni con la necesidad de estar en el mismo país (Tobares Catalá y Castro Arguello, 2010).

Asimismo, la doctrina enuncia que se han utilizado para el espionaje de las más diversas herramientas y artefactos, entre ellas: tintas invisibles, micrófonos, grabadoras y micro cámaras. Sin embargo, los más empleados actualmente son las computadoras y los dispositivos móviles que graban video, audio, ubicaciones, y datos (Fernández, 2017).

En este sentido, resulta posible afirmar que cualquier persona que acostumbre a navegar por Internet o a utilizar el correo electrónico puede ser víctima de espionaje, incluso aunque no lo percate. Como ya se ha dicho, los avances de la tecnología no siempre son utilizados para realizar buenas obras, siempre existen quienes los utilizan en perjuicio de otros y para beneficio propio. Al respecto se agrega:

> La aparición en el mercado de nuevas técnicas y programas, difundidos en su mayor parte a través de Internet, posibilitan la recogida de información privada de un determinado usuario, sin dejar de mencionar aquellos programas que reconfiguran parámetros de los ordenadores aprovechándose del desconocimiento de las personas en el campo de las nuevas tecnologías (Porta ley, s/f, p.1).

Sumado a lo dicho, las fuentes doctrinarias mencionan diferentes técnicas para la comisión del espionaje electrónico, se mencionarán a continuación alguna de ellas:

Dialers: marcador que provoca que la conexión a Internet se realice a través de un número de tarificación especial y no de la manera indicada por el operador con el que se haya contratado dicha conexión.

Adware: programas que recogen o recopilan información sobre los hábitos de navegación del usuario y, por ejemplo, con propósitos publicitarios se logra determinar información que indiquen las conductas frecuentes de los internautas.

Programas de acceso remoto: programas que acceden a la computadora de otra persona para atacar o alterar sus datos. Son fácilmente reconocibles por los antivirus.

Caballos de Troya: programa que una vez instalados en la computadora genera daños o pone en peligro la seguridad del sistema.

Virus o gusanos (worms): programas o códigos que provocan daños en el sistema, tales como alteración o borrado de datos, y que se propagan a otros ordenadores a través de la Red, del correo electrónico, etc.

Programas de espionaje o spyware: programas que registran todo lo que se realiza en una pc. Se utiliza para obtener información confidencial o conocer cuál es el funcionamiento de una determinada computadora (Porta ley, s/f).

2.7 Otros delitos informáticos conocidos

2.7.1 Amenazas y coacciones por internet

El delito de coacciones consiste en impedir a otra persona que realice algo que la ley no prohíbe, u obligar a que haga algo que simplemente no desea hacer. Aquí no interesa si el hecho es justo o injusto, sino que importa la obligación de hacer que alguien haga lo que no deseaba. Es decir, se destaca la anulación de la capacidad de obrar libremente de la persona afectada. “Así, el delito de coacciones se perfila como un delito contra la libertad de las personas, y más concretamente, como un atentado contra su libertad de obrar” (Alfocea, 2016, p.1).

Mientras que el delito de amenazas es aquel que “(…) atenta contra el derecho de las personas a no ser víctimas de actos susceptibles de alterar su tranquilidad espiritual, produciéndose inquietud y temor” (Tobares Catalá y Castro Arguello, 2010, p. 226).

De esta manera, la marcada diferencia entre las coacciones y las amenazas es que en las primeras se actúa sobre la víctima y sus acciones mientras que las amenazan se ejercen sobre los pensamientos o motivaciones de las personas.

2.7.2 Robo de identidad

La utilización de datos personales en la Red lleva implícita la posibilidad de ser víctima de un tipo de ciberdelito de los más extendidos: el robo de identidad. Al respecto, el aporte de información personal sensible como por ejemplo datos de cuentas bancarias y tarjetas de créditos conlleva la amenaza de caer presa de ciberdelincuentes, quienes buscan obtener beneficios propios a través de la información privada de las demás personas (Alfocea, 2015).

> Una fase avanzada de robo online es el robo de identidad que ocurre cuando alguien se apropia de los datos de acceso (usuario y contraseña) a nuestro correo electrónico, cuentas de redes sociales, etcétera y actúa en nuestro nombre dañando así nuestra reputación online además de poder provocar de nuevo importantes pérdidas económicas (Alfocea, 2015, p.1)

Por último, se destaca la dificultad en lograr descubrir a los delincuentes en estos tipos de delitos justamente por la posibilidad que brindan las redes de actuar bajo la protección del anonimato.

3. Clasificaciones de los delitos informáticos

Sin dudas existen diversas clasificaciones de delitos informáticos, no obstante, ello aquí se aporta aquella brindada por Julio Téllez Valdés (2008, quien los divide en base a dos criterios: como instrumento o medio y como fin u objetivo.

3.1 Como instrumento o medio

En esta categoría se encuentran las conductas criminales que utilizan a las computadoras como método, medio o símbolo en la comisión del ilícito, entre ellas, la falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.); la modificación de los estados contables de las empresas; el planeamiento o simulación de delitos comunes como robos, homicidios, etc.; la revisión, sustracción o copiado de información de carácter confidencial; la

violación de códigos para entrar a un sistema; la desviación de cantidades de dinero hacia una cuenta bancaria apócrifa; el uso no autorizado de programas de cómputo, la alteración de los sistemas a través de virus informáticos, entre otros tantos ejemplos en los que el uso de las tecnologías sirven como medios para la comisión del delito (Téllez Valdés, 2008).

Es decir, respecto a esta clasificación se sostiene que los delitos informáticos se denominan como tal porque se utiliza a la tecnología como instrumento para lograr determinado resultado. A modo de ejemplo se hace referencia al uso de las computadoras para lograr falsificaciones de documentos de uso comercial.

> Las fotocopiadoras computarizadas en color a base de rayos láser dieron lugar a nuevas falsificaciones. Estas fotocopiadoras pueden hacer copias de alta resolución, modificar documentos, crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos (Téllez Valdés, 2008, p.190).
>
> .

3.2 Como fin u objetivo

El citado autor afirma además que los delitos informáticos pueden clasificarse como de fin u objetivo cuando las conductas criminales van dirigidas directamente contra las computadoras, accesorios o programas como entidad física. En esta clasificación se incluye por ejemplo a: la programación de instrucciones que producen un bloqueo total al sistema; la destrucción de programas por cualquier método, los daños a los dispositivos de almacenamiento; el atentado físico contra la computadora; el sabotaje político o terrorismo; el secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.) (Téllez Valdés, 2008).

3.3 Otras clasificaciones

Dentro de lo que se conoce como otras clasificaciones se pueden nombrar distintas maneras de agruparlos, según la doctrina o fuente que lo haya hecho. Así de acuerdo al “Convenio sobre la Ciberdelincuencia” de 1 de Noviembre de 2001 surge la clasificación siguiente (Nelguard, s/f):

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: que comprende el acceso ilícito a sistemas informáticos, la Interceptación ilícita de datos informáticos, la interferencia en el funcionamiento de un sistema informático, el abuso de dispositivos que faciliten la comisión de delitos. Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.
- Delitos informáticos: dentro de los cuales se contempla a la falsificación informática mediante la introducción, borrada o supresión de datos informáticos; y al fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos. El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.
- Delitos relacionados con el contenido: que contempla aquellos delitos de producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines: entre ellos la copia y distribución de programas informáticos, o piratería informática (Nelguard, s/f)

En este orden de ideas, otra clasificación es aquella que proviene de la página de la Brigada de Investigación Tecnológica de la Policía Nacional Española

- Ataques que se producen contra el derecho a la intimidad: Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos.
- Infracciones a la Propiedad Intelectual: especialmente la copia y distribución no autorizada de programas de ordenador.
- Falsedades: falsificación de moneda a las tarjetas de débito y crédito.
- Sabotajes informáticos: daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos.
- Fraudes informáticos: estafa mediante la manipulación de datos o programas para la obtención de un lucro ilícito.
- Amenazas.

- Calumnias e injurias: Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión.
- Pornografía infantil: inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz, entre otros (Nelguard, s/f).

Por otro lado, la doctrina brinda otra clasificación, aquella sostenida por el político y abogado Jorge Pacheco Klein, quien distingue a los delitos informáticos entre:

1. Delitos informáticos internos. Ej.: sabotaje de programas.
2. Delitos a través de las telecomunicaciones. Ej.: hacking.
3. Manipulación de computadoras. Ej.: apropiación indebida, peculado y fraudes informáticos. Es la más vinculada a delitos de cuello blanco.
4. Utilización de computadoras en apoyo a empresas criminales, como el lavado de dinero y la distribución ilícita de drogas.
5. Robos de software (piratería). (Viega Rodríguez, 2011, p.4)

Asimismo, la Organización de las Naciones Unidas (ONU) ha reconocido a los delitos informáticos y también ha adoptado un criterio propio para clasificarlos en diferentes títulos que comprenden distintos tipos delictivos, tal como se enuncia a continuación (Estrada Garavilla, 2008):

A. Fraudes cometidos mediante manipulación de computadoras.

En este subtítulo queda incluida la manipulación de los datos de entrada (sustracción de datos- fraudes informáticos); la manipulación de programas (modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Ej. Caballo de Troya); la manipulación de los datos de salida, por ejemplo, el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

A esta categoría de delitos se suma el fraude efectuado por manipulación informática, que consiste en la denominada técnica del salchichón ya que se habla de "rodajas muy finas" apenas perceptibles de transacciones financieras. Es decir, se extrae dinero de manera repetitiva de una cuenta y se transfieren a otra.

B. Falsificaciones informáticas.

Bajo el título de falsificaciones la Organización de las Naciones Unidas comprende a todas las operaciones que se utilizan como objeto (esto quiere decir cundo se alteran datos de los documentos almacenados en forma computarizada) o como instrumentos (ya que las

computadoras se utilizan para efectuar falsificaciones de documentos de uso comercial); tal como se analizó en la clasificación pertinente al punto 3.1 y 3.2 de este trabajo.

C. Daños o modificaciones de programas o datos computarizados.

Ahora bien, dentro de esta clasificación se comprende al sabotaje informático que ya se ha definido con anterioridad, dentro del que se incluyen: a los virus (como aquella serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos); a los denominados gusanos (se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse); a la bomba lógica o cronológica (programación de la destrucción o modificación de datos en un momento dado del futuro).

Sumado al sabotaje informático, dentro de este apartado se comprende también al acceso no autorizado a servicios y sistemas informáticos, lo que se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Por otro lado, también se incluye aquí a la reproducción no autorizada de programas informáticos de protección legal, lo que puede significar una gran pérdida económica para los propietarios legítimos. Sin embargo, algunos autores afirman que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual (Estrada Garavilla, 2008).

Finalmente, sólo resta aclararse que, tal como se puede observar, todas estas clasificaciones provienen de doctrinarios pertenecientes al derecho comparado ya que en Argentina la materia en cuestión- el estudio de los delitos informáticos- es de reciente data y aún no se cuenta aquí con suficiente material específico para el desarrollo exhaustivo de estos conceptos.

Conclusiones parciales

En este segundo capítulo se ha desarrollado el análisis doctrinario de los principales delitos informáticos. Se hizo especial hincapié en brindar los conceptos que permiten identificar cada uno de ellos y distinguirlos entre sí. Así como también se exploraron las distintas clasificaciones que la doctrina ha enunciado para agrupar a estas conductas delictivas. Se ha podido observar en este

apartado la necesaria utilización de fuentes extranjeras para la redacción de los temas aquí analizados, lo que acredita una vez más que en Argentina la temática en cuestión aún no encuentra el debido tratamiento doctrinario, legislativo ni jurisprudencial.

Al clasificar los delitos, se ha utilizado doctrina de España, de México e incluso de la propia Organización de las Naciones Unidas, ya que se ha explorado la doctrina argentina y nada se ha hallado al respecto. Esto nuevamente demuestra el escaso tratamiento específico en materia de delitos informáticos en este país.

Ahora bien, al inicio de esta investigación se planteó como hipótesis que mediante la ley 26.388 que modifica el Código Penal argentino pareciera no haberse logrado adecuar las normas internas a los parámetros internacionales de regulación y control de los delitos informáticos.

Indudablemente aquí surge con evidencia la carencia de leyes específicas que contemplen las principales figuras delictivas en el campo de la informática. Se ha podido describir a estos delitos, pero no existe legislación especializada que los contemple y que posibilite determinarlos con precisión. De hecho, si se compara la regulación de estas figuras en Argentina con los parámetros internacionales sobre delincuencia informática, aún se observa un largo trecho que este país debe recorrer para alcanzarlos.

En este sentido no se discute que el ordenamiento jurídico argentino ya ha logrado con la sanción de la ley 26.388 un avance en materia de delitos informáticos; sin embargo, aún queda mucho trabajo por delante.

Se estudiará a continuación la recepción legislativa que el derecho internacional ha otorgado a los delitos informáticos para poder conocer aquellas normas que este país debería imitar o a las que debería, si aún no lo ha hecho, adherir.

CAPÍTULO III

ANÁLISIS LEGISLATIVO DEL DERECHO INTERNACIONAL SOBRE DELITOS INFORMÁTICOS

Introducción

En este tercer capítulo se estudiará el análisis legislativo de los delitos informáticos en el derecho comparado. Puntualmente se analizará su recepción legal en los tratados internacionales, para lo que se indagará lo contemplado por la Organización de las Naciones Unidas y por la Unión Europea sobre delitos informáticos. Es decir, se analizará lo expresado en los Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal y lo dispuesto en el Convenio de Budapest.

Asimismo, en este capítulo se estudiarán las normas de algunos países extranjeros que se destacan por haber incorporado en su legislación interna la protección, prevención y/o reparación de las consecuencias que originan los delitos informáticos. Entre ellos, se analizará la regulación de Estados Unidos, Francia, Alemania, Reino Unido, España y Venezuela.

1. Recepción legislativa de los delitos informáticos en tratados internacionales

A continuación se analizará lo contemplado por la Organización de las Naciones Unidas y por los Convenios de la Unión Europea sobre todo lo vinculado con los delitos informáticos.

1.1 La Organización de las Naciones Unidas (ONU)

"Durante más de medio siglo, las Naciones Unidas han celebrado congresos destinados a fortalecer la cooperación internacional contra la expansión de la delincuencia" (Oficina de las Naciones Unidas contra la Droga y el Delito, 2010, p.1).

Esta organización desde el año 1945 lucha por los problemas que enfrenta la humanidad en el siglo 21, entre ellos por los derechos humanos, la paz, la seguridad, el cambio climático, el terrorismo, las emergencias humanitarias, la salud, entre otros tantos conceptos de vital importancia.

Dentro de sus debates se han organizado congresos quinquenales que repercuten en las políticas de la justicia penal y en los procedimientos nacionales y en las prácticas profesionales de todo el mundo. Se afirma al respecto que actualmente estos congresos adquieren importancia decisiva debido a que los problemas contemporáneos entre los que se incluye a la delincuencia

requieren de urgente colaboración internacional (Oficina de las Naciones Unidas contra la Droga y el Delito, 2010).

De esta manera, se continuará con la descripción de los principales congresos que han tenido lugar dentro del marco de la ONU y de sus políticas de actuación.

1.1.1 Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal

Afirma la doctrina que luego de la disolución de la Comisión Internacional Penal y Penitenciaria después de la Segunda Guerra Mundial, las funciones de este organismo fueron transferidas en 1950 a las Naciones Unidas. Ente ellas se incluían celebrar conferencias internacionales vinculadas con la lucha contra la delincuencia cada cinco años. De esta manera, se conoce que el primer Congreso de las Naciones Unidas se celebró en Ginebra en 1955 (Oficina de las Naciones Unidas contra la Droga y el Delito, 2010).

Cuando se realiza un repaso por los diferentes congresos de la ONU se parte del primero de ellos celebrado, tal como se dijo, en Ginebra en 1955. Allí se establecieron las reglas mínimas que permitieron el trato con los reclusos y entre ellas se contempló la administración general de los establecimientos penitenciarios.

Luego, en 1960 en Londres se celebró el segundo congreso en donde se decidió la implementación de servicios especiales de policía para la justicia de menores. Así, cada cinco años se continuó con la celebración de los distintos congresos vinculados con la prevención de la delincuencia y algún aspecto en particular como el desarrollo social, la calidad de vida, la paz, la justicia, entre otros (Oficina de las Naciones Unidas contra la Droga y el Delito, 2010).

Finalmente, se destaca dentro de los temas políticos de discusión de la Organización de las Naciones Unidas que han adquirido gran importancia en su agenda internacional a todo lo relacionado con los delitos cometidos mediante el uso de la tecnología y las redes informáticas (Altmark y Molina Quiroga, 2012).

De esta manera, recién en el Octavo Congreso sobre Prevención del Delito y Justicia Penal celebrado en La Habana, Cuba, se afirmó que el mayor conflicto presentado por la aplicación de las TIC’s en la sociedad se encontraba relacionado con la reproducción y difusión no autorizada de programas informáticos, así como el uso indebido de cajeros automáticos. A esto se agrega que para aquellos tiempos (1990) aún no existían los delitos que se conocen actualmente. Sin embargo,

ya se podía observar desde allí que la delincuencia, con sus dimensiones internacionales iba en alarmante aumento (Oficina de las Naciones Unidas contra la Droga y el Delito, 2010). En realidad, en esta reunión lo que se procuró es buscar medidas de prevención que sirvieran también para evitar el aumento de los delitos informáticos. Asimismo, se afirmó que:

> (…) el uso irresponsable de la red y los equipos informáticos podría traer consecuencias desastrosas; por tal razón, se aconsejó el establecimiento de normas y directrices sobre la seguridad informática, con la finalidad de ayudar a la comunidad internacional a hacer frente a la nueva forma de delincuencia de guante blanco (Altmark y Molina Quiroga, 2012, p.153).

Por otro lado, en el seno de la Organización de las Naciones Unidas (ONU) y en el marco de este Octavo Congreso sobre Prevención del Delito y Justicia Penal se consideró que el mayor empleo del proceso de datos en las economías y burocracias de los distintos países ha generado la delincuencia relacionada con la informática.

En este sentido, a pesar de que como se dijo en aquel entonces aún no existían la cantidad de delitos informáticos que hoy en día se conocen, ya se pudo detectar que un gran número de este tipo de delitos no se encontraba regulado. Así, "(…) en vista de que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas" (Estrada Garavilla, 2008, p.3).

Como consecuencia, el Congreso recomendó el establecimiento de normas y pautas vinculadas con la seguridad de las computadoras para colaborar con la comunidad internacional y combatir estas nuevas formas de delincuencia. Al respecto, las Naciones Unidas para la Prevención y Control de Delitos Informáticos ha afirmado que estos delitos constituyen una nueva modalidad de crimen trasnacional y que por lo tanto su combate requiere de una eficaz cooperación internacional.

En este sentido, la ONU enuncia ciertos problemas vinculados con la cooperación internacional en materia de delitos informáticos; entre ellos expresa:

> a) Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos. b) Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas. c) Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos. d) No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos. e) Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras. f) Ausencia de tratados de extradición, de acuerdos de ayuda

> mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional. (Estrada Garavilla, 2008, p.3).

Tal como se puede observar, la Organización de las Naciones Unidas ha demostrado interés en el combate de este tipo de delitos; de hecho, desde 1955 se han organizado diferentes congresos dedicados al estudio de medidas apropiadas para frenar con la delincuencia en general.

Esto permite concluir que los organismos internacionales – a diferencia de las legislaciones internas de algunos países como Argentina- desde hace tiempo ya se han esforzado para encontrar los mecanismos idóneos que permitan dar lucha a los delitos generados con las nuevas tecnologías.

Por último, dentro de los aspectos a destacar de la ONU se menciona a la Comisión de Prevención del Delito y Justicia Penal. En la 19ª Sesión de esta Comisión que se celebró en Viena, Austria, entre 17 y 21 de mayo se estableció como desafío el "(…) garantizar que los países tengan leyes, conocimientos y herramientas necesarias para una justicia apropiada al siglo XXI" (Oficina de las Naciones Unidas contra la Droga y el Delito, 2010, p.1).

Tal como se observa, la ONU se preocupa por la correcta actualización de las legislaciones internas de los países miembros en concordancia con la situación actual que se vive. La justicia de cada país debe ser apropiada para hacer frente a los problemas de este siglo, por lo que indudablemente el tratamiento de los delitos informáticos debe quedar comprendido dentro de las normas de un país. La nueva era tecnológica genera una urgente adaptación en el derecho para evitar o combatir situaciones provocadas por la informática.

Esta Comisión tuvo como uno de sus propósitos analizar la manera adecuada para controlar el seguimiento de lo debatido en el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en Salvador, Brasil, entre 12 y 19 de abril de 2010. De hecho, se aprobó una resolución que creaba grupos de expertos para que estudien la delincuencia cibernética y sus problemas y para que revisen las normas mínimas de las Naciones Unidas para el tratamiento de los reclusos. Asimismo, se realizó una convocatoria para mejorar la eficiencia de los próximos Congresos sobre la delincuencia (Oficina de las Naciones Unidas contra la Droga y el Delito, 2010).

En suma, se destaca que el tema principal de la 20ª Sesión de la Comisión de Prevención del Delito y Justicia Penal, que se ha celebrado en 2011 ha sido la "Protección de los niños en la era digital: el mal uso de la tecnología en el abuso y la explotación sexual de niños". Se observa

aquí la creciente preocupación de la ONU por la utilización de las tecnologías para ocasionar daños que incluso llegan a tildarse de delitos penales.

Finalmente, dentro de este tema vinculado con los Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal se destaca que el en 12° Congreso, se afirmó lo siguiente:

> (…) los cambios dimanantes de la normalización técnica van mucho más allá de la globalización de la tecnología y los servicios y podrían conducir a la armonización de las legislaciones nacionales. Sin embargo, los principios de la legislación nacional cambian con mucha mayor lentitud que los aspectos técnicos. Por ello se recomienda analizar los enfoques encaminados a territorializar Internet. Se afirma que, aunque Internet pueda estar al margen de los controles fronterizos, hay formas de restringir el acceso a determinada información, por lo que los gobiernos nacionales y las organizaciones internacionales han comenzado a prestar atención a las obligaciones de los proveedores de servicios de Internet de bloquear el acceso a los sitios web que contengan pornografía infantil (Altmark y Molina Quiroga, 2012, p.160).

Como se puede observar la legislación interna de un país no se adecua conforme al ritmo de avance de las nuevas tecnologías; sino que lo hace con mayor lentitud tal como lo afirman los autores citados. Al respecto surge evidente el ejemplo de Argentina, en donde la legislación aún no se considera acorde a los parámetros internacionales existentes sobre la delincuencia informática. De hecho, a pesar de la modificación del Código Penal argentino mediante la ley 26.388 que incorpora ciertos delitos informáticos -ley que es presentada en este trabajo de investigación como materia de análisis- aún existe un vacío legal importante ya que no se han logrado tipificar algunas figuras delictivas relacionadas con la informática que día a día se vuelven más frecuentes.

Esto quiere decir que si bien la citada ley tipifica diversos delitos vinculados con el uso de las tecnologías, como los siguientes: delito de pornografía infantil por internet u otros medios electrónicos (art. 128 CP); violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP); intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP); acceso a un sistema o dato informático (artículo 153 bis CP); etcétera, se considera que aún existen figuras que se presentan cada día de manera más frecuente y que no fueron contempladas por el legislador al momento de redactar la ley 26.388. Al respecto, entre las figuras aún no tipificadas se debe otorgar urgente regulación a las calumnias e injurias, al *spam* y a las amenazas y coacciones a través de Internet.

Dentro de este listado de conductas se destacan las amenazas y las calumnias e injurias vía Internet. En la actualidad y de la manera en la que vive la sociedad - todos “empapados” con el

uso de redes sociales de todo tipo -resulta imposible no contar con normas que sancionen este tipo de ilícitos. Por supuesto que existen las normas penales tradicionales sobre los delitos de calumnia e injurias y amenazas- por mencionar un ejemplo-; no obstante ello, estas disposiciones no son precisas para cuando la conducta delictiva sucede por medios electrónicos.

En realidad, todas estas conductas aún no reguladas también perjudican a los usuarios de Internet y de las nuevas tecnologías de la información y causan daños e inconvenientes impensados para la sociedad.

Finalmente, a modo de ilustración respecto de las medidas que se han dialogado en el 12° Congreso se conoce aquella que requiere de los proveedores de acceso el control del sitio web que un usuario quiere entrar. Si éste se halla en la lista negra se bloqueará su entrada. Puntualmente se afirma que: "Las soluciones técnicas van desde la manipulación del sistema de nombres de dominio y el uso de servidores intermediarios hasta soluciones híbridas que combinan diversos métodos" (Altmark y Molina Quiroga, 2012, p.160). De hecho este método se aplica en diversos países europeos, entre ellos Italia, Noruega, el Reino Unido, Suecia y Suiza, y países tales como China, el Irán (República Islámica del) y Tailandia.

La única crítica que se le ha hecho a estas medidas es que algunas veces la implementación conjunta de todas ellas puede generar un exceso en el bloqueo del acceso a la información de Internet (Altmark y Molina Quiroga, 2012).

.

1.2 El delito informático en la Unión Europea

La doctrina ha dejado en evidencia que la transición de Europa a la sociedad de la información se encuentra marcada por grandes progresos en diversos aspectos de la vida de las personas, entre ello, en el trabajo, la educación y el ocio, el gobierno, la industria y el comercio. Las nuevas tecnologías de información y comunicación han generado un impacto revolucionario y fundamental en las economías y sociedades de los distintos países. "El éxito de la sociedad de la información es importante para el crecimiento, la competitividad y las posibilidades de empleo de Europa, y tiene repercusiones económicas, sociales y jurídicas de gran envergadura" (Comisión de las Comunidades Europeas, 2001, p.2).

En materia de delitos vinculados con las tecnologías, la Comisión de las Comunidades Europeas planteó un plan de acción para realizarse antes de finales de 2002 que procuraba destacar la importancia de la seguridad en las redes y la lucha contra la delincuencia informática. Esto

demuestra que la Unión Europea, entre otras medidas, ha decidido adoptar aquellas que permitan "(…) luchar contra los contenidos ilícitos y nocivos en Internet, para proteger la propiedad intelectual y los datos personales, para promover el comercio electrónico y el uso de la firma electrónica y para aumentar la seguridad de las transacciones" (Comisión de las Comunidades Europeas, 2001, p.2).

Finalmente, la doctrina expresa que, en abril de 1998, la Comisión ha presentado al Consejo los resultados de un estudio vinculado con la delincuencia informática, denominado estudio *"comcrime"*. Mientras que en octubre del año siguiente el mismo Consejo en la cumbre de Tampere afirmó que entre las tareas para acordar definiciones y sanciones comunes se debe incluir a la delincuencia de alta tecnología. Asimismo, el Parlamento Europeo ha convocado a todos los países a que definan de manera unánime y aceptable en todos los Estados a los delitos informáticos y a que se aproximen las legislaciones internas, en especial en el ámbito del derecho penal (Comisión de las Comunidades Europeas, 2001).

De esta manera, así como la Organización de las Naciones Unidas ha generado Congresos con el propósito de combatir la delincuencia, y en sus últimas reuniones ha incluido a la delincuencia informática como tema de preocupación; la Unión Europea también ha tomado medidas al respecto, tal como lo demuestra el estudio realizado por la Comisión de las Comunidades Europeas.

Esta citada Comisión, a través del comunicado que ha emitido en 2001 con el propósito de informar la necesidad de la "creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos"[5], ha buscado establecer parámetros internacionales vinculados con la delincuencia informática que resulten de utilidad a todos los Estados Europeos para controlar estos crímenes.

Se destaca allí la importancia de las tecnologías, su rápido avance y el crecimiento agigantado de los delitos informáticos. Se define a éstos, para lo que se diferencia los delitos informáticos específicos de aquellos delitos tradicionales ocasionados mediante el uso de las tecnologías. Por otro lado, respecto de la legislación en materia internacional, se especifica:

> Muchos países han adoptado legislación dirigida a abordar la delincuencia informática. En los Estados miembros de la Unión Europea, se han establecido varios instrumentos jurídicos. Aparte de una Decisión del Consejo sobre pornografía infantil en Internet, por ahora no existen instrumentos

[5] Título del documento emitido por la Comisión de las Comunidades Europeas en Budapest, 2001.

> jurídicos de la UE que aborden directamente la delincuencia informática, pero sí existen diversos instrumentos jurídicos que tratan indirectamente la cuestión (Comisión de las Comunidades Europeas, 2001, p.12).

Se destaca aquí entonces los instrumentos jurídicos, que, aunque de manera indirecta, abordan las problemáticas vinculadas con la delincuencia informática. De hecho, la doctrina enunciada expresa que las principales cuestiones sobre este tipo de ilícitos proveniente de la Unión Europea o de sus Estados miembros, comprende los siguientes delitos informáticos específicos:

Delitos contra la intimidad: comprende disposiciones penales vinculadas con la recogida, almacenamiento, modificación, revelación o difusión ilegales de datos personales. "En la Unión Europea, se han adoptado dos Directivas para la aproximación de las normas nacionales sobre protección de la intimidad por lo que se refiere al tratamiento de datos personales" (Comisión de las Comunidades Europeas, 2001, p.13).

Delitos relativos al contenido: "La difusión, especialmente por Internet, de pornografía, y en especial de pornografía infantil, las declaraciones racistas y la información que incita a la violencia plantea la cuestión de hasta qué grado estos actos pueden combatirse con ayuda del derecho penal" (Comisión de las Comunidades Europeas, 2001, p.13). Al respecto la Comisión afirma que todo lo que es ilegal fuera del mundo de la informática también lo es en éste.

Delitos económicos, acceso no autorizado y sabotaje: en muchos países ya se han aprobado leyes que contemplan delitos económicos perpetrados por ordenador y que permiten tipificar nuevos delitos vinculados con el acceso no autorizado a sistemas informáticos; entre ellos a modo de ejemplo se menciona a la piratería, al sabotaje informático y a la distribución de virus, al espionaje informático y a la falsificación y fraude informáticos. Asimismo, estas leyes permiten conocer nuevas formas de cometer delitos, tales como la manipulación de un ordenador en vez de engañar a una persona (Comisión de las Comunidades Europeas, 2001).

Delitos contra la propiedad intelectual: se afirma la necesidad de protección de los derechos de autor y afines y su respectiva sanción en caso de violación de éstos. Asimismo, debe penalizarse la omisión de las medidas tecnológicas diseñadas para proteger estos derechos. Se adoptaron al respecto, dos Directivas que buscan la protección jurídica de programas de ordenador y la protección jurídica de las bases de datos (Comisión de las Comunidades Europeas, 2001).

1.2.1 Convenio de Budapest

Este Convenio, también denominado Convenio sobre la Ciberdelincuencia- o más frecuentemente llamado Convenio o Convenio de Budapest- fue sancionado en el año 2001 por el Consejo de Europa en Budapest. Aquí se abordan todos los temas vinculados con los delitos cometidos a través del uso de las nuevas tecnologías de la información y las comunicaciones (Sain y Azzolin, 2017).

Pues el Comité Europeo para los Problemas Criminales (por sus siglas en inglés CDPC) decidió crear en 1996 un comité de expertos encargados de tratar asuntos vinculados con los delitos informáticos. Como consecuencia de este trabajo, cinco años más tarde se logra el Convenio de Budapest que representó el primer tratado internacional en asuntos de delitos informáticos, tales como fraude, pornografía infantil o violación de la propiedad intelectual. [6]

Es decir, este instrumento se destaca por ser el único acuerdo internacional sobre este tipo de delitos que existe hasta la actualidad, sin discutir por supuesto la existencia de otras normas de países del derecho comparado que puedan haber incorporado en su legislación interna la regulación de la delincuencia informática.

Puntualmente en esta norma se hace hincapié en delitos como infracciones de derechos de autor, fraude informático, pornografía infantil, delitos de odio y violaciones de seguridad de red.

Se establece la urgente necesidad de prevenir todo acto que pueda menoscabar la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Asimismo, se establece el combate contra estos delitos, para lograr su detección, investigación y sanción, tanto a nivel nacional como internacional, y se determinan acciones que permitan una cooperación internacional rápida y fiable (NicArgentina, 2017).

En suma, se procura:

> (…) homogeneizar las definiciones sobre ciberdelito, establecer el intercambio de información en lo que respecta a estos ilícitos, garantizar el debido equilibrio entre los intereses de la acción penal y el respeto a los derechos humanos que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto de la vida privada. (NicArgentina, 2017, p.1).

[6] Fuente: "Argentina se suma a la Convención de Budapest para tratar delitos informáticos". (13/05/18). *Infobae*. Recuperado el 17/07/18 de https://www.infobae.com/tecno/2018/05/13/argentina-se-suma-a-la-convencion-de-budapest-para-tratar-delitos-informaticos/

Tal como se puede observar, los instrumentos internacionales buscan convertirse en un marco regulatorio de estos delitos para que todos los países que se adhieran a él respeten lo allí establecido. Se pretende que todos los Estados utilicen la misma terminología, proteger ante todo la confidencialidad, integridad y disponibilidad de datos en la red, la protección de la propia opinión y, ante todo, la detección, investigación y sanción de los delitos informáticos.

De esta manera, resulta evidente que los parámetros internacionales vinculados con la ciberdelincuencia difieren en gran medida de lo regulado y comprendido por la legislación argentina. Pareciera ser que este país se halla "camino hacia"; es decir, que se encuentra aún en el camino para lograr lo que otros países como la Unión Europea o Estados Unidos han logrado ya hace varios años. Esto queda en evidencia a partir de la adhesión de Argentina a este Convenio en 2017.

Sin embargo, debe remarcarse la urgente necesidad de adecuar el ordenamiento interno argentino a estos parámetros- con cierta prisa- debido a que los avances tecnológicos transforman a esta sociedad de manera impensada y sin pausa. Quedarse en el camino y no adecuarse a estas normativas internacionales generaría consecuencias impensadas en el ámbito de la delincuencia informática.

Por lo dicho, una vez adheridos a este Convenio internacional resulta importante que el legislador argentino elabore la debida actualización normativa y adapte no solo los tipos penales de este país (vinculados con este tipo de actos cometidos mediante el uso de la informática) sino que también contemple la normativa procesal correspondiente; todo ello para lograr equiparar las leyes internas con aquellas de los países más desarrollados en ciberdelito.

Ahora bien, el Convenio de Budapest aborda distintos ejes temáticos. El primero de ellos busca establecer un catálogo de figuras que penalicen las modalidades de criminalidad informática. Se definen aquí a los delitos y se los clasifica en cuatro categorías que resultarán conocidas por las clasificaciones anteriormente brindadas en esta investigación. Es decir, se distingue a los delitos entre: 1. Delitos que tienen a la tecnología como fin; 2. Delitos que tienen a la tecnología como medio; 3. Delitos relacionados con el contenido; 4. Delitos relacionados con infracciones a la propiedad intelectual (Pastorino, 2017).

Puntualmente en el título 1 (clasificados como delitos que tienen a la tecnología como fin) se mencionan los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, y dentro de este rubro define en sus artículos a los delitos de acceso

ilícito, intercepción ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema y abuso de los dispositivos. Luego, en el título 2 se definen específicamente a los delitos informáticos (según la clasificación se hace referencia a los delitos que tienen a la tecnología como medio) y se incluye aquí a la falsificación informática y al fraude informático. En el titulo 3 se comprende a los delitos relacionados con el contenido, es decir a todos los delitos relacionados con la pornografía infantil. Con posterioridad en el título 4 se hace referencia a los delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines.

Ya en la segunda parte o segundo eje del Convenio se regulan las normas procesales; esto significa que aquí "(…) se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia". Este punto aplica a todo tipo de delito cometido por un medio informático o cualquier tipo de evidencia en formato electrónico. "Entre otras cosas determina la obtención y conservación de datos digitales para ser utilizados como pruebas" (Pastorino, 2017, p.3).

Finalmente, el último eje contiene las normas de cooperación internacional, lo que comprende aquellas reglas de cooperación que permiten investigar todo tipo de delito que implique recurrir a evidencia digital, ya sean delitos tradicionales o informáticos. Puntualmente aquí se distinguen dos títulos, el primero de ellos hace referencia a los principios generales relativos a la cooperación internacional y el segundo, a los principios relativos a la extradición.

En conclusión, a través de tres ejes centrales este acuerdo internacional logra establecer los tipos delictivos, las normas procesales y las reglas de cooperación internacional que todo país que adhiera a éste debe respetar con el propósito de combatir de manera conjunta con la delincuencia informática.

Por último, se destaca que los Estados miembros del Consejo de Europa, en oportunidad de la suscripción del Convenio de Budapest, con el propósito de luchar efectivamente contra el ciberdelito y a facilitar su detección, investigación y sanción a nivel nacional e internacional de manera rápida y fiable, se comprometieron a:

- Designar órganos jurisdiccionales que serán competentes en el caso de las infracciones penales antes mencionadas;
- Apoyar la aprobación de disposiciones que facilitarán la cooperación judicial en materia de asistencia judicial;

> - Apoyar la aprobación de disposiciones relativas al almacenamiento y conservación de los datos relativos a la delincuencia vinculada a la alta tecnología; (Tobares Catalá y Castro Arguello, 2010, p.12).

Para finalizar se reitera que Argentina recientemente ha adherido a este Convenio. De hecho, las noticias periodísticas han ilustrado tal decisión en títulos como "Argentina se suma a la Convención de Budapest para tratar delitos informáticos". Esta decisión fue aprobada por la Cámara de Diputados en noviembre de 2017, cuando aprobaron la ley de ratificación de dicha Convención.[7]

Al respecto, Marcos Salt- impulsor de la inclusión de Argentina al Convenio de Budapest- afirmó que:

> Si bien la Convención de Budapest fue creada por el Consejo Europeo, tiene características especiales. "Está abierta al mundo. Están dentro países como Estados Unidos, Italia, España, Japón, Canadá, Israel, Chile, República Dominicana y Panamá. Es el único convenio internacional sobre delitos informáticos y obtención de evidencia digital (con cooperación internacional específica en este sentido)".[8]

Esto demuestra que Argentina cada día se halla más interesada en la protección de sus ciudadanos víctimas de delitos informáticos. No obstante ello, aún queda mucho trabajo por delante en cuanto a la adecuación de su legislación interna a los parámetros internacionales vigentes, sin negar que estas medidas -como la adhesión al Convenio de Budapest- indudablemente reflejan un paso importante y necesario en la lucha contra la ciberdelincuencia.

La doctrina afirma que:

> Las nuevas tecnologías constituyen un desafío para los conceptos jurídicos existentes. La información y la comunicación fluyen con mayor facilidad por todo el mundo. Las fronteras han dejado de ser barreras para ese flujo. Los delincuentes se encuentran cada vez menos en los lugares en que se hacen sentir los efectos de sus actos (Altmark y Molina Quiroga, 2012, p.117).

En realidad, la legislación nacional se dedica a regular un territorio específico y por ende no podrá brindar soluciones a problemas planteados en un radio mucho más amplio que el que abarca un país. Como consecuencia, el Convenio de Budapest considera que estos delitos

---

[7] Fuente: "Argentina se suma a la Convención de Budapest para tratar delitos informáticos". (13/05/18).*Infobae*. Recuperado el 17/07/18 de https://www.infobae.com/tecno/2018/05/13/argentina-se-suma-a-la-convencion-de-budapest-para-tratar-delitos-informaticos/

[8] Fuente: "Argentina se suma a la Convención de Budapest para tratar delitos informáticos". (13/05/18).*Infobae*. Recuperado el 17/07/18 de https://www.infobae.com/tecno/2018/05/13/argentina-se-suma-a-la-convencion-de-budapest-para-tratar-delitos-informaticos/

vinculados con la informática- cuyos efectos superan las barreras nacionales- deben ser regulados mediante instrumentos jurídicos internacionales adecuados que respeten los derechos humanos en la nueva Sociedad de la Información (Altmark y Molina Quiroga, 2012).

No obstante lo dicho, sin negar la importancia de la adhesión a los instrumentos internacionales específicos en la materia en cuestión, se destaca la necesidad de que los distintos países adecuen sus normas internas (y también los aspectos procesales) a las previsiones allí contempladas para lograr la lucha conjunta contra estos delitos que generan daños a grandes escalas.

2. Recepción legislativa de los delitos informáticos en leyes internas de otros países

A continuación de brindará un análisis de la legislación interna del derecho comparado; es decir, se mencionarán los aspectos sobresalientes vinculados con los delitos informáticos y su recepción legislativa específica.

2.1 Estados Unidos

Ya se ha afirmado que este país es uno de los más avanzados en la regulación de los delitos informáticos ya que cuenta con la tecnología y los conocimientos necesarios, así como también con la legislación pertinente para su control. Especifica la doctrina:

> El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho (Segu.Info. Seguridad de la Información, s/f, p.1).

Así, se conoce que la primera propuesta de legislar el delito informático fue la introducida por el Senador Ribicoff en 1977 en el Congreso Federal de Estados Unidos y con posterioridad en el año 1983 la Organización para la Cooperación Económica y el Desarrollo (OECD) en París designó un comité de expertos para que estudie sobre los crímenes que se relacionen con las computadoras y la necesidad de realizar modificaciones a los Códigos Penales de los distintos países (Paterlini, Vega, Guerriero y Velázquez, s/f).

Puntualmente en cuanto a la regulación de estos delitos por parte del derecho, los Estados Unidos cuentan con leyes federales específicas que protegen a sus víctimas de los ataques a los ordenadores, del uso indebido de contraseñas, de las invasiones en la privacidad en las redes y diversas transgresiones que han sido tipificadas como delitos vinculados con el uso de las tecnologías, o también denominados delitos informáticos (Paterlini, et. al., s/f).

Al respecto, dentro de las dos legislaciones federales más importantes sobre delincuencia informática se destaca el Código Penal de los Estados Unidos, título 18, capítulo 47, sección 1029 y 1030 de 1994 que sirvió de modificación de lo contenido en el Acta de Fraude y Abuso Computacional de 1986.

Puntualmente la sección 1029 "(…) prohíbe el fraude y cualquier actividad relacionada que pueda realizarse mediante el acceso o uso de dispositivos falsificados como PINs, tarjetas de crédito, números de cuentas, y algunos tipos más de identificadores electrónicos" (Paterlini, et. al., s/f, p.9). Dentro de esta parte del Código Penal de Estados Unidos se incluyen distintas áreas de actividad criminal que se mencionan allí y que requieren por supuesto que el delito implique comercio interestatal o con el extranjero. Se enuncian a continuación estas nueve áreas:

1. Producción, uso o tráfico de dispositivos de acceso falsificados.
2. Uso u obtención sin autorización de dispositivos de acceso para obtener algo de valor totalizando $1000 o más, durante un periodo de un año.
3. Posesión de 15 o más dispositivos de acceso no autorizados o falsificados.
4. Fabricación, tráfico o posesión de equipo de fabricación de dispositivos de acceso ilegales.
5. Realización de transacciones con dispositivos de acceso pertenecientes a otra persona con el objetivo de obtener dinero o algo de valor totalizando $1000 o más durante un periodo de un año.
6. Solicitar a una persona con el objetivo de ofrecerle algún dispositivo de acceso o venderle información que pueda ser usada para conseguir acceso a algún sistema.
7. Uso, producción, tráfico o posesión de instrumentos de telecomunicación que hayan sido alterados o modificados para obtener un uso no autorizado de un servicio de telecomunicaciones.
8. Uso, fabricación, tráfico o posesión de receptores-escaneadores o hardware o software usado para alterar o modificar instrumentos de telecomunicaciones para obtener acceso no autorizado a servicios de telecomunicaciones.
9. Hacer creer a una persona que el delincuente es un miembro de su compañía de tarjeta de crédito o su agente para obtener dinero o realización de transacciones hechas con un dispositivo de acceso y viceversa (tratar de hacer creer a la compañía de crédito que se trata de la persona legítima). (Paterlini, et. al., s/f, p.9).

Respecto de todos estos delitos se remarca que la acción debe ser cometida conscientemente y con voluntad de estafar

Por su parte, la sección 1030, Título 18, Capítulo 47 del Código Penal de Estados Unidos "(…) como parte de la Ley sobre Abuso y Fraude Informático de 1986, prohíbe el acceso no autorizado o fraudulento a ordenadores gubernamentales, y establece diversas condenas para esa clase de accesos" (Paterlini, et. al., s/f, p.11). Al respecto se expresa que esta legislación es una de las pocas, dentro de las leyes federales, que se refiere únicamente a ordenadores. Precisamente mediante la Ley de Abuso y Fraude Informático, tanto el Servicio Secreto americano como el F.B.I. gozan de jurisprudencia para investigar los delitos definidos en este decreto. Finalmente, las seis áreas de actividad criminal que incluye la sección 1030 son:

> 1. Adquisición de información restringida relacionada con defensa nacional, asuntos exteriores o sobre energía nuclear con el objetivo o posibilidad de que sean usados para dañar a los Estados Unidos o para aventajar a cualquier otra nación extranjera.
> 2. Obtención de información en un registro financiero de una institución fiscal o de un propietario de tarjeta de crédito; o de información de un cliente en un archivo de una agencia de información de clientes.
> 3. Atacar un ordenador que sólo corresponda ser usado por algún departamento o agencia del gobierno de los EEUU, para el caso de que no sólo puede ser usada por esta agencia, atacar un ordenador usado por el gobierno en el que la intrusión producida afecte el uso que el gobierno hace de él.
> 4. Promover un fraude accediendo a un ordenador de interés federal y obtener algo de valor, a menos que el fraude y la cosa obtenida consistan solamente en el uso de dicho ordenador.
> 5. A través del uso de un ordenador utilizado en comercio interestatal, transmitir intencionadamente programas, información, códigos o comandos a otro sistema informático.
> 6. Promover el fraude traficando con passwords o información similar que haga que se pueda acceder a un ordenador sin la debida autorización. Todo esto si ese tráfico afecta al comercio estatal o internacional o si el ordenador afectado es utilizado por o para el Gobierno (Paterlini, et. al., s/f, p.10 y 11).

Respecto de todos estos delitos se remarca que la acción debe ser cometida conscientemente accediendo a un ordenador sin autorización o exceder el acceso autorizado.

Asimismo, se debe destacar que existe una abundante legislación dentro de cada uno de los más de cincuenta estados, tanto en la tipificación como en los aspectos procesales.

Tal como se afirmó en 1994 el Acta Federal de Abuso Computacional fue modificada mediante la sección 1030 del título 18 anteriormente descriptos. Con esta reforma se elimina

finalmente aquellos argumentos híper técnicos vinculados con qué es y qué no es un virus, un gusano, un caballo de Toya, etcétera (Paterlini, et. al., s/f)

Expresan los autores citados que modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. De esta manera esta ley representa un acercamiento real al problema, alejado de argumentos técnicos para dar lugar a una nueva era de ataques tecnológicos.

Como conclusión, la sociedad norteamericana se ha preocupado por la regulación y penalización de la delincuencia informática incluso desde 1986, lo que demuestra un real avance en la especialización sobre el uso indebido de las tecnologías.

2.2 Francia

En este país mediante la ley número 88-19 de fecha 5 de enero de 1988 se legisla sobre el fraude informático. Puntualmente se contempla el acceso fraudulento a un sistema de elaboración de datos y se sanciona no sólo el acceso al sistema sino también al que se mantenga en él. Asimismo, se aumenta la pena si de dicho acceso resultara la supresión o modificación de los datos contenidos en el sistema o la alteración del funcionamiento del sistema (Segu.Info. Seguridad de la Información, s/f).

Sumado a lo dicho, también se regula en la citada legislación al sabotaje informático, que incluye la acción de falsear el funcionamiento de un sistema de tratamiento automático de datos.

Por otro lado, se contempla la destrucción de datos y se sanciona a la persona que de manera intencional y con menosprecio de los derechos de los demás introduce datos en un sistema de tratamiento automático de datos, suprime o modifica los datos que allí existen o los modos de tratamiento o de transmisión.

Finalmente, en la citada ley 88-19 se incluye a la falsificación de documentos informatizados. En este aspecto se castiga a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro (Segu.Info. Seguridad de la Información, s/f).

2.3 Alemania

Respecto de este país se habla de que su legislación penal para la lucha contra la criminalidad informática se ha construido sobre la base de dos tipos de acciones atentatorias para

ciertos bienes jurídicos; es decir, se tipifica al fraude informático y al delito de sabotaje informático y principalmente se protege al patrimonio como bien jurídico (Paterlini, *et. al*., s/f).

Asimismo, en lo vinculado con las acciones que atentan contra la vida personal y la privacidad de una persona, la regulación penal alemana sanciona el espionaje de datos, pero a la vez excluye la información que se encuentra almacenada o que pueda transmitirse de manera electrónica o de forma inmediatamente accesible. Al respecto se agrega:

> Con ello, prácticamente no se regula ningún tipo penal que pudiera estar referido a un espionaje de datos informatizados. No se quiso punir la mera intrusión informática, sino sólo en aquellos casos de conductas que signifiquen la manipulación de las computadoras y persigan un ánimo de lucro (Paterlini, *et. al*., s/f, p.6).

Por otro lado, la doctrina expresa que a partir del primero de agosto de 1986 para hacer frente a la delincuencia relacionada con la informática se adoptó en Alemania la Segunda Ley contra la Criminalidad Económica en la que se contemplan los siguientes delitos:

> - Espionaje de datos (202 a)
> - Estafa informática (263 a)
> - Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273)
> - Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
> - Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, Inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
> - Utilización abusiva de cheques o tarjetas de crédito (266b) (Acurio Del Pino, 2015, p.34)

Ahora bien, la doctrina hizo hincapié que, para el caso particular de la estafa informática, surgieron problemas en la formulación de un nuevo tipo penal ya que costó hallar un equivalente análogo al triple requisito de acción engañosa, causa del error y disposición patrimonial, en el engaño del computador. Sumado a ello, se tornó complejo el hecho de garantizar las posibilidades de control de la nueva expresión legal, por lo que su redacción se afirmó que "el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa" (Acurio Del Pino, 2015, p.34 y 35). Todo ello, mediante la utilización de datos incorrectos o incompletos, o a través del uso no autorizado de datos o de una intervención ilícita.

Finalmente expresan los doctrinarios especializados en la materia, que el legislador alemán, aunque ha introducido un número relativamente alto de nuevos preceptos penales, no ha llegado tan lejos como Estados Unidos. Ya se observó al respecto que este último país se destaca por ser uno de los más avanzados en materia de regulación informática.

Se critica en cierta forma a la legislación de Alemania porque se conoce que se ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras y no se castiga el uso no autorizado de equipos de procesos de datos, incluso aunque ocurra de forma cualificada. Puntualmente, al momento de incorporar nuevas figuras penales para lograr el castigo de los delitos informáticos, el gobierno alemán reflexionó acerca de dónde se hallaban las dificultades reales para aplicar el derecho penal tradicional a estos nuevos comportamientos dañosos y acerca de qué bienes jurídicos resultaban lesionados (Ramírez Bejerano y Aguilera Rodríguez, 2009).

Como consecuencia de estas reflexiones se comprobó que en realidad los delitos informáticos, sobre todo aquellos vinculados con el tratamiento electrónico de datos para la comisión de hechos delictivos, representaban un nuevo modo operandi. Así se concluyó que en realidad la protección de los bienes jurídicos menoscabados requería de un derecho penal distinto al vigente en aquel momento ya que surgían nuevas formas de agresión ocasionadas por la utilización abusiva de las instalaciones informáticas.

Finalmente se concluyó que el surgimiento de las nuevas formas de criminalidad informática generaba nuevas lesiones de bienes jurídicos merecedores de pena, sobre todo cuando el ovejo de la acción eran datos almacenados o transmitidos o cuando se trataba de daños a los sistemas informáticos (Ramírez Bejerano y Aguilera Rodríguez, 2009).

2.4 Reino Unido

En el Reino Unido existe desde junio de 1990 la ley denominada *"Computer Misuse Act 1990"* (Ley de los abusos informáticos), que comenzó a regir a partir de un conocido caso de hacking en 1991. Como consecuencia, se crearon disposiciones para otorgar seguridad al material de las computadoras contra accesos no autorizados y disposiciones conexas. Esta legislación fue actualizada en julio de 2014.

Puntualmente se afirma que, mediante esta norma, el intento-sin importante si resulta exitoso o no- de alterar datos informáticos es castigado con hasta cinco años de prisión o multas. Asimismo, se penaliza la modificación de datos sin autorización y se incluye aquí a los virus (Ramírez Bejerano y Aguilera Rodríguez, 2009).

En cuanto a la estructura de esta ley, ésta se divide en tres partes: hackear (ingresar sin permiso a una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada. En este sentido, bajo la aplicación de esta ley, liberar un virus constituye un delito. De hecho, en enero de 1993 se produjeron distintos arrestos que han sido considerados la primera prueba de la nueva ley en un entorno real (Segu.Info. Seguridad de la Información, s/f).

2.5 España

En España, el Código Penal de 1995 aprobado por Ley-Orgánica 10/1995, de 23 de noviembre ha incorporado a los tipos delictivos clásicos, la realidad informática de manera global. No se ha limitado a regular solo los delitos informáticos de mayor conocimiento; sin embargo, se ha intentado lograr armonía jurídica entre las figuras clásicas penales y el fenómeno informático (Acurio Del Pino, 2015).

En este sentido afirma la citada doctrina que se destaca el esfuerzo español por lograr la regulación de estos delitos incluso a pesar de no haber adoptado la solución que han tomado otros ordenamientos jurídicos, que ha sido la creación de leyes especiales, que consideran de manera puntual a los delitos informáticos.

De hecho, el contenido del Nuevo Código Penal Español penaliza la delincuencia informática a través de la tipificación de ciertas acciones como la interceptación del correo electrónico, el fraude informático, la usurpación y cesión de datos reservados de carácter personal, los daños informáticos, la difusión de mensajes injuriosos o calumniosos, los robos de tarjetas magnéticas, la revelación de secretos, las falsedades documentales, entre otros (Acurio Del Pino, 2015).

Esto demuestra cierta semejante con el derecho argentino en donde se han introducido modificaciones al Código Penal que permitan abarcar ciertas conductas delictivas ocasionadas

mediante el uso de la tecnología. Sin embargo, al igual que la legislación de Argentina, España no cuenta con leyes específicas en la materia.

Al respecto la doctrina expresa que aunque los delitos informáticos no están contemplados de manera aislada y como un tipo especial de delito en la legislación española, existen varias normas relacionadas con este tipo de conductas, entre ellas se menciona a la Ley Orgánica de Protección de Datos de Carácter Personal, la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico, el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, la Ley General de Telecomunicaciones, la Ley de Propiedad Intelectual y la Ley de Firma Electrónica (RecoveryLabs, s/f).

Sumado a lo dicho la actual Ley Orgánica de Protección de Datos de Carácter Personal aprobada el 15 de diciembre de 1999 ha reemplazado distintas leyes anteriores similares y ha contemplado la mayor cantidad de acciones lesivas sobre la información. Allí se incluye de manera detallada "(…) la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el *phreacking*, la introducción de virus, etc.; aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos" (Segu.Info. Seguridad de la Información, s/f).

2.6 Venezuela

En este país se destaca la Ley Especial contra los delitos Informáticos, promulgada en 2001 por la Asamblea Nacional de la República Bolivariana de Venezuela. Tal como resulta evidente, los venezolanos han tardado varios años más en regular la delincuencia informática si se compara con países europeos o de América del Norte. Sin embargo, se destaca su especialización a la hora de regular este tipo de delincuencia.

El artículo primero de la citada norma expresa:

> Artículo 1. Objeto de la Ley. La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

Tal como se afirma, esta legislación busca por un lado proteger los sistemas de información y por otro lado sancionar los delitos que utilizar a la tecnología como medio o como fin.

En el artículo siguiente se definen los términos que permitirán la comprensión homogénea de lo dispuesto por dicha norma, entre ellos: tecnología de la información, sistema, virus, data, documento, computador, hardware, firmware, etcétera.

Por otro lado, en el título II se tipifican puntualmente los delitos que la ley comprende, para lo que se dividen en distintos capítulos: de los delitos contra los sistemas que utilizan tecnologías de información; de los delitos contra la propiedad; de los delitos contra la privacidad de las personas y de las comunicaciones; de los delitos contra niños, niñas o adolescentes; de los delitos contra el orden económico. Así se conforman los cinco capítulos que agrupan las distintas conductas delictivas según el bien jurídico, el derecho o la persona que se vulnere. Sumado a lo dicho, en el título III se incluyen las disposiciones comunes, entre las que se mencionan las agravantes, las penas accesorias y otros elementos como la indemnización civil y la obligación de divulgar la sentencia condenatoria.

Así, resulta posible afirman que, aunque de manera más tardía, la legislación venezolana ha procurado la sanción de este tipo de acciones delictivas que día a día invaden a las sociedades sin límites ni barreras que puedan controlarlas.

Conclusiones parciales

En este tercer capítulo se ha hecho hincapié en la recepción legislativa del derecho comparado para ilustrar la manera en que el mundo en general brinda soluciones legales a estas nuevas figuras delictivas que no encuentran barreras ni fronteras que las detengan.

Se estudió aquí la normativa del derecho internacional, principalmente lo referido a las disposiciones provenientes de la Organización de las Naciones Unidas y de la Unión Europea. Se hizo hincapié en los distintos Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, que han tenido lugar cada cinco años en distintas ciudades y cuya materia de debate, entre otros temas, ha sido la delincuencia y la protección de la sociedad. Se pudo observar en este punto, el necesario tratamiento de la ciberdelincuencia como tema novedoso en los últimos años.

Asimismo, se desarrollaron las disposiciones legislativas provenientes de la Unión Europea, entre las que se encuentra el Convenio sobre la Ciberdelincuencia (o también llamado Convenio de Budapest), que sirvió de marco regulatorio para que todos los países miembros de la UE sepan qué medidas tomar en el control de los delitos informáticos.

Por último, se indagó acerca de la recepción legislativa de estos delitos en las leyes internas de otros países. Puntualmente se destacó el rol de los Estados Unidos como país del primer mundo que debido a sus conocimientos especializados en tecnologías y su consecuente mal uso de éstas, ha debido implementar medidas específicas para el control de la ciberdelincuencia. Asimismo, se describió la legislación de Francia, Alemania, el Reino Unido, España y Venezuela. Por supuesto, y tal como surge evidente en el análisis desarrollado en este capítulo, algunos países cuentan con mayor cantidad de normas o más dedicadas a la materia, mientras que otros simplemente han modificado ciertos artículos del propio Código Penal sin muchas especificaciones sobre los delitos informáticos.

Finalmente, a esta altura de la investigación resulta posible afirmar que el derecho internacional brinda ciertos parámetros de vital importancia en la regulación de los delitos vinculados con el uso de las tecnologías.

Se ha podido observar que en la mayoría de los instrumentos internacionales y de las leyes internas de otros países, en primer lugar, la norma define los conceptos que serán de utilidad para la comprensión de lo allí dispuesto. Luego, se dedica parte del ordenamiento jurídico del que se trate para la conceptualización de las distintas acciones típicas que se identifican como "delito informático". Así, la sociedad cuenta con un catálogo cierto y determinado de acciones tipificadas y puede conocer qué es o qué no es un delito.

Asimismo, se mencionan los aspectos procesales vinculados con la materia, se regula la jurisdicción y/o competencia e incluso las reglas vinculadas con la conservación de las pruebas digitales.

Por su parte se destaca que el Convenio de Budapest ha regulado ciertas pautas de cooperación internacional que permiten afirmar la necesidad de una modificación en las legislaciones internas de los países-sobre todo en los aspectos procesales- para hacer frente a los objetivos que el propio Convenio contempla.

Argentina se ha adherido a este Convenio internacional y ha marcado así un gran avance en la materia. Podría decirse de hecho que este instrumento ha servido de base para la normativa penal que actualmente este país se encuentra promoviendo.

Todas estas observaciones permiten sostener la importancia de contar con parámetros homogéneos sobre la materia en cuestión para que los distintos países adopten en su legislación

interna dichas normativas a la hora de combatir este fenómeno tan actual e incontrolable que representa la ciberdelincuencia.

A continuación, en el último capítulo, se analizarás las normas que el derecho argentino ha adoptado con el propósito de corroborar o desechar la hipótesis planteada al inicio de este trabajo de investigación.

CAPÍTULO IV

ANÁLISIS LEGISLATIVO Y JURISPRUDENCIAL DEL DERECHO INTERNO ARGENTINO SOBRE DELITOS INFORMÁTICOS

Introducción

En este último capítulo se hará hincapié en el análisis legislativo y jurisprudencial de la Argentina.

Para corroborar lo planteado al comienzo de la investigación- respecto a la hipótesis de este trabajo vinculada con la necesidad de adecuar el ordenamiento jurídico interno a los parámetros del derecho internacional sobre delitos informáticos- se debe en primer lugar describir las características de estas normas del derecho comparado, así como también conocer en profundidad qué leyes existen en este país sobre la materia en cuestión.

Con dicha finalidad es que a continuación se describirá la legislación argentina sobre delitos informáticos. Es decir, se intentará estudiar aquellas disposiciones contenidas en leyes o en el ordenamiento jurídico en general, que de alguna manera se encuentren vinculadas con los delitos cometidos mediante el uso de las nuevas tecnologías.

Así, se describirá por un lado lo contenido en el Código Penal argentino originario para luego hacer hincapié en la Ley de Propiedad Intelectual (Ley 11.723), la Ley de Protección de Datos Personales (Ley 25326) y finalmente la Ley 26.388 de modificación de Código Penal.

Desde ya se resalta el importante rol de esta última ley en materia de delitos informáticos debido a que su sanción ha permitido tipificar diversos delitos penales informáticos que en otros tiempos no hallaban respuesta alguna.

Asimismo, se analizará la Ley sobre *grooming* (Ley 26.904), como figura delictiva incorporada recientemente en el año 2013.

Por último, se desarrollará cierta jurisprudencia seleccionada vinculada con los delitos informáticos que permitirá ilustrarse cuáles han sido las resoluciones judiciales sobre la materia.

1. Análisis legislativo del ordenamiento jurídico argentino

1.1 Código Penal argentino originario

En esta oportunidad debe destacarse en primer lugar que resulta lógico afirmar que el legislador que elaboró el originario Código Penal promulgado por el presidente Hipólito Irigoyen

el 29 de octubre de 1921 no podía prever ni imaginar incluso tantos avances tecnológicos que ocurrirían en el futuro (Arocena, 2012).

De hecho, cuando una norma se crea se piensa que a través de su implementación se podrán resolver y sobre todo legislar las cuestiones que caracterizan a la sociedad en la que se vive, en dicho momento; y tal vez con cierta visión hacia el futuro. Sin embargo, en la mayoría de los casos uno no puede imaginar las dimensiones de los cambios que vendrán. Así como la sociedad cambia, la legislación debe adecuarse a ésta para poder brindar las respuestas que las personas necesitan en el tiempo y espacio en que se encuentren.

Por lo tanto, si se piensa así, quizás se destaca un dato relevante a la hora de determinar la eventual idoneidad de los delitos penales tipificados, los que indudablemente no son acordes en la actualidad para acoger la delincuencia informática. Es decir, el legislador del Código Penal originario no pudo haberse imaginado la necesidad de regular figuras delictivas de la magnitud que hoy en día se necesita.

Como consecuencia se afirma la existencia de hipótesis fácticas de imposible subsunción en las figuras penales existentes, lo que provee casos a contemplar en eventuales nuevas tipificaciones legales (Arocena, 2012).

Por lo tanto, afirma el autor citado que se requiere la construcción de nuevas figuras delictivas ya que se ha constatado que los intentos de subsunción de un supuesto fáctico novedoso en un tipo penal existente acaban en respuestas impropias brindadas por el sistema normativo penal de este país. Puntualmente agrega: "Una respuesta impropia de los tipos penales sería una pena cuya naturaleza no corresponda al contenido de injusto del hecho atrapado en el tipo penal" (Arocena, 2012, p.949).

En este sentido señala el autor Rosende (citado por Figari, 2009) que en realidad el derecho o el ordenamiento jurídico en su conjunto que tiende a regular las relaciones sociales entre los particulares y la de éstos con el propio Estado, se relaciona con el mundo que se vive en dicho momento. Es decir, una vez observados los hechos, recién allí pueden analizarse. De esta manera se afirma al respecto "(…) por más evolucionada que esté una sociedad en su fase legislativa, nunca podrá establecer con anterioridad normas que regulen hechos futuros, y por lo tanto inexistentes, y más aún cuando los mismos, pueden llegar a ser inimaginables (…)" (Figari, 2009, p.1).

De esta manera surge con evidencia que en el momento de la redacción del originario Código Penal hace más de ochenta años no se pudo haber imaginado los tipos delictivos, la forma que éstos adquieren o incluso los medios de comisión de estos delitos que ocurrirían en la actualidad y en esta sociedad.

A esto agrega Rosende que en realidad en Argentina la explosión digital ha sido paulatina, pero en cierta manera no ha sido acompañada por la consecuente evolución legislativa. O si lo ha sido, sus características se observaron de manera aislada (Figari, 2009).

No obstante lo dicho, la doctrina menciona cantidad de proyectos que han surgido en estos años pero que, por no haber sido tratados adecuadamente, han perdido vigencia. Entre ellos se mencionan por ejemplo: 1) los proyectos de ley que proponían la incorporación del delito de intrusión en el Código Penal (de Pascual, Mercader, Benedetti, Galván, etc.); 2) el proyecto sobre delitos informáticos (de Leonor E. Tolomeo) que pretendía la incorporación de terminología y definiciones tales como violación de secreto, estafas y otras defraudaciones, daño, interrupción de las comunicaciones, delitos que comprometen la paz y dignidad de la Nación y delitos de propiedad intelectual; 3) el proyecto de ley (de Carlos R. Álvarez) que buscaba la incorporación de una ley complementaria que contenía tres artículos relacionados con la comisión de los tipos de hurto y daño mediante medios informáticos; 4) el proyecto de ley (de José A. Romero Feris) que contaba con cinco artículos que regulaban las figuras de hurto, estafa y daño a través de medio informático y agravaba las conductas cuando fueran perpetradas por funcionarios públicos; 5) el proyecto de Ley sobre el Régimen Penal del Uso Indebido de Computación (de Berhongaray); 6) la Ley Penal y Protección de la Informática (de Bauzá); 7) el proyecto de ley sobre delitos informáticos (de Almirón); 8) la apropiación de mensajes y registros enviados por correo electrónico; delitos informáticos (proyecto del 26/11/01 que constaba de tres tipos básicos: "Acceso ilegítimo informático", "Daño informático" y "Fraude informático"); 9) el anteproyecto de delitos informáticos del 04/03/05 que regulaba los delitos autónomos, dentro de una ley complementaria, entre ellos: "Daño informático", "Estafa informática", "Delitos contra la privacidad" y "Ofrecimiento o difusión de pornografía infantil" (Figari, 2009).Sumado a lo dicho, en el año 2006 se presentaron como proyectos de ley los siguientes:

> 1) "Proyecto Delia Bisutti" (2032-D-06), a través del cual se proponía equiparar el correo electrónico a la correspondencia epistolar; 2) "Proyecto Canevarolo" (3001-D-06), similar al proyecto precedente; 3) "Proyecto Diana Conti y Agustín Rossi" (2291-D-06), en el cual proponía modificaciones al tipo penal de violación de secreto e introducía un nuevo bien jurídico, la

> privacidad (…) 4) "Proyecto Silvia Martínez" (1798-D-05), el que expresamente punía el ofrecimiento y difusión de la pornografía infantil y prostitución infantil; 5) "Proyecto Marta Osario" (1225-D-05) que introducía modificaciones a los tipos penales de estafa y daño (…) y 6) "Proyecto Andrés Sotos" (985-D-05), que como ley especial o complementaria que contenía cinco capítulos: Capítulo I.- Acceso ilegítimo informático; Capítulo II.- Violación al correo electrónico; Capítulo III.- Daño informático; Capítulo IV.- Fraude informático y Capítulo V.- Pornografía infantil" (Figari, 2009, p. 2 y 3).

Tal como se afirmó con anterioridad, todos estos proyectos o leyes no hay sido tratados ni sancionados por lo que perdieron vigencia legislativa. Sin embargo, no en vano han sido dichos intentos por regular esta materia que con el paso del tiempo se ha tornado de necesario tratamiento, en la sociedad actual.

Ahora bien, este trabajo plantea la necesidad de una adecuación de las leyes penales para incluir delitos que en la actualidad han comenzado a ser frecuentes por lo que los citados proyectos- aunque hayan quedado sin aplicación- han servido para sentar las bases de las nuevas normativas. De hecho, la adecuación de la normativa argentina a los parámetros internacionales en materia de delincuencia informática necesita de un arduo trabajo, por lo que estos intentos legislativos sirven como impulso inicial.

Así las cosas, surge el proyecto de ley que dio origen a la conocida ley 26.388 que ha marcado un antes y un después en lo vinculado con los delitos informáticos. Este proyecto ha sido producto del trabajo conjunto de los Diputados Nemirovsci, Romero, Bisutti, Irrazábal, Lovaglio Saravia, Osorio, Ritondo, Zottos, Canevarolo, Morini, Conti, Pinedo y Solanas y surge del tratamiento de varios expedientes legislativos. Se afirma al respecto que viene a ser una versión mejorada y refinada de todos los anteriores proyectos desde 1996 hasta 2008 (Figari, 2009).

De esta manera se sanciona la ley 26.388 conocida como aquella que incorpora al Código Penal argentino ciertos delitos informáticos. Tal como se ha podido observar, esta norma ha tenido por antecedente el dictamen de las comisiones de Comunicaciones e Informática y de Legislación Penal de la Cámara de Diputados de la Nación en el año 2006.

Puntualmente la ley citada recibió tratamiento en Diputados el 1/11/06 en donde se introdujeron algunas modificaciones en el texto sugerido por las comisiones. Luego ingresó en la Cámara de Senadores para su estudio en las comisiones pertinentes y finalmente fue votada el 28/11/07 con algunas modificaciones (Figari, 2009). Vale destacarse aquí que esta normativa será desarrollada en profundidad en uno de los apartados siguientes.

Ahora bien, para concluir resulta posible afirmar que del análisis del anterior Código Penal argentino surge evidente la inexistencia de normas vinculadas con los delitos informáticos. Ello así, y tal como se analizó anteriormente, debido a que en el año de sanción de este instrumento jurídico- año 1921- ni los legisladores ni la sociedad misma se hallaban en la necesidad de regular situaciones que no ocurrían en aquel momento. Pues bien, resulta obvio que nadie puede regular ni legislar el futuro incierto.

Como consecuencia y para finalizar, es importante destacar la necesidad de que el derecho se ajuste a los acontecimientos sociales una vez que éstos comiencen a ocurrir, para lograr así la protección de los derechos de todos los ciudadanos en el tiempo y espacio en el que se hallen.

1.2 Ley de Propiedad Intelectual (Ley 11.723)

Esta ley ha sido sancionada en Argentina en el año 1933 y regula principalmente a la propiedad intelectual, aunque contiene asimismo disposiciones sobre el fomento del libro y la lectura, sobre el dominio público pagante y sobre la gestión de derechos colectivos de autores y de titulares de derechos conexos (Unesco, 2009).

Al respecto se afirma que la Dirección Nacional del Derecho de Autor se encarga del cumplimiento de los objetivos establecidos en el régimen legal de la propiedad intelectual en este país. Este organismo mencionado depende de la Secretaría de Asuntos Registrales que a su vez depende del Ministerio de Justicia, Seguridad y Derechos Humanos. Puntualmente su trabajo es realizar tareas como, por ejemplo:

> (…) el registro y supervisión de la inscripción de obras científicas, literarias, artísticas, publicaciones periódicas, fonogramas, audiovisuales, software, musicales, editoriales, seudónimos, páginas web, contratos y otros actos jurídicos atinentes al derecho de autor; la tramitación de recursos de oposición sobre inscripciones; la reunión y catalogación de la legislación, doctrinas y jurisprudencia nacionales y extranjeras sobre la materia; prestar asesoría a los organismos públicos, entidades privadas y/o particulares acerca de la interpretación de las normas vigentes en materia de derecho de autor y derechos conexos, entre otras (Unesco, 2009, p.4).

En cuanto a la estructura, esta Ley sobre el Régimen de la Propiedad Intelectual se compone de 83 artículos, entre los que se destacan los primeros doce ya que allí se definen las obras científicas, literarias y artísticas y se regulan todas las facultades que implica tener la propiedad de

tales obras, los que se consideran titulares de las mismas, la duración de la propiedad intelectual (Unesco, 2009).

Así, su organización se divide de acuerdo a los siguientes títulos: 1. De las obras extranjeras; 2. De la colaboración; 3. Disposiciones especiales; 4. De la edición; 5. De la representación; 6. De la venta; 7. De los intérpretes; 8. Del registro de obras; 9. Del registro de propiedad intelectual; 10. Fomento de las artes y letras (artículos derogados); 11. De las penas; 12. De las medidas preventivas; 13. Procedimiento civil; 14. De las denuncias ante el registro nacional de propiedad intelectual; 15. Disposiciones transitorias.

Puntualmente se afirma que esta ley garantiza los derechos morales y patrimoniales del autor y así también del intérprete. Sumado a lo dicho contempla las excepciones y limitaciones (uso gratuito o licencias no voluntarias) y también el caso de las obras extranjeras.

Por otro lado, se regula también la duración de la protección que brinda esta norma lo que implica garantizar por regla general, la vida del autor y 70 años contados desde el primero de enero siguiente a la fecha de su fallecimiento (artículo 5 de la ley 11.723).

Ahora bien, desde que se ha sancionado esta ley (año 1933) hasta la actualidad se pueden observar diversas modificaciones en el mundo con el surgimiento de la denominada revolución tecnológica, las que indudablemente repercuten en la aplicación de la legislación.

De esta manera, se afirma esto "(…) como lógica consecuencia del avance de la sociedad en materia de tecnología, y la permanente interacción de las manipulaciones de dichas tecnologías, las cuales pueden ser aplicadas con fines lícitos o no" (Cilleruel, 2006, p.1). De hecho, ya se ha hecho referencia a que la tecnología en la actualidad muchas veces no es utilizada con fines lícitos y es allí cuando surgen los nuevos delitos informáticos.

A modo de ejemplo el autor citado menciona a los reproductores y grabadores de discos compactos que actualmente son accesibles a costos no tan elevados. Sin embargo, algunos pocos deciden adquirirlos en las tiendas y utilizarlos con fines lícitos, mientras que otros optan por realizar copias de éstos de manera ilegal y venderlos en formato CD, DVD, etc. (Cilleruel, 2006).

Y esto sirve simplemente a modo de ilustración ya que en realidad en la actualidad existen cantidad de acciones que pueden resultar violatorias de los derechos protegidos por esta ley.

El propio artículo 72 de la ley 11.723 establece ciertos casos especiales de defraudación y entre ellos menciona el que edita, venda o reproduzca por cualquier medio una obra inédita o publicada sin autorización de su autor, así como también el que falsifique obras intelectuales, o el

que edita, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor o el título, etc. Imagínese la cantidad de casos en Internet en los que se publica material sin especificar el verdadero autor, incluso apropiándose de las ideas de otro en clara violación de lo contemplado en esta ley.

1.3 Ley de Protección de Datos Personales (Ley 25.326)

Esta ley, promulgada en octubre de 2000 tiene por propósito la protección integral de los datos personales, los que pueden hallarse en en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, tal como lo prescribe el artículo 1 de la citada norma.

Se afirma que esta ley ha venido a reglamentar el habeas data, establecido por el artículo 43 de la Constitución Nacional[9] y el 50 de la Constitución de la Provincia de Córdoba[10]. Asimismo, a través de sus artículos se garantiza el derecho al honor y a la intimidad de las personas y el acceso a la información que exista sobre ellas. Se incluyen los datos de personas física y también de personas jurídicas; y toda información que exista en archivos, registros, bancos de datos de carácter público o privado (Sain y Azzolin, 2017).

Además, afirman los citados autores que surge de la ley 25.326 el derecho a la información sobre la existencia de los archivos, a su finalidad y a la manera en que se realiza la transmisión de esos datos, sumado a que es posible conocer quién es el titular del registro. Se agrega asimismo la posibilidad de la rectificación de los datos que constan en estos registros.

En cuanto a su relación con el Código Penal, se conoce que mediante esta ley se ha incorporado al propio Código los artículos 117 bis y 157 bis (Sain y Azzolin, 2017).

Artículo 117 bis.

1°. (Inciso derogado por art. 14 de la Ley N° 26.388, B.O. 25/6/2008)

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

[9]Artículo 50 Constitución de la Provincia de Córdoba: "Toda persona tiene derecho a conocer lo que de él conste en forma de registro, la finalidad a que se destina esa información, y a exigir su rectificación y actualización. Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando tengan un interés legítimo.

La ley reglamenta el uso de la informática para que no se vulneren el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos".

2°. La pena será de seis meses a tres años, al que proporcionará a un tercero a sabiendas información falsa contenida en un archivo de datos personales. (…) (Artículo incorporado por art. 32 de la Ley N° 25.326 B.O. 2/11/2000)

Aquí queda regulada la proporción falsa de información que se halle en un archivo de datos personales y que haya sido realizada con total intención.

Mientras que el artículo 157 bis prescribe textualmente:

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 otra 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. (…)

(Artículo sustituido por art. 8° de la Ley N° 26.388, B.O. 25/6/2008)

Tal como se observa se penaliza aquí a quien violente sistemas de datos y acceda a ellos, o proporcione información registrada en un archivo o banco de datos, de manera ilegítima.

Pues bien, respecto de estos dos artículos agregados como consecuencia de esta Ley de Protección de Datos Personales, el Código Penal se actualiza en cierta medida a lo que la sociedad ha demandado. No obstante ello, debe pensarse en que hoy en día la protección de datos personales se torna aún más complicada ya que debe realizarse a través de los medios informatizados.

Es innegable la influencia de la tecnología para la facilitación en la comisión de delitos vinculados con la información. Piénsese lo fácil que es tener acceso ilegítimo a bases de datos y a todo tipo de información personal a través de la computadora y de la red en general.

1.4 Ley 26.388 de modificación de Código Penal

Como se ha indicado con anterioridad, la principal reforma que ha experimentado el Código Penal argentino en materia de delitos informáticos es aquella que ha sido consecuencia de la ley 26.388, que justamente se ha dado a conocer como Ley de modificación del Código Penal o en algunos casos Ley de Delitos Informáticos.

Esta norma ha introducido nuevos artículos y modificados algunos ya existentes para agregar al texto del Código las actualizaciones que la sociedad requería en base a los avances tecnológicos que ocasionan día a día nuevas figuras delictivas.

Al respecto la doctrina entiende que esta reforma no solo actualiza el Código Penal en relación a las lagunas legislativas que la jurisprudencia habría señalado, sino que implica asimismo un cambio de concepción en muchos conceptos legales que el avance tecnológico había dejado obsoletos (Palazzi, 2016).

Puntualmente en lo vinculado con la protección de delitos contra la seguridad de los medios de transporte y comunicación, por ejemplo, a través de la citada ley se amplía el concepto de comunicaciones protegidas por el artículo 197 del Código Penal.

> Artículo 197. - Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.
> (Artículo sustituido por art. 12 de la Ley N° 26.388, B.O. 25/6/2008)

Estos servicios cuando se redactó el Código Penal eran proveídos por el Estado en forma monopólica. Ahora en cuanto a las telecomunicaciones, la ampliación de éstas generó nuevos servicios que principalmente se hallan en manos del sector privado y que han desafiado la concepción de comunicaciones tradicionales (Palazzi, 2016).

Por lo tanto, la utilización de las nuevas tecnologías permite la comisión de actos ilegales que entorpecen o interrumpen las comunicaciones; entendidas éstas también como aquellas que se dan a través de celulares, computadoras y todo otro aparato conectado a la Red.

Asimismo, la reforma lograda mediante la ley 26.388 amplía las formas comisivas de la estafa e incluye el engaño de sistemas automatizados, cuando antes la jurisprudencia no permitía aplicar esta figura a ordenadores o máquinas automatizadas que no contaban con la intervención de personas. “De esta forma se reconoce que, debido a la informatización, muchos bienes y servicios se encuentran "custodiados" por computadoras y la manipulación a los fines de obtenerlos indebidamente es una defraudación” (Palazzi, 2016, p,8).

Por otra parte, el citado autor afirma que la ley en cuestión también modifica el delito de daño ya que se permite ahora el daño a bienes intangibles. Entre ellos se incluye, por ejemplo, el borrado de software o de datos contenidos en un ordenador, lo que en ciertos casos resulta tan o más perjudicial que la destrucción de documentos almacenados en soportes tradicionales. Sumado

a lo dicho, se incluye como delito el distribuir programas destinados a causar daños, por ejemplo, los virus informáticos. Además, se agregan dos agravantes relacionadas con la informática.

> ARTICULO 183. - Será reprimido con prisión de quince días a un año, el que (…).
>
> En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. (Párrafo incorporado por art. 10 de la Ley N° 26.388, B.O. 25/6/2008)

Continúa la doctrina citada y enuncia que otra de las modificaciones realizadas mediante esta ley 26.388 ha sido la ampliación del concepto de correspondencia que se hallaba amparada por los delitos de violación de secretos. Se agrega ahora al correo electrónico y a cualquier otra comunicación electrónica. De hecho, se afirma aquí que era imprescindible tipificar de manera expresa no solo a la interceptación, sino también al acceso y desvío de las comunicaciones electrónicas.

En suma, Palazzi (2006) expresa que las nuevas figuras, tales como el acceso ilegítimo a un sistema informático, o la unificación de los delitos introducidos por la Ley de Protección de Datos Personales, junto con el cambio de epígrafe del capítulo, generan una noción mucho más amplia de lo que se considera espacio digital amparado penalmente.

Ahora bien, a pesar de que esta legislación se destaca por la incorporación de diversas nuevas figuras delictivas- las que incluso serán profundizadas en los apartados siguientes- resulta posible afirmar que esta norma aún no ha logrado introducir una reforma omnicomprensiva. Al respecto enuncia la doctrina:

> Muchos de los nuevos delitos que requieren una respuesta, a veces de fondo y a veces procesal, no tienen una clara recepción en el código penal. Si bien pueden estar cubiertos por figuras más generales, siempre es necesario entender el nuevo fenómeno y resolverlo con las normas existentes (Palazzi, 2016, p.8).

De esta manera, es evidente que se necesita mayor esfuerzo legislativo para adecuarse a las nuevas tecnologías que invaden la sociedad actual. Se requiere de la tipificación de los delitos faltantes y de su regulación procesal que permita poner en práctica la prevención y control de estos actos ilegales. Esto quiere decir que la Argentina aún tiene mucho por hacer en materia penal si quisiera adaptarse y ser concordante con los parámetros que el derecho internacional ha demostrado en materia de delincuencia informática.

En este sentido, la doctrina citada explica que por ejemplo mediante la ley 26.388 no se ha legislado sobre el robo de identidad debido a que esta figura se consideraba cubierta en forma abarcativa por la estafa y la falsedad de documentos.

> Sin embargo, queda más que claro que en materia de robo de identidad existe un enorme vacío de parte del Estado en prevención y educación de usuarios de Internet y una real toma de conciencia de entidades financieras" El robo de identidad no se limita a obtener créditos de baja monta en entidades financieras con documentos falsificados. Hay robo de identidad y de claves en forma masiva, a través de phishing o nombres de dominio falsos. Todo esto afecta la seguridad del comercio electrónico y la seguridad y estabilidad de la infraestructura de Internet. Es un delito que analizado globalmente supera claramente a la víctima individual del caso concreto (Palazzi, 2016, p.8).

Pues en Argentina si bien existe este tipo de delitos, no tiene la misma dimensión que ha adquirido en los Estados Unidos. Sin embargo, implicaría un gran avance para esta sociedad la regulación de estas conductas si se considera que cada vez podrán tornarse más frecuentes y que sus perjuicios serán de gran magnitud.

Sumado a lo dicho, mediante esta modificación del Código Penal tampoco se ha legislado sobre la propiedad intelectual, materia ésta que se halla regulada por nuevos tratados internacionales como el Tratado de Derecho de Autor de la OMPI, y el Acuerdo de los Derechos de Propiedad Intelectual relacionados con el Comercio. Por lo tanto, resulta de gran importancia que al momento de legislarse dichas materias se cuente con normativa adecuada al respecto. Es decir que de manera especial se procure la protección del software, de las bases de datos, de las obras multimedia, del intercambio de archivos en redes peer to peer y sobre todo que se capacite a los cuerpos de investigación.

Finalmente, se destaca que los aspectos procesales vinculados con la cuestión probatoria no han sido abordados por esta ley, ya que en realidad sólo se ha procurado modificar el Código Penal en lo sustancial. Al respecto es evidente la necesidad de una adecuada reforma procesal penal que facilite la compresión y la investigación de la delincuencia informática. Ello así para dar por acabada y cerrar congruentemente el círculo de la legislación relacionada con el delito informático (Palazzi, 2016).

A continuación, se estudiarán puntualmente las figuras delictivas incorporadas a través de esta ley 26.388 del año 2000.

1.4.1 Distribución y tenencia con fines de distribución de pornografía infantil

En este aspecto la ley sustituye el artículo 128 del Código Penal por el siguiente.

> Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
>
> Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución y comercialización.
>
> Sera reprimido con prisión de (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

El artículo 2 de la ley 26.388 se halla dirigido a la tutela de los menores ante la difusión de pornografía por medio de las tecnologías de la información. Actualmente este tipo de delitos ha logrado una gran extensión ligada a la producción, publicación y distribución a causa del avance de las tecnologías, su fácil comisión y anonimato.

Esta disposición normativa incluye tanto la creación yla elaboración de imágenes, fotografías o representaciones de menores de edad, como el lucro de la misma y la facilitación de recursos de carácter material y humano para la organización de un negocio vinculado con este material.

Asimismo, se incluye aquí la oferta, venta, alquiler y distribución gratuita mediante soportes físicos (CD, DVD), sumado a la transmisión por Internet. “La tenencia personal a los fines de consumo no se encuentra incluida en esta figura, salvo que el material sea transmitido o cedido a otra persona” (Sain y Azzolin, 2017, p.95).

Al respecto, las nuevas tecnologías facilitan por sobremanera la extensión del tráfico de este tipo de material y la producción de estos contenidos. De hecho, el anonimato que provee Internet permite que los delincuentes utilicen las redes para gozar de las ventajas que éstas significan. Es decir, cuentan con el medio para la realización de la conducta ilícita sumado a la protección que le otorga el propio sistema informático por no dar a conocer la verdadera identidad.

Lo dicho queda en evidencia cuando se observa el incremento de procedimientos judiciales internacionales vinculados con la temática en los diversos medios periodísticos. Se agrega además que:

> Se trata de una actividad gravemente disvaliosa en la que la nota de globalización se ha acentuado justamente por la aparición de herramientas que permiten la configuración de verdaderas "redes" delictivas. Se trata, además, de un tema que genera alto nivel de consenso en cuanto a la necesidad de afrontarlo a nivel global, siendo muy importante la cantidad de documentos suscriptos sobre el particular (Altmark y Molina Quiroga, 2012, p.266).

1.4.2 Violación de correos electrónicos

En esta oportunidad mediante el artículo 4 de la ley 26.388 se ha modificado el artículo 153 del Código Penal, el que textualmente reza:

> Artículo 153: Sera 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 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 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 de tiempo de la condena.

Pues bien, este artículo refiere puntualmente al acceso indebido de comunicaciones de carácter privado, es decir, de acceso restringido. Se mencionan como ejemplo la violación de la privacidad en los casos en los que se ingresa con nombre de usuario y contraseña al correo electrónico de otro, o se accede al texto de un mensaje privado de una red social, chats personalizados, mensajes de texto o de servicios de mensajería por celular. Se incluye aquí a toda comunicación electrónica tanto texto como audio y video. Se destaca asimismo que el decir “apertura y acceso” implica específicamente tener acceso al contenido del mensaje y no a los sistemas que los contienen, como por ejemplo una casilla de mail (Sain y Azzolin, 2017).

En otras palabras, se afirma que en cuanto al correo electrónico y las modernas técnicas de comunicación “(…) se incluyen el clásico mensaje de correo electrónico, un chat, un fax, una llamada a través de VOIP o un mensaje de texto enviado de celular a celular” (Palazzi, 2016, p.11). Aquí el autor especifica que el mensaje no tiene que contener necesariamente la voz o caracteres

alfanuméricos, sino que también puede ser todo tipo de signo y gráfico e incluso ser audios o videos.

Ahora bien, al hablarse de comunicación electrónica, la ley de telecomunicaciones —ley 19.798 de 1972 define como "telecomunicación" a la “transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos" (Palazzi, 2016, p.11). En realidad, afirma el autor citado que mediante la utilización del término “comunicación electrónica” se incluye todo tipo de comunicación, o por lo menos las actualmente conocidas.

El legislador no se limitó al correo electrónico, sino que estableció un concepto de mayor extensión como el de comunicación electrónica.

Asimismo, la ley de inteligencia (n°25.250) enuncia en su artículo 5 respecto de las telecomunicaciones que:

> Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario (Palazzi, 2016, p.11).

Esto quiere decir que en esta conducta delictiva podrían quedar comprendidos distintos actos que día a día son frecuentes en la sociedad. Posiblemente el desviar la comunicación o suprimirla o modificarla no sea tan común, sin embargo, revisar o acceder al correo electrónico de otra persona o incluso tener acceso a los mensajes de texto del celular es un acto muy común para muchas personas.

Finalmente se agrega que el tipo penal- tanto para autores como Soler y como Núñez, especialistas en derecho penal- requiere ante todo que el acto sea cometido de manera indebida. Es decir, se funda el delito sobre una figura que excluye toda posibilidad de actuar culposo, por lo que la acción debe realizarse intencionalmente. Puntualmente Núñez, citado por Palazzi (2016) expresa que "El dolo del autor, a la par del conocimiento de ser una correspondencia dirigida a un tercero, exige la conciencia de que la abre sin derecho (…)” (p. 11).

Por el modo en que las tecnologías de la información avanzan constantemente se han comenzado a crear las condiciones apropiadas- dentro de la red – para que los delincuentes las aprovechen para la comisión de estos delitos caracterizados por los bajos costos y facilidad de acceso.

1.4.3 Acceso ilegítimo a sistemas informáticos

Por su parte, el artículo 5 de la ley 26.388 agrega al Código Penal el artículo 153 bis:

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

En este artículo a diferencia del anterior que hace referencia específicamente a las comunicaciones electrónicas, se alude aquí al acceso indebido y no autorizado a un sistema de carácter privado o restringido. Es decir, se incluye en este apartado a una casilla de correo electrónico, al perfil de una red social, a una cuenta de chat o cualquier otro archivo de carácter restringido y no público. De hecho, los programas espías que sirven para recopilar datos personales sin el consentimiento del dueño (usuario) quedan incluidos en esta figura delictiva, así como también el acceso a un dispositivo que requiera del uso personal y específico de un usuario (Sain y Azzolin, 2017).

Ahora bien, al hablar de "acceso restringido" se deja afuera la posibilidad de castigar el acceso a redes, sistemas y contenidos de sitios públicos. Para lo que se suma que además se deja fuera del ámbito típico de este artículo aquellas conductas que incluyan:

> a) la del testeo de seguridad de falencias de redes informáticas ("ethical hacking") en el marco de investigación académica, casera o empresaria, muchas veces realizado además con consentimiento de la "víctima", interesada en la detección de errores para su subsanación; b) la ingeniería inversa o reversa, que es la destinada a obtener información técnica a partir de un producto accesible al público (como programas de computación y componentes electrónicos), con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado, actividad que evidentemente no se relaciona con la "privacidad" sino, a todo evento, con la protección de la propiedad intelectual (Altmark y Molina Quiroga, 2012, p.271).

Por último, la doctrina agrega que aquí el bien jurídico protegido es la reserva, sumado a la confidencialidad y el derecho a la privacidad del titular del sistema y del dato informático (Altmark y Molina Quiroga, 2012).

1.4.4 Daño informático y distribución de códigos maliciosos

En este título se analizará la incorporación, a través del artículo 10 de la ley 26.388, del segundo párrafo del artículo 183 del Código Penal argentino. Textualmente se especifica: "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

En este sentido se afirma que la ley bajo análisis ha venido a cerrar una de las polémicas antiguas relacionadas con el alcance de los tipos penales tradicionales para incluir las nuevas modalidades de comisión de delitos que son generadas por los avances de la tecnología.

En cuanto al daño puntualmente, ciertos autores entendían que bajo el artículo 183 del ordenamiento penal [11] ya se comprendían los daños informáticos al hablarse de cosas muebles. Ello así ya que los propios tribunales consideran "cosa" a la electricidad, a los pulsos telefónicos e incluso a las señales de televisión o de cable (Altmark y Molina Quiroga, 2012).

Por lo tanto, se podría incluir dentro de este artículo a algunas de las actividades que desarrollan los conocidos *cracker*s y *cyberpunk* (vándalos). Sin embargo, surgió la necesidad de acabar con analogías y de decidir si se reformaría dicho artículo y se agregaría a la frase "(...) cosa mueble o inmueble o un animal (…)" la palabra "intangible" para incluir los daños informáticos o si se dictaría una nueva ley especial al respecto (Altmark y Molina Quiroga, 2012).

Surge evidente que la solución ha sido la modificación de dicho artículo 183, al que se le ha agregado un párrafo específico- citado con anterioridad- vinculado con los daños causados en los sistemas informáticos.

1.4.5 Interrupción de comunicaciones o DoS.

Finalmente se destaca de la ley 26.388 el artículo 11 que sustituye el artículo 197 del Código Penal, el que queda redactado de la siguiente manera: "Artículo 197: Será reprimido con

[11] Artículo 183 Código Penal: "Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado.
En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. (Párrafo incorporado por art. 10 de la Ley N° 26.388, B.O. 25/6/2008)".

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".

El artículo comprende comunicaciones de diversos tipos, tutela las públicas y las privadas.

En este sentido, se incluye -según la doctrina- a los ataques de denegación de servicio, dentro de lo vinculado con las comunicaciones mediadas por las computadoras. Esto significa el ataque de varias computadoras contra otros dispositivos con el propósito de ralentizar y obstruir sus comunicaciones. El *hackeo* a una página web es el claro ejemplo de estas conductas.

En realidad, se contempla dentro de este tipo delictivo a:

> Cualquier ataque que afecte el software y hardware de un dispositivo utilizado para establecer comunicaciones, como un celular o cualquier factor que altere o impida la comunicación entre personas a través de correo electrónico, comunicaciones de audio por internet, video conferencias y sistemas de mensajería por celular, entre otros (Sain y Azzolin, 2017, p.100).

Para agregar a lo dicho, se especifica que el llamado DDoS (siglas en inglés de *distributeddenial of service*, denegación de servicio distribuida) es una ampliación del ataque DoS. Consiste puntualmente en instalar varios agentes remotos en muchas computadoras, que se encuentren incluso ubicadas en distintos puntos geográficos. Lo que hace el invasor es coordinar los agentes para amplificar el volumen o saturación de la información, de manera masiva. De hecho, se conoce que han sido posibles casos de ataques de cientos o millares de computadoras dirigidos a una máquina o red objetivo.

No obstante, la magnitud del daño que se causa con esta conducta, el número de denuncias es bajísimo:

> (…) 58% de los ISP afectados optaron por no denunciar el hecho. El motivo de la falta de denuncias en algunos casos se fundó en que las fuerzas prevencionales tienen limitadas capacidades de reacción ante estos hechos (29%); en otros, que esperaban que fueran los clientes de los ISP quienes hicieran la denuncia (26%), y finalmente en que informar estos ataques carece de utilidad alguna (17%) (Palazzi, 2016, p.15).

Finalmente se especifica que esta técnica viene a ser una de las más eficaces y sencillas a la hora de colapsar servidores. La tecnología distribuida permitió causar daños impensados y serios a aquellas personas con escaso conocimiento técnico.

No obstante, ello la doctrina especifica que este artículo no comprende a los ataques informáticos que afecten a otros servicios públicos distintos de los medios de comunicación, como

así tampoco a los ataques a sistemas informáticos que no se relacionen con la comunicación (Palazzi, 2016).

1.5 Ley sobre grooming (Ley 26.904)

Esta nueva legislación tiene por finalidad incorporar al Código Penal el delito de acoso sexual por Internet a menores de edad, conocido como *"grooming*" o "ciberacoso" sexual. Este consiste en el establecimiento de penas para aquellos quienes contacten a chicos por la Web con ese fin.

La norma es la número 26.904 y fue sancionada el 13 de noviembre de 2013 por el Senado.[12] Tal como se observa es ésta una ley actual, lo que demuestra cierta preocupación legislativa por avanzar en la regulación de delitos informáticos, como lo es el *grooming*.

Puntualmente esta ley incorpora como artículo 131 del Código Penal el siguiente texto:

> Artículo 131: "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* -traducción de la palabra "acicalamiento" en inglés- se define como aquella acción de captar y manipular a menores de edad a través del uso de la Red y con claros propósitos sexuales. Es decir, es el proceso que encamina una persona adulta para ganarse la confianza de un menor de edad por vía de Internet, esto es a través de chats, redes sociales, juegos o servicio en línea. Asimismo, se destaca que para lograr su cometido el delincuente simula ser otro menor (Sain, 2018).

En este sentido, este tipo delictivo no es una figura nueva, de hecho, se conoce que es ésta la técnica utilizado por los pedófilos para minar o socavar moral o psicológicamente al niño con el objetivo de controlarlo emocionalmente y cuyas características son claramente aquellas que se asocian con el acoso.

Sumado a lo dicho, el *grooming* no es una simple tentativa de abuso sexual; en realidad se afirma que a priori es:

[12] Fuente: "Internet. Promulgaron la ley de grooming" (11/12/2013). *Diario Clarín*. Recuperado el 21/07/18 de https://www.clarin.com/sociedad/promulgaron-ley-grooming-ciberacoso_0_rJL8rIWiDmx.html

> (…) acoso sexual infantil realizado por un pedófilo que mediante el engaño y la extorsión se aprovecha de la vulnerabilidad de los menores para diferentes fines, entre los que puede incluir el abuso o la violación en un posterior encuentro con la víctima o la inducción para que el niño, niña o adolescente se desnude frente a la webcam para producir material de contenido sexual para consumo personal y/o distribución o venta en la dark web -redes ocultas y encriptadas de internet (Sain, 2018, p.1).

Por su estructura, esta legislación sólo cuenta con dos artículos. El primero de ellos es el citado al inicio de este apartado que modifica el artículo 131 del Código Penal y tipifica así la conducta delictiva, mientras que el segundo simplemente ordena la comunicación al Poder Ejecutivo para su publicación. Esto demuestra que en realidad este delito ha sido conceptualizado para que sea incorporado al ordenamiento penal, aunque no se ha precisado demasiado al respecto. De hecho, entre las lagunas o vacíos de la ley quedará pues a libre interpretación del aplicador de la ley, por ejemplo, qué se entenderá por "contactar a un menor".

No obstante ello, se destaca el avance que la sociedad de la mano del derecho logra al incorporar figuras delictivas tan novedosas como la aquí planteada, en protección de las víctimas de las tecnologías que día a día aumentan su número.

1.5.1 El caso del Club Independiente

A comienzos de este año 2018 se comenzó a sentir en todos los medios de comunicación-televisión, páginas web, radio y sobre todo periódicos- noticias vinculadas con supuestos casos de abuso sexual en menores por parte de miembros del Club Independiente. De la mano con la investigación, sale a viva voz la comisión del delito de *grooming* acompañado con el de abuso sexual.

El caso surge con la denuncia de Fernando Berón, coordinador de las Inferiores de Independiente, quien relata que una de las víctimas habría sido abusada. El menor confesó al psicólogo de la pensión los actos que habría padecido tanto él como varios de sus compañeros. El profesional recurrió al coordinador para dar a conocer los hechos y éste presentó la denuncia en marzo del año en curso (2018).

Como consecuencia, desde aquél día la justicia investiga los supuestos delitos de abuso sexual y promoción y facilitación de la prostitución, a lo que se sumó el delito de *grooming*.

Entre los relatos de las víctimas se hablan de hechos aberrantes de prostitución que implicarían la actuación en red, que consistían en trasladar a los menores a departamentos o a un hotel (los que han sido allanados) para que allí mantuvieran relaciones sexuales con los pedófilos, a cambio de dinero, de crédito en la tarjeta SUBE y hasta incluso a cambio de pasajes de colectivos y vestimenta. [13]

Con el paso del tiempo, de la investigación de los hechos resulta que, salvo el abogado de uno de los imputados a quien se lo ha despojado de su libertad por el delito de encubrimiento, todos los restantes implicados se hallan investigados por los hechos caratulados como "Abuso Sexual en Concurso Ideal con la Corrupción de Menores" y que llegarían a ser 500 las víctimas de estos hechos. [14]

Ahora bien, con claro criterio jurídico la Fiscal del caso imputó a algunos de los responsables del delito de *grooming*. Al respecto, los medios periodísticos especifican para que el lector comprenda que es ésta una figura penal incluida en el artículo 130 del Código Penal en el año 2013 que incluye penas de prisión de seis meses a cuatro años. Afirman estas fuentes: "Según la ley, el *grooming* es "el acoso contra menores por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".[15] A lo que se agrega que durante la investigación se han encontrado 120 perfiles de redes sociales que se investigarán para determinar los casos de este ilícito.

En este sentido, la institución "*Grooming Argentina"* afirma que el acoso sexual de niños, niñas y adolescentes es un problema real que crece en los últimos meses y que ha adquirido visibilidad a raíz de la difusión de las denuncias que surgieron hacia el Club Atlético Independiente. Afirma el presidente de esta institución que las tareas realizadas por la Fiscal y el Procurador han sido excelentes en cuanto a la tipificación de estas conductas como *grooming* ya

[13] Fuente: "9 claves para entender el escándalo de abuso de menores de la pensión de Independiente" (22/03/18). *Infobae*. Recuperado el 26/07/18 de https://www.infobae.com/deportes-2/2018/03/22/9-claves-para-entender-el-escandalo-de-abuso-de-menores-de-la-pension-de-independiente/

[14] Fuente: "El caso Independiente destapó la red de pedofilia más grande de Argentina: habría 500 menores afectados" (30/03/18) *La Nación*. Recuperado el 26/07/18 de https://www.infobae.com/deportes-2/2018/03/30/el-caso-independiente-destapo-la-red-de-pedofilia-mas-grande-de-argentina-habria-500-menores-afectados/

[15] Fuente: Escándalo sexual en Independiente: creen que filmaban a menores teniendo sexo con adultos (13/04/18). *La Nación*. Recuperado el 26/07/18 de https://www.lanacion.com.ar/2125266-escandalo-sexual-en-independiente-creen-que-filmaban-a-menores-teniendo-sexo-con-adultos

que aquí se busca priorizar la protección integral y la no revictimización de los adolescentes abusados.

> El #Grooming es un delito que trasciende a las cuestiones deportivas, que atraviesa todos los estratos sociales; omnipresente en el día a día. Es una problemática que se está instalando y creciendo silenciosa y considerablemente en nuestro país, de la que tenemos que hablar y enfocar desde todos los estamentos del Estado. Los pedófilos encontraron un nuevo método también, de captación, lo que significa la puerta de entrada para cometer delitos aberrantes cómo la trata de personas, abusos con acceso carnal o crímenes (Navarro, 2018, p.2).

Al respecto se agrega que la gravedad de este delito se halla en la naturaleza de la problemática: esto es una nueva modalidad de abuso sexual infantil en la que no hace falta el contacto físico, el abuso es digital (Navarro, 2018).

Se demuestra así, tal como se ha dicho, que el *grooming* no es una tentativa de delito, sino que constituye un delito en sí. De hecho, el menor ya ha sido perjudicado desde el momento en que se dan a través de Internet los actos de acoso.

2. Análisis jurisprudencial sobre delitos informáticos

En esta oportunidad se describirán brevemente algunas causas vinculadas con la comisión de delitos informáticos que por algún motivo- que ya se destacará- han merecido este análisis. Se intenta aquí demostrar mediante casos concretos las decisiones de la justicia a la hora de juzgar este novedoso fenómeno que, en pocos años, si no se lograra controlar, podría invadir los tribunales de este país.

2.1 Causa: "Castelo, Pablo Alejandro s/ recurso de casación"

La Cámara Federal de Casación Penal ha resuelto esta causa caratulada "Castelo, Pablo Alejandro s/ recurso de casación"[16], con fecha 16 de junio de 2015, luego de haber sido elevada por la defensa quien resultó condenada por el Tribunal Oral en lo Criminal n° 18 el 10 de octubre de 2014.

[16]Cám. Fed. Casación. Sala III. (2015). "Castelo, Pablo Alejandro s/ recurso de casación" AR/JUR/24390/2015

Los hechos que se le imputan al condenado en primera instancia constan de la realización, fuera del país, de una transferencia indebida de dinero entre cuentas bancarias, lo que se tipifica como supuesto de defraudación mediante técnicas de manipulación informática en calidad de autor *(phishing)*.

La defensa alega la incapacidad técnica de su defendido, sin embargo, ésta no se corresponde con las tareas que desempeñaba a favor de su empleador ni con su carácter de estudiante universitario de ingeniería en sistemas.

Puntualmente el Tribunal Oral en lo Criminal n° 18 resolvió condenar a P.A.C. por ser autor penalmente responsable del delito de defraudación mediante técnicas de manipulación informática. La pena que decidió imponer fue de un año de prisión en suspenso y costas. Sin embargo, contra esta resolución la defensa de P.A.C. interpuso recurso de casación.

Los argumentos para sostener este recurso se fundaron principalmente en que el conocimiento de informática que tenía el supuesto autor – era programador- no implica el manejo o semejante capacidad como para realizar la maniobra que se le atribuye, la que se conoce como *"phishing"*.A esto el abogado defensor le suma el hecho de que durante todo el proceso judicial se ha intentado invertir la carga probatoria para que su defendido sea quien haya tenido que brindar las pruebas para demostrar su inocencia, lo que implicaría violentar el principio constitucional de presunción de inocencia.

Ahora bien, en cuanto los hechos, se ha acreditado que P.A.C. a través de la manipulación indebida de datos informáticos obtuvo el usuario y contraseña de M. C. B., (titular de la cuenta n°... del Banco Francés), para realizar una transferencia de capitales mediante el sistema "home banking Frances-net". Esta operación ha sido por la suma de pesos $3.000 hacia la cuenta bancaria nº... que D. O. A. poseía en la misma entidad bancaria, desde la cual el dinero fue retirado por el nombrado.

Respecto a la valoración del Tribunal, para tener por aprobado el hecho imputado ha considerado la declaración testimonial de M.C.B., junto con los informes emitidos por el Banco Francés y por el Área Especial de Investigaciones Telemáticas de la Policía Metropolitana, sumado a los informes de Telefónica Argentina y de la firma "Google Inc.".

Precisamente el denunciante M.C.B. confirmó ser titular de la cuenta del Banco Francés y que al ingresar al sistema electrónico de dicha entidad pudo corroborar un faltante de tres mil pesos ($3.000) que habían sido transferidos a la cuenta de ahorro de D. O. A. Asimismo la

documentación aportada por el Banco permitió constatar que al seguirse la ruta del dinero se pudo detectar la manipulación indebida de los datos informáticos que permitían acceder a esa cuenta y que la operación habría sido realizada desde el exterior; precisamente desde la ciudad de Guadalajara, México. Fue por ello que el titular de la cuenta corriente tuvo que modificar sus datos de usuario y la contraseña.

Por lo tanto, luego de haberse analizado las pruebas aportadas: testigos, documentación, informes, etc.- que no merecen aquí ser detalladas en profundidad- el Tribual de juicio pudo concluir que, de la totalidad de los elementos aportados, analizados en su conjunto, se puede afirmar que P.A.C. se ha manifestado en "forma mendaz, brindando una mera excusa como para intentar una posición más favorable en su comprometida situación procesal".

De hecho, las pruebas no permiten otorgar verosimilitud al descargo efectuado por P. A. C., quien afirmó que el origen de las sumas de dinero depositadas en la cuenta bancaria de su amigo y compañero laboral, D. O. A. habría sido la venta de software. No obstante ello, no pudo localizarse el supuesto comprador ni se hallaron registro alguno de las llamadas telefónicas del imputado con el teléfono de esta persona. Asimismo, se suma las contradicciones testimoniales que acreditaron que su compañero de trabajo y amigo no tenía conocimiento de los supuestos trabajos *"freelance"* (la venta del software) y el hecho de que P.A.C. no utilizó su propia cuenta bancaria, aunque fuera de otro Banco.

De esta manera, y una vez analizadas todas las pruebas vertidas en el juicio, la Cámara Federal afirma que existen prueba suficiente para tener por acreditada la autoría de P. A. C. en el hecho materia de estudio. A lo que se suma que estos elementos probatorios ya habrían sido valorados correctamente por el Tribunal inferior.

Como consecuencia, debido a que la sentencia impugnada se encuentra correctamente fundamentada de conformidad con lo dispuesto por los arts. 123 y 404 inc. 2° del C.P.P.N., corresponde rechazar el planteo efectuado por la recurrente.

Esto implica resumir que la sentencia que condenó al imputado por el delito phishing se ha confirmado, ya que se ha comprobado "(…) la relación lógica entre las distintas piezas probatorias a través de las cuales se pudo averiguar que había sido aquel quien, mediante manipulaciones informáticas, había extraído indebidamente fondos de la cuenta bancaria del damnificado".[17]

[17]Cám. Fed. Casación. Sala III. (2015). "Castelo, Pablo Alejandro s/ recurso de casación" AR/JUR/24390/2015

Finalmente, respecto de este fallo se destaca el correcto criterio de la Cámara de penalizar conductas como la descripta, para sentar jurisprudencia al respecto y evitar que estos delitos informáticos queden impunes y por ende adquieran mayor relevancia. No debe olvidarse que la tecnología es una herramienta que, así como provee a la sociedad de innumerables ventajas, también ocasiona daños impensados y a grandes escalas. Por lo tanto, si no se actúa para evitar conductas ilegales como la aquí analizada, en poco tiempo el número de víctimas crecerá a pasos agigantados.

2.2 Causa "C. A. Q".

Con fecha 3 de noviembre de 2009 la Cámara Nacional de Apelaciones en lo Criminal y Correlacional decide revocar el sobreseimiento dictado por Sr. Juez de grado de la causa en que se investigaban los hechos de difusión- mediante correos electrónicos- de un documento informático apócrifo, que consistía en un informe reservado del Poder Ejecutivo Nacional.[18]

El Fiscal interpone recurso de apelación contra la resolución dictada por el Juez quien ordenó sobreseer a C.A.Q -propietario de la computadora en la que se encontró dicho documento- debido a la imposibilidad de acreditar que el acto hubiere sido generado en ella. No obstante lo dicho, resulta necesario indagar sobre ciertos aspectos que hacen a la individualización de la forma en que el archivo ingresó al equipo del imputado.

Precisamente a juicio de la Cámara la resolución cuestionada es prematura ya que los elementos aportados en la investigación aún no permiten descartar la materialidad del hecho denunciado ni que C.A.Q. no haya tenido participación en él.

La conducta delictiva que se investiga aquí es la amplia difusión a través de correos electrónicos de un documento informático apócrifo, que aparentemente sería un informe reservado del Jefe de Gabinetes de Asesores del Secretario de Finanzas. En éste constaría la viabilidad de un plan de financiamiento económico de emergencia a través de la incautación de fondos en diferentes plazas del país. "Según la información registrada en ese archivo digital, el documento que circuló habría sido generado en una computadora del imputado de la empresa Intelap S.A".[19]

[18]Cám. Nac. de Apel. En lo Crim. y Corr. Sala II. "C. A. Q". (2009). AR/JUR/43986/2009

[19]Cám. Nac. de Apel. En lo Crim. y Corr. Sala II. "C. A. Q". (2009). AR/JUR/43986/2009

A pesar de que los peritajes comprobaron que el archivo informático se hallaba guardado en ese equipo, no había otros con logos e inscripciones oficiales que permitieran acreditar que el documento en cuestión haya sido creado en la computadora secuestrada por orden del juez de instrucción.

Por lo tanto, comprobada esta circunstancia no es posible descartar por completo la hipótesis delictiva que se denuncia. En realidad, será necesario indagar en profundidad respecto de la individualización de la forma en que ingresó el archivo informático al equipo del imputado. Será menester incluso determinar si ha sido enviado por correo electrónico desde dicha computadora y si lo ha sido de manera masiva.

Como consecuencia el Fiscal considera que los elementos son insuficientes para descartar la materialidad del hecho y por ello decide recurrir el sobreseimiento. Así, luego del análisis expuesto la Cámara consideró apropiado "revocar el sobreseimiento dictado hasta tanto el a quo lleve a cabo todas las medidas expuestas y las que considere necesarias para la investigación de la causa".

Al respecto resulta esencial destacar que el criterio de revocar el sobreseimiento resulta apropiado cuando en realidad aún existen elementos que pueden ser indagados y que podrían acreditar la autoría del hecho. En la actualidad, la delincuencia informática ocasiona daños impensados y a grandes escalas, pues permitir que situaciones queden en "escalas de grises" contribuiría a la impunidad de estas conductas que día a día perjudican a la sociedad en mayor medida. Por lo tanto, continuar con la investigación del caso parece ser la mejor resolución.

Conclusiones parciales

En este último capítulo se ha profundizado el análisis legislativo del ordenamiento jurídico argentino, el que incluye por un lado el Código Penal argentino originario y por el otro las leyes específicas de Propiedad Intelectual y de Protección de Datos Personales.

Asimismo, y, sobre todo, se ha analizado aquí la ley 26.388 de modificación de Código Penal, a través de la que se introdujeron ciertos delitos informáticos a la legislación argentina. Se pudieron precisar distintas figuras delictivas entre las que se destacan la distribución y tenencia

con fines de distribución de pornografía infantil, la violación de correos electrónicos, el acceso ilegítimo a sistemas informáticos, el daño informático y distribución de códigos maliciosos y la interrupción de comunicaciones o DoS1.5.

Finalmente se estudió la reciente legislación sobre *el grooming*, figura ésta que ha adquirido especial relevancia este año luego del caso del Club Atlético Independiente.

Por último, se relataron brevemente dos causas de la justicia penal en las que el Tribunal ha tomado la resolución adecuada en miras a la protección de las víctimas de delitos informáticos.

Al comienzo de esta investigación se planteó la hipótesis que afirmaba que mediante la ley 26.388 que ha modificado el Código Penal Argentino parecería no haberse logrado adecuar las normas internas a los parámetros internacionales de regulación y control de los delitos informáticos. A esta altura, y ahora sí con certeza, resulta posible corroborar lo planteado.

Deben destacarse las innumerables ventajas de haber agregado al Código Penal ciertas conductas delictivas vinculadas con la informática; sin embargo, tal como se observó, los parámetros internacionales en la materia alcanzan otro nivel digno de imitación.

No resulta suficiente legislar algunos delitos informáticos, sino que además deben reglamentarse y deben preverse los aspectos procesales vinculados con esta nueva forma de delincuencia.

Conclusión final

El desarrollo tecnológico se ha vuelto el motor de la vida de las personas, la transforma y es fundamental para el avance de la sociedad en su conjunto. No obstante lo dicho, su mal uso acarrea consecuencias que no sólo invaden todo los ámbitos sino que impactan por sobremanera en perjuicio de los derechos de los ciudadanos.

En este trabajo se ha indagado respecto a esta nueva modalidad de comisión de delitos, que permite que los delincuentes actúen desde cualquier lugar geográfico e incluso con total reserva de su autoría. Internet es una herramienta de gran valor y repleta de ventajas para las personas, pero su utilización indebida puede causar daños impensados.

Ahora bien, a lo largo de este trabajo se han desarrollado aspectos vinculados con los delitos informáticos, ya que se cree que el mayor conocimiento de éstos contribuye a que la sociedad sea día a día menos víctima de estos actos.

Puntualmente en cuanto a la estructura de esta investigación, tal como se observa, en el primer capítulo se han estudiado las primeras aproximaciones sobre este tipo de ilícitos. Se definió a los delitos informáticos y se describieron sus principales características, así como también se desarrollaron los sujetos intervinientes en estos hechos: el delincuente, con sus cualidades específicas que implica cierto conocimiento profesional, y la víctima. Asimismo, se analizaron a los sistemas informáticos como medios de comisión de estos delitos, principalmente el correo electrónico, los mensajes de texto y las redes sociales.

En el segundo capítulo se analizaron los principales delitos vinculados con las tecnologías. Su definición y caracterización les permite a las víctimas identificarlos para denunciarlos, o en caso de ser posible, para evitar padecerlos. En este sentido, se indagó sobre la estafa informática, el fraude, el sabotaje informático, el ciberterrorismo, las calumnias e injurias, el espionaje informático, ente otros delitos informáticos.

Sumado a lo dicho, se brindó una clasificación de estas figuras delictivas, para lo que se procedió a distinguir la utilización de la tecnología como instrumento o medio para cometer los delitos informáticos (por ejemplo, el fraude informático); del uso de ésta como fin u objetivo (esto es, por ejemplo, hackear una computadora); y de otras clasificaciones brindadas por distintos autores y organismos como la ONU.

Luego, en el capítulo tercero se ha brindado un análisis legislativo del derecho internacional sobre la materia en cuestión. Se describieron las normativas provenientes de la Organización de las Naciones Unidas (ONU) y sobre todo las disposiciones debatidas en los distintos Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Se pudo observar aquí el trabajo incansable de estos Congresos en lo vinculado con la delincuencia y el establecimiento de la paz y de la seguridad de las personas.

En suma, en materia de derecho comparado el delito informático ha sido estudiado en profundidad en la Unión Europea, puntualmente a través del Convenio de Budapest. Este instrumento internacional se destaca por contener distintas disposiciones que invitan a que todos los países miembros en conjunto, cooperen para erradicar la delincuencia informática. Por último, en este capítulo se describió brevemente la recepción legislativa que comprenden las leyes internas de países que se han destacado en sus ordenamientos jurídicos sobre delincuencia vinculada con la tecnología, entre ellos, Estados Unidos, Francia, Alemania, Reino Unido, España, etc.

Finalmente, en el último capítulo de este trabajo se hizo hincapié en la regulación legislativa y jurisprudencial del derecho interno argentino.

En primer lugar, se describieron los aspectos que el originario Código Penal contenía, por lo que se destacó que sus normas eran acordes a la realidad que se vivía hace más de 80 años. Luego se describieron ciertas leyes que con el paso del tiempo ha surgido para regular aspectos particulares que de cierta manera se relacionan con la informática, entre ellas la Ley de Propiedad Intelectual (Ley 11.723) y la Ley de Protección de Datos Personales (Ley 25326).

Asimismo, se estudió en este capítulo a la Ley 26.388 de modificación de Código Penal, la que se destaca por su gran aporte en materia penal y sobre todo en delitos informáticos. De hecho, tal como se analizó, esta legislación contribuyó con la tipificación de conductas delictivas que hasta aquél momento (2008) no se hallaban contempladas expresamente en el ordenamiento penal. En este sentido, se describieron las conductas de distribución y tenencia con fines de distribución de pornografía infantil, violación de correos electrónicos, acceso ilegítimo a sistemas informáticos, daño informático y distribución de códigos maliciosos e interrupción de comunicaciones o DoS1.5. Esto por supuesto no significa que actualmente sean sólo éstas las conductas típicas penales relacionadas con el uso de las tecnologías, sino que en realidad en esta modificación del 2008 los legisladores decidieron incluir a las citadas, tal vez porque eran las más frecuentes en dicho momento.

Sumado a lo dicho, se describió en este capítulo la ley del *grooming*, figura ésta que se destaca por ser actual (año 2013) y por haberse hecho conocer a través del reciente caso del Club Atlético Independiente, vinculado con el abuso sexual de menores mediante el uso de las tecnologías; tal como se ha desarrollado.

Por último, se brindó un breve análisis jurisprudencial de dos causas penales en las que los magistrados han dado la debida importancia al juzgamiento de los delitos informáticos de *phishing* y de difusión- mediante correos electrónicos- de un documento informático apócrifo.

Ahora bien, para finalizar resta retomar los aspectos planteados al comienzo de este trabajo. Se planteó en aquél momento el objetivo principal que consistía en indagar si mediante la ley 26.388 que modificó el Código Penal argentino, el legislador habría logrado adecuar sus normas internas a los parámetros internacionales respecto a la regulación y control de los delitos informáticos. A lo que se sumaba el interrogante de si el ordenamiento jurídico argentino brinda las herramientas necesarias que permitan controlar la comisión de delitos producidos mediante el uso de nuevas tecnologías.

Pues bien, una vez desarrollados todos los temas aquí tratados resulta posible dar por corroborada la hipótesis. De hecho, la ley bajo análisis (ley 26.388) ha significado un gran avance en materia de delincuencia informática, ya que mediante sus disposiciones el Código Penal se ha adecuado, en cierta forma, a los cambios que la sociedad demandaba. No obstante, ello, se entiende que aún queda mucho trabajo por delante si se pretende que las normativas argentinas se adecuen a los parámetros internacionales existentes en materia de ciberdelincuencia.

Se ha estudiado la legislación internacional y se pudo observar que los países del primer mundo- y no en vano lo son- ya cuentan desde hace varios años con la reglamentación apropiada que incluye tanto a los delitos cometidos mediante la utilización de la tecnología como a aquellos cuyo objetivo son los propios sistemas informáticos. Al respecto, se destaca lo estudiado sobre los Congresos de la ONU en materia de delitos y justicia penal o el destacado Convenio de Budapest de la Unión Europea. Allí, tal como se ha dicho, las normas sobre delitos informáticos son abarcativas no sólo de la definición de sus conceptos sino de la tipificación de muchas otras figuras que Argentina aún no ha contemplado y de las normas procesales que permiten poner en práctica la prevención y control de la delincuencia de este siglo. Así como también estos instrumentos internacionales incluyen normas de cooperación entre los distintos Estados que permitirían erradicar este tipo de delitos.

En realidad, el avance que hasta la actualidad Argentina ha realizado en materia de delitos informáticos podría decirse que ha sido en respuesta de un intento de adecuación a la normativa internacional. Estos delitos no tienen fronteras, por lo tanto, la solución requiere de coordinación entre los distintos países a la hora de sancionar estas conductas. Es posible afirmar entonces que ya es hora de pensar en la creación de normas con un núcleo común y en la unificación de criterios para erradicar este tipo de crímenes.

Consecuentemente, la hipótesis de este trabajo ha sido claramente acertada, lo que implica reafirmar que, aunque el ordenamiento jurídico argentino ha logrado con la sanción de la ley 26.388 un avance en materia de delitos informáticos, lo allí contemplado no resulta suficiente. Es decir, no se ha logrado aún tipificar todas las figuras delictivas que se tornan día a día más frecuentes en la sociedad actual y no se cuenta con las herramientas que permitan poner en práctica el control de este novedoso tipo de delitos.

Producto de estos comentarios es que se considera que un avance legislativo interno de la Argentina contribuiría en gran medida a la erradicación de estas conductas ilegales.

Esto es, debería pensarse en una ley específica en la materia de ciberdelincuencia o al menos en una nueva modificación del Código Penal que incluya todos los delitos informáticos que hoy en día son frecuentes e incluso las normas procesales pertinentes. A la vez, deberá procurarse la unificación de criterios, para adecuar la normativa interna argentina a las normas internacionales ya existen.

Tal vez con una consecuente reforma del Código Procesal Penal que contemple, por ejemplo, las disposiciones vinculadas con las pruebas digitales. En este último aspecto se agrega que se torna necesario avanzar en la legislación procesal argentina para estarse acorde a las nuevas herramientas que aportan las tecnologías de la información y la comunicación (Rivolta, 2007).

De esta manera, se invita a la reflexión aquí planteada y se intenta que con todo lo desarrollado al menos la sociedad actúe de manera un poco más precavida en su relación con la tecnología, justamente para evitar ser víctima de los delincuentes informáticos que muchas veces no encuentran barreras ni límites en su actuar delictivo.

Listado de bibliografía

1. Doctrina

Abogados porta ley (2008). La incorporación de los delitos informáticos al Código Penal argentino. *Delitos Informáticos.com.* Recuperado el 01/05/18 de https://delitosinformaticos.com/06/2008/noticias/la-incorporacion-de-los-delitos-informaticos-al-codigo-penal-argentino

Abogados porta ley (2013). Estafas en internet. Delitos informáticos.com. Recuperado el 01/06/18 de https://delitosinformaticos.com/04/2013/fraudes/estafas-en-internet

Abogados porta ley (2014). Se pueden manipular conversaciones de whatsapp y sms con aplicaciones. *Delitos Informáticos.com.* Recuperado el 02/05/18 de https://delitosinformaticos.com/08/2014/seguridad-informatica/se-pueden-manipular-conversaciones-de-whatsapp-y-sms-con-aplicaciones

Abogados porta ley. (2013). Calumnias e injurias en Internet. *Delitos informáticos.com.* Recuperado el 11/17/18 de https://delitosinformaticos.com/10/2013/noticias/calumnias-e-injurias-en-internet

Abogados portaley. (s/f). El delito de espionaje por medios electrónicos. *Portaley.com.* Recuperado el 12/07/18 de http://www.portaley.com/delitos-informaticos/espionaje.shtml

Acurio Del Pino, S. (2015) Delitos informáticos: generalidades. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

AE Tecno (2018). Radiografía a las estafas por whatsapp: la lucrativa práctica que sigue dejando víctimas. Recuperado el 02/05/18 de https://tecno.americaeconomia.com/articulos/radiografia-las-estafas-por-whatsapp-la-lucrativa-practica-que-sigue-dejando-victimas

Alfocea, J. (2015) Ciberdelitos: robo de identidad, phishing y spamming. *Delitos informáticos.net.* Recuperado el 12/07/18 de https://delitosinformaticos.com/04/2015/delitos/ciberdelitos-robo-identidad-phishing-spamming

Alfocea, J. (2016) Internet también es escenario para el delito de coacciones. *Delitos informáticos.net.* Recuperado el 12/07/18 de https://delitos-informaticos.net/delitos/coacciones/internet-tambien-es-escenario-para-el-delito-de-coacciones

Altmark, D. y Molina Quiroga, E. (2012) *Tratado de Derecho Informático.*Tomo III. (1ª Ed.). Buenos Aires: La Ley

Anzit Guerrero, R. (2008). Los delitos de "cuello blanco" y los delitos de "cuello azul". *Dialnet.* Recuperado el 27/04/18 de https://es.scribd.com/document/368416560/Dialnet-LosDelitosDeCuelloBlancoYLosDelitosDeCuelloAzul-5259753

Arocena, G. A. (2012). La regulación de los delitos informáticos en el Código Penal argentino. Introducción a la Ley Nacional núm. 26.388. *Boletín Mexicano de Derecho Comparado*. (135) 945-988. Recuperado el 20/07/18 de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002&lng=en&tlng=en

Arregoitia López, S. L. (2014). Posibles sujetos de los delitos informáticos. *Informática Jurídica. Com*. Recuperado el 27/04/18 de http://www.informatica-juridica.com/trabajos/posibles-sujetos-de-los-delitos-informaticos/

Casanova, C. M. R. (s/f). La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de internet. *Facultad de Derecho. Universidad de Huelva. Derecho y conocimiento*. (2). 123-149

Castro Ospina, S. J. (2002). Delitos informáticos: La información como bien jurídico y los delitos informáticos en el nuevo código penal colombiano. *Delitosinformáticos.com*. Recuperado el 01/06/18 de https://www.delitosinformaticos.com/delitos/colombia1.shtml

Ciber derecho (2015). Ciberterrorismo en Argentina. Recuperado el 11/07/18 de http://www.ciberderecho.com/ciberterrorismo-en-argentina/

Cilleruel, A. R. (2006). La Ley Nº 11.723: algunas consideraciones desde la dogmática y la práctica jurídica. *Revista de la Asociación de Magistrados y Funcionarios de la Justicia de la Nación*. (41/42). IJ-LI-906. Recuperado el 20/17/18 de http://ijeditores.com/articulos.php?idarticulo=48906&print=1

Comisión de las Comunidades Europeas. (2001). Comunicación de la Comisión al Consejo, al Parlamento europeo, al Comité económico y social y al Comité de las regiones. Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos. Eeruope2002. Recuperado el 16/07/18 de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52000DC0890&from=ES

Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (n°12). (2010). Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético. Documento de trabajo preparado por la Secretaría. Recuperado el 01/05/18 de https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf

Cueto, M. (2015). ““Facebook” y el artículo 153 bis del Código Penal”. L.L. AR/DOC/780/2015

Definición ABC (s/f). Definición de Calumnia. Recuperado el 11/07/18 de https://www.definicionabc.com/derecho/calumnia.php

Derecho tecnológico.com. (s/f). Definición de Delito informático. Diccionario de informática y tecnología. Recuperado el 26/04/18 de http://www.derechotecnologico.com/delitos.html

Estrada Garavilla, M. (2008). Delitos Informáticos. *Universidad Abierta*. Recuperado el 25/05/18 de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

Estrada, P. R. (2001). Delito informático, virus y legislación.*Id SAIJ: DACF010038*. Recuperado el 14/04/18 de http://www.saij.gob.ar/doctrina/dacf010038-roca_de_estrada-delito_informatico_virus_legislacion.htm?bsrc=ci

Fernández, L. J. (2017). El espionaje informático: la poderosa estrategia del siglo XXI. *Techne*. Recuperado el 12/07/18 de https://www.technemexico.com/espionaje-informatico-la-poderosa-estrategia-del-siglo-xxi/

Figari, R. E. (2009). Reflexiones sobre la defraudación informática ley 26.388. *SAIJ*. *Id SAIJ: DACF10007*. Recuperado el 20/07/18 de http://www.saij.gob.ar/ruben-enrique-figari-reflexiones-sobre-defraudacion-informatica-ley-26388-dacf100073-2009-08-12/123456789-0abc-defg3700-01fcanirtcod

Gil, T. (2011). Ciberterrorismo. *Blogspot*. Recuperado el 10/07/18 de http://ciberterrorismoinfo.blogspot.com.ar/

González, J. (2008). Qué diferencias hay entre injurias y calumnias. *Seo Barcelona Jorge González*. Recuperado el 11/07/18 de http://www.xn--jorgegonzlez-kbb.com/que-diferencias-hay-entre-injurias-y-calumnias

Legal Information Institute (s/f). Fraude Cibernético e Informático. Recuperado el 10/07/2018 de https://www.law.cornell.edu/wex/es/fraude_cibern%C3%A9tico_e_inform%C3%A1tico

Legalium (2016). Injurias. Recuperado el 12/07/18 de http://www.legalium.com/derecho-penal/injurias/

Martínez Fazzalari, R. (2008). Sobre la reciente ley de delitos informáticos. *Educ.ar*. Recuperado el 01/06/18 de http://portal.educ.ar/debates/sociedad/documento-oficial-argentino/sobre-la-reciente-ley-de-delit.php

Massana, S. (2002) El ciberterrorismo: ¿una amenaza real para la paz mundial? Tesis de maestría FLACSO – *Facultad Latinoamericana de Ciencias Sociales*. Recuperado el 11/07/18 de http://www.argentina-rree.com/documentos/ciberterrorismo.pdf

Mayer Luxl, L. (2017). El bien jurídico protegido en los delitos Informáticos. *Revista Chilena de Derecho*, *44* (1), 235 – 260.

Maza Correa, J. P. (2018). El perfil de la víctima de delitos informáticos o cibercrimen. *Law and Trends. Com.* Recuperado el 27/14/18 de http://www.lawandtrends.com/noticias/tic/el-perfil-de-la-victima-de-delitos-informaticos-o-cibercrimen-1.html

Melo, F. (2009). El crimen de cuello blanco, según Sutherland. *Hoy Digital*. Recuperado el 24/04/18 de http://hoy.com.do/el-crimen-de-cuello-blanco-segun-sutherland/

Nava Garcés, A. E. (2017). Ciberterrorismo: La Nueva Cara de la Delincuencia en el Siglo XXI. *Foro Jurídico*. Recuperado el 11/07/18 de https://www.forojuridico.org.mx/ciberterrorismo/

Nelguard, M. (s/f) Clasificación de los delitos informáticos. *Scribd*. Recuperado el 12/07/18 de https://es.scribd.com/document/248913377/Clasificacion-de-Los-Delitos-Informaticos

Nic Argentina. (2017). ¿Qué es el Convenio de Budapest? Recuperado el 17/07/18 de https://nic.ar/es/enterate/novedades/que-es-convenio-budapest

Oficina de las Naciones Unidas contra la Droga y el Delito. (2010). Congresos de las Naciones Unidas sobre prevención del delito y justicia penal 1955–2010 55 años de logros. Recuperado el 17/07/18 de http://www.un.org/es/events/crimecongress2010/pdf/55years_ebook_es.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito. (2010). Comisión de Prevención del Delito y Justicia Penal de la ONU aborda nuevos desafíos. Recuperado el 16/07/18 de https://www.unodc.org/lpo-brazil/es/frontpage/2010/05/26-comissao-sobre-prevencao-do-crime-e-justica-penal-da-onu-encara-novos-desafios.html

Palazzi, P. A. (2016). *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388*. (3º Ed. actualizada y ampliada). [Versión electrónica]. Buenos Aires: AbeledoPerrot.

Pastorino, C. (2017). Convenio de Budapest: beneficios e implicaciones para la seguridad informática. *Welivesecurity.com.* Recuperado el 17/07/18 de https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/

Paterlini, N., Vega, C., Guerriero, G. y Velázquez, M. (s/f). Delitos informáticos. Antecedentes Internacionales para una Legislación Nacional. Proyectos Legislativos. *Asociación Argentina de Derecho de Alta Tecnología*. Recuperado el 18/07/18 de http://www.aadat.org/delitos_informaticos20.htm

PeritoIT.com (2017). Delito de estafa CON o POR medios informáticos. Recuperado el 01/06/18 de https://peritoit.com/2017/05/03/delito-de-estafa-con-o-por-medios-informaticos/

Piñeiro Bertot, M. I. (2007). Los delitos contra el medio ambiente como expresión de delitos de cuello blanco. *Pensamiento Penal*. Recuperado el 24/14/18 de http://www.pensamientopenal.com.ar/system/files/2007/06/doctrina33166.pdf

Pullido, C. (2012). Delitos informáticos. Sabotaje informático. *Blogspot*. Recuperado el 10/07/18 de http://puliido4e.blogspot.com.ar/p/sabotaje-informatico.html

Ramírez Bejerano, E.E. y Aguilera Rodríguez, A. R. (06/03/2016). Los delitos informáticos. Tratamiento internacional. *La Razón*. *La Gaceta jurídica*. Recuperado el 27/04/18 de http://www.la-razon.com/la_gaceta_juridica/delitos-informaticos-Tratamiento-internacional_0_2447755331.html

RecoveryLabs (s/f). Delitos informáticos. Glosario. Recuperado el 01/05/18 de http://www.delitosinformaticos.info/delitos_informaticos/glosario.html

RecoveryLabs. (s/f). Delitos informáticos. Legislación. Recuperado el 18/07/18 de http://www.delitosinformaticos.info/delitos_informaticos/legislacion.html

Rivolta, M. (2007). Medios de prueba electrónicos: estado de avance en la legislación argentina. *SAIJ*. *Id SAIJ: DACC070049*. Recuperado el 26/07/18 de http://www.saij.gob.ar/doctrina/dacc070049-rivolta-medios_prueba_electronicos_estado.htm

Rodríguez, P. (2013). Casos especiales de defraudación. Código Penal Comentado de acceso libre. *Asociación Pensamiento Penal*. Recuperado el 10/07/18 de http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37768.pdf

Sáez Capel, J. (2001). *Informática y delito* (2da Ed.) Buenos Aires: Proa XXI Editores

Sain G. y Azzolin H. (2017). *Delitos Informáticos* (1ª Ed.). Buenos Aires: B de F

Sain, G. (2018). Hacia una nueva ley de grooming. *Política Argentina*.http://www.politicargentina.com/notas/201803/25081-hacia-una-nueva-ley-de-grooming.html

Segu.Info. Seguridad de la Información(s/f). Legislación y Delitos Informáticos - El Delincuente y la Víctima. Recuperado el 27/14/18 de https://www.segu-info.com.ar/delitos/delincuenteyvictima.htm

Segu.Info. Seguridad de la Información. (s/f). Legislación y Delitos Informáticos - La Información y el Delito. Recuperado el 18/07/18 de https://www.segu-info.com.ar/delitos/delitos.htm

Seguridad informática. (2007) ¿Qué es Fraude y Estafa? Recuperado el 10/07/18 de https://seguinfo.wordpress.com/2007/07/24/%C2%BFque-es-fraude-y-estafa-2/

Seguridad Informática. Noticias de Seguridad Informática (2007). ¿Qué es fraude y estafa? Recuperado el 01/06/18 de https://seguinfo.wordpress.com/2007/07/24/%C2%BFque-es-fraude-y-estafa-2/

Tazza, A. (2014). El delito de grooming - Art. 131 Cod. Penal. *Cátedra de Derecho Penal II de la Facultad de Derecho de la Universidad Nacional de Mar del Plata*. Recuperado el 02/05/18 de http://penaldosmdq.blogspot.com.ar/2014/04/el-delito-de-grooming-art-131-cod-penal.html

Techlandia.com. (s/f). Diez delitos cometidos por medio de redes sociales. Recuperado el 02/05/18 de https://techlandia.com/10-delitos-cometidos-medio-redes-sociales-galeria_378067/

Telam. Agencia Nacional de Noticias (2018). El grooming entró a la cancha pero no para jugar. Recuperado el 26/07/18 de http://www.telam.com.ar/notas/201804/267786-el-grooming-entro-a-la-cancha-pero-no-para-jugar.html

Téllez Valdés, J. (2008) *Derecho informático* (4ta Ed.). México: Mc Grow Hill.

Tobares Catala, G. H. y Castro Arguello, M. J. (2010). *Delitos informáticos*. Córdoba: Advocatus.

Tognoli, M. E. (2016). Delitos Informáticos en el Derecho Argentino. Facultad de Ingeniería y Ciencias Hídricas. Universidad Nacional del Litoral. Recuperado el 18/04/18 de http://fich.unl.edu.ar/ciiddi2016/wp-content/uploads/2017/03/9Delitos-Inform%C3%A1ticos-en-el-Derecho-Argentino.pdf

Unesco. (2009). El observatorio mundial de lucha contra la piratería Argentina. *Unesco.org*. Recuperado el 20/17/18 de http://www.unesco.org/culture/pdf/argentina_cp_es

Van den EyndeAdroer, A. (2015). Análisis jurídico del sabotaje informático. *Abogacía española*. Recuperado el 11/07/18 de https://www.abogacia.es/2015/03/09/analisis-juridico-del-sabotaje-informatico/

Vaninetti, H. A. (2017). "Estafa en internet. Transferencia electrónica de fondos. Operatoria de home banking. La competencia en los delitos informáticos." L.L. Cita Online: AR/DOC/99/2017

Viega Rodríguez, M. J. (2011). "Un nuevo desafío jurídico: Los Delitos Informáticos". *MjvViegasociados*. Recuperado el 12/07/18 de http://mjv.viegasociados.com/wp-content/uploads/2011/05/DelitosInformaticos.pdf

Virus y delitos informáticos.blogspot. (2012). Virus y delitos informáticos. Recuperado el 01/15/18 de http://virusydelitosinformaticos.blogspot.com.ar/

Yuni J., Urbano. C. (2014) *Técnicas para investigar 2* (Vol. 2). [Versión electrónica]. Buenos Aires: Editorial Brujas.

2. Legislación

- Código Penal argentino originario
- Ley de Propiedad Intelectual (Ley 11.723)
- Ley de Protección de Datos Personales (Ley 25326)
- Ley 26.388 de modificación de Código Penal
- Ley sobre *grooming*(Ley 26.904)
- Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal
- Convenio Budapest

3. Jurisprudencia

- Cám. Fed. Casación. Sala III. (2015). "Castelo, Pablo Alejandro s/ recurso de casación" AR/JUR/24390/2015
- Cám. Nac. de Apel. En lo Crim. y Corr. Sala II. "C. A. Q". (2009). AR/JUR/43986/2009