UNIVERSIDAD NACIONAL DE LA PAMPA

FACULTAD DE CIENCIAS ECONOMICAS Y JURIDICAS

SEMINARIO SOBRE APORTACIONES TEORICAS Y TECNICAS RECIENTES

Título: "EL DERECHO Y LAS NUEVAS TECNOLOGIAS: NOCIONES DE DELITOS INFORMATICOS"

Alumnos:

- **Agustín Nicolás Bambini**
- **Constanza Noel Casal**
- **Rocío Belén Coronel**

Asignatura:

- **Derecho Penal II**

Profesor encargado de la Investigación:

- **Eduardo Aguirre**

Año de realización del trabajo : 2015

I. INTRODUCCION

En estos tiempos en los que vivimos actualmente, resulta innegable el impacto masivo que ha tenido el desarrollo tecnológico e informático tanto en el área de la ciencia y del conocimiento, como así también en la vida cotidiana de todas las personas, de las organizaciones, sociedades y empresas y por qué no, en las bases mismas sobre las que se erigen los países.

La masividad de Internet, la proliferación de las redes sociales, la velocidad en las comunicaciones, el desarrollo de computadoras, teléfonos celulares y artículos de esta misma especie, han sido herramientas determinantes que han llevado a que la sociedad moderna en forma vertiginosa y por qué no muchas veces descuidada, confíe sus datos personales, comerciales, bancarios, fotos, e información en general, vía web a gigantes servidores que se encargan de almacenar, procesar y transmitir estos datos alrededor del mundo, al alcance concreto de millones de interesados y de usuarios.

Éste enorme caudal de datos y de conocimiento puede obtenerse así en minutos (o en segundos inclusive), al alcance de un clic, lo que lleva a muchos a sostener que hoy por hoy las perspectivas del mundo virtual no tienen límites previsibles, y derivar así en la conclusión de que la informática es hoy una forma de poder social.

A su vez, también cabe advertir que la mayoría de los sistemas de seguridad y defensa de los países, los sistemas financieros y bancarios mundiales se han estructurado sobre estas bases tecnológicas informatizadas, lo que provoca que los mismos sean objetivos vulnerables de ataques de todo tipo para su desestabilización, lo que representa una amenaza para las bases mismas de la economía y gobierno de un país, como así también para la sociedad en su conjunto.

En este campo de la tecnología e informática, se observan cada vez con más frecuencia conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen medios y oportunidades nuevas, accesibles y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales, y acá lo que resulta dificultoso es como probar la comisión del delito, lo que conlleva también a la dificultad de encontrar al autor/es del mismo. Es en esta realidad planteada anteriormente, donde resulta necesario la intervención del Derecho como regulador de los múltiples efectos de la nueva

realidad global y de tantas potencialidades, tanto positivas como negativas, legales o ilegales.

Sin perjuicio de lo antes expuesto, aclaramos inicialmente que el presente trabajo no enuncia ni analiza los delitos de espionaje informático que suceden a nivel internacional. Por ejemplo, los episodios que involucran las revelaciones de Julian Assange (programador, ciberactivista, periodista y activista de internet australiano, conocido por ser el fundador, editor y portavoz del sitio web WikiLeaks), de Edward Snowden (consultor tecnológico estadounidense, informante, antiguo empleado de la CIA y de la NSA y conocido por ser el encargado de hacer públicos documentos secretos sobre programas de la NSA entre otros) y el rol de EEUU en materia de espionaje a escala internacional no son materia de análisis, por más que sean -nada más y nada menos- que una parte de las guerras de cuarta generación (la III Guerra Mundial, según el Papa y otros analistas). Tampoco reporta el poder de los servicios de inteligencia. Pero esto forma parte del acotamiento temático y la perspectiva metodológica elegida sobre un objeto de conocimiento específico sobre el que versa la presente tesis.

Para llevar a cabo dicha tarea, tenemos que empezar trazando una delimitación lo más precisa posible del objeto de estudio, en este caso los delitos informáticos, analizando así las conductas de los sujetos activos y pasivos; realizar las clasificaciones que pueden idearse dentro de este tipo de delitos, para su mejor análisis y comprensión; qué legislación actual, ya sea local o comparada, puede ser aplicada, en qué casos y sobre qué bases; y sobre todo la tarea más difícil a afrontar por la sociedad moderna, que es cómo deben ser las nuevas leyes que se dicten en los países a los fines de asegurar la mayor cantidad de derechos y brindar las garantías de protección de los ciudadanos/as frente al fenómeno de la llamada “era de la informática” tanto a nivel local como a nivel mundial.

II. DESARROLLO

1. DEFINICION DE DELITOS INFORMATICOS

En la actualidad las computadoras y artefactos tecnológicos (notebooks, tablets, celulares de alta gama, iphones, ipods, entre otros) se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener información, lo que las ubica también como un nuevo medio de comunicación fundado en la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos. La informática está hoy presente en casi todos los campos de la vida moderna.

Ha llegado a sostenerse que la informática es hoy una forma de poder social.

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica DELITOS INFORMATICOS.

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robo o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras y demás dispositivos lo que ha propiciado a su vez la necesidad de regulación por parte del derecho. A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales e internacionales concretas.

A modo de ejemplo, el autor mexicano Julio Téllez Valdés señala que : "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún."

Para Carlos Sarzana, en su obra “Criminalita e Tecnología”, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas". Y asi también dieron su definición Rafael Fernandez Calvo, Maria de la Luz Lima y otros tantos autores y expertos en el tema, planteando lo que es para cada uno de ellos un Delito Informatico.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la Organización de Cooperación y Desarrollo Económico (OCDE) a Paris, Francia, en mayo de 1983, el término delitos relacionados con las computadoras se define como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos".

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito".

No obstante cabe aclarar, que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora, delincuencia relacionada con el ordenador, todos usados como sinónimos del delito informatico.

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin", y por las segundas, "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Características de estos delitos según Tellez Valdés:

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.

2. CLASIFICACION DE DELITOS INFORMATICOS:

DELITOS INFORMATICOS RECONOCIDOS POR NACIONES UNIDAS:

1. Fraudes cometidos mediante manipulación de computadoras

- MANIPULACIÓN DE LOS DATOS DE ENTRADA
  Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.
  Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

- MANIPULACIÓN DE PROGRAMAS
  Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

- MANIPULACIÓN DE LOS DATOS DE SALIDA
  Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es 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. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas

de las tarjetas bancarias y de las tarjetas de crédito.

- MANIPULACIÓN INFORMÁTICA APROVECHANDO REPETICIONES AUTOMÁTICAS DE LOS PROCESOS DE CÓMPUTO
  Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2. Falsificaciones informáticas

- COMO OBJETO
  Cuando se alteran datos de los documentos almacenados en forma computarizada.
- COMO INSTRUMENTOS
  Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

3. Daños o modificaciones de programas o datos computarizados

- SABOTAJE INFORMÁTICO
  Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

- VIRUS
  Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

- 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.
  En términos médicos podría decirse que un gusano es un tumor benigno,

mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

- BOMBA LÓGICA O CRONOLÓGICA
  Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

4. Acceso no autorizado a servicios y sistemas informáticos

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

PIRATAS INFORMÁTICOS O HACKERS
El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL
Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna.

Al respecto, consideramos, 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.

CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS SEGÚN JULIO TELLEZ VALDES

Este autor clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio y como fin u objetivo.

Como instrumento o medio: en esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).

d) Lectura, sustracción o copiado de información confidencial.

e) Modificación de datos tanto en la entrada como en la salida.

f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

h) Uso no autorizado de programas de computo.

i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.

l) Acceso a áreas informatizadas en forma no autorizada.

m) Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo: en esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a los dispositivos de almacenamiento.

d) Atentado físico contra la máquina o sus accesorios.

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

CLASIFICACION SEGÚN MARIA DE LA LUZ LIMA

Esta presenta una clasificación, de lo que ella llama "delitos electrónicos", diciendo que existen tres categorías, a saber:

a) Los que utilizan la tecnología electrónica como método: conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

b) Los que utilizan la tecnología electrónica como medio: conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

c) Los que utilizan la tecnología electrónica como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

CLASIFICACION SEGÚN OLIVIER HANCE:

En lo que se refiere a delitos informáticos, Olivier Hance en su libro “Leyes y Negocios en Internet”, considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

a) Acceso no autorizado: es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.

b) Actos dañinos o circulación de material dañino: una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).

c) Interceptación no autorizada: en este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.

3. SUJETOS ACTIVO Y PASIVO EN LOS DELITOS INFORMATICOS

En el Derecho Penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo.

CARACTERÍSTICAS DEL SUJETO ACTIVO:

En la generalidad de los casos, se han identificado como sujeto activo de los delitos informáticos a individuos que poseen ciertas características peculiares que no presentan el denominador común de los delincuentes, esto es, tener habilidades para el manejo de los sistemas informáticos y que generalmente, producto de 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, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos, o ni siquiera cursen o hayan cursado estudios relacionados al área de las comunicaciones ni de la informática; con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos que son llevados a cabo: de esta forma, podemos distinguir a la persona que "entra" en un sistema informático sin intenciones delictivas, por el mero placer que le supone el desafío a su ego, distinta de aquella como la del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes a una cuenta personal, con el propósito de obtener un enriquecimiento

dinerario. Al respecto, según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada (Insiders). Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones informáticas cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa (Outsiders).

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de habilidades no es indicador de delincuencia informática, en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos, lo que supone a priori la delineación de un estereotipo o por lo menos la enumeración de rasgos que terminan componiendo un perfil criminalístico. Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como *"delitos de cuello blanco"*, término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943. Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como delitos de cuello blanco, aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros. Asimismo, este criminólogo estadounidense dice que tanto la definición de los delitos informáticos como la de los delitos de cuello blanco no se formula de acuerdo al interés protegido, como sucede en los delitos convencionales, sino justamente de acuerdo al sujeto activo que los comete.

Así, entre las características en común que poseen ambos delitos tenemos que el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional. Klaus Tiedemann, frente a esta caracterización nos dice "De manera creciente, en la nueva literatura angloamericana se emplea el término "hecho penal profesional" (Occupational Crime), con referencia al papel profesional y a la actividad económica desplegada; así la caracterización del delito económico se fundamenta ahora en la pertenencia del autor a las capas sociales más altas y más en la peculiaridad del acto (modus operandi) y en el objetivo del comportamiento.

Es difícil elaborar estadísticas sobre ambos tipos de delitos: la "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo en razón del poder económico de quienes los cometen, pero no obstante los daños económicos que suelen ocasionar son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad, la cual no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables", algo así como un "héroe" o mismo también un

“revolucionario”, un “libertario” que se atreve a vulnerar el sistema, y que sus logros no son otra cosa que una proclama social, o por lo menos de un cierto sector con el que se siente identificado.
Otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad: es excepcional que sobre el comitente del delito recaiga una condena de prisión o reclusión de algún tipo.
Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas y suelen estar previstos para casos bastante graves, lo que torna aun más dificultosa su operatividad.

CARACTERÍSTICAS DEL SUJETO PASIVO:

En primer término, tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser tanto individuos, instituciones crediticias, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados los unos a los otros a otros.
El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos con objeto de prever las acciones antes mencionadas, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos. Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables, y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos, las lagunas que se producen en los ordenamientos jurídicos que no se actualizan y corren varios años por detrás de las nuevas tecnologías, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantengan bajo la llamada "cifra oculta" o "cifra negra", provocando que no se pueda contar así con datos veraces y empíricos de la realidad, y en consecuencia desarrollar teorías y prácticas en pos de comprender acabadamente estos nuevos fenómenos, y así luchar y castigar este tipo de delitos.
Por lo anteriormente expuesto, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis

objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento. En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración e impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más, a la velocidad de los descubrimientos científicos en el área de las comunicaciones y de la electrónica. Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que, educando a la comunidad de víctimas y estimulando la denuncia de los delitos, se lograría echar luz sobre estos asuntos, instalándolos socialmente, e incluso promovería la confianza pública en la predisposición y la capacidad de los encargados tanto de dictar la ley, como de hacerla cumplir, y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos, o en su caso, castigarlos de la manera más adecuada posible para desalentar su comisión, que no se alimente la idea instalada en el imaginario colectivo de que los autores de estos delitos quedan impunes, y las víctimas desprotegidas y sin poder obtener un resarcimiento apropiado por el daño sufrido, sea cual sea su índole.

4. OBJETO JURIDICO DE LOS DELITOS INFORMATICOS

El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. El mismo no puede dejar de existir ya que constituye justamente la razón de ser del delito, es el fundamento y la vinculación lógica y necesaria que hace de nexo entre los sujetos activo y pasivo. No suele estar expresamente señalado en los tipos penales, sino que se los infiere, producto de los derechos y garantías inherentes a los individuos, derivados de la Constitución y de los tratados internacionales.
Circunscribiendo lo antes expuesto al campo de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente. De otro lado otra vertiente doctrinaria supone que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la INFORMACIÓN misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la

intangible. Esto por cuanto la información no puede, a criterio de Pablo Palazzi, ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que ella la información y otros intangibles son objetos de propiedad, la cual está constitucionalmente protegida. En fin la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de "dañosidad" o "lesividad". Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada. Así inspira tanto a la criminalización como a descriminalización de conductas. Su origen directo es la teoría del contrato social, y su máxima expresión se encuentra en la obra de BECCARIA "Los Delitos y las Penas" (1738-1794). En conclusión podemos decir que el bien jurídico protegido en general es la información, pero considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como: EL PATRIMONIO, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar; LA RESERVA, LA INTIMIDAD Y CONFIDENCIALIDAD DE LOS DATOS, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos; LA SEGURIDAD O FIABILIDAD DEL TRÁFICO JURÍDICO Y PROBATORIO, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos; EL DERECHO DE PROPIEDAD, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático. Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere. Para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo". En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos. Por tanto podemos decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos, en tal sentido de María Luz Gutiérrez Francés, respecto de la figura del fraude informático nos dice que: "las conductas de fraude informático presentan indudablemente un carácter pluriofensivo. En cada una de sus modalidades se produce una doble afección: la de un interés económico (ya sea micro o macrosocial), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macrosocial vinculado al funcionamiento de los sistemas informáticos". Por tanto diremos que el nacimiento de esta nueva tecnología, está proporcionando a nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, como sería la calidad,

pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa. En tal razón considero que este tipo de conductas criminales son de carácter netamente pluriofensivo.

III. LEGISLACION NACIONAL

Ley 26.388 (2008)

Denominada de “Delitos informáticos” ha incorporado las figuras típicas a diversos artículos del Código Penal de la Nación. Incorpora a las nuevas tecnologías como medios de comisión de distintos tipos previstos en el Código Penal. Los artículos incorporados sancionan: * Tenencia con fines de distribución por Internet; u otros medios electrónicos de pornografía infantil.- *la violación, apoderamiento y desvío de comunicación electrónica; *Intercepción o captación de comunicaciones electrónicas o telecomunicaciones; *interrupción de las comunicaciones electrónicas; *el acceso ilegítimo a sistemas informáticos; *Publicación de una comunicación electrónica.- *Acceso a un banco de datos personales; *revelación de información registrada en un banco de datos personales; *daño informático y distribución de virus; *Inserción de datos falsos en un archivo de datos personales; *Fraude informático ;*Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP). Las penas que establece son: a) prisión; b) inhabilitación (cuando el delito lo comete un funcionario público o el depositario de objetos destinados a servir de prueba); c) multa.-
La Ley 26.388 ha desembarcado en la República Argentina con el fin de cubrir un importante vacío legal hasta ese momento. Ello sin dejar de ser cierto que la ley con las penas actuales que establecen son artículos de muy poca utilidad.

Solamente al ver las penas establecidas en el artículo 128 (*prisión de seis meses a cuatro años el que produjere, financiare, etc. una representación de un menor de edad…)* se corrobora tal afirmación, que la Ley fue elaborada y posteriormente promulgada sin dudas para llenar ese vacío legal sin tener presente o por desidia o por inoperancia que el daño que ocasiona la producción y/o financiación de la pedofilia es muchísimo mayor que la pena que por cierto, es de un delito excarcelable. Este delito va en crecimiento y más allá de aplicar un riguroso control a nivel mundial de pedófilos, no deja de ser cierto que las penas deberían ser mayores, las multas aplicables incalculables y debería establecerse un sistema de exposición pública para estos individuos.

Interpretación de la Ley 26.388
Art. 1°.- *Incorporase como últimos párrafos del artículo 77 del Código Penal, los siguientes: El término "documento" comprende toda representación de actos o*

hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.-

El artículo 6 de la ley 25.506 de firma digital el cual define al documento digital como la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.- Documento es todo soporte material de naturaleza mueble, que incorpora una información de manera estable, lo cual le confiere cierto valor probatorio. Giannantonio entiende por documento electrónico aquel documento proveniente de un sistema de elaboración electrónica. La tecnología de la informática permite garantizar la autenticidad y la inalterabilidad de los documentos contenidos en soportes informáticos. Tanto la Ley 25.506 de firma digital como este primer artículo de la Ley 26.388 le da valor jurídico probatorio al documento electrónico y como tal es protegido por la normativa.-
El artículo se refiere, del mismo modo a "firma digital", "suscripción", "instrumento privado y certificado". La misma ley 25.506 establece en sus artículos primero y segundo el valor jurídico probatorio y las definiciones de firma electrónica y firma digital. Reconociendo el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la Ley. Del mismo modo define a la Firma Digital como "al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.-…".-
Se diferencia la firma digital a la firma electrónica en que ésta última es un conjunto de "datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital."
Desde la incorporación al Código Penal de la Ley de delitos informáticos, como la Ley de firma digital, la firma manuscrita, electrónica como la digital pasan a tener la misma validez legal.-
El artículo XIII del segundo capítulo de la Ley 25506 define al "Certificado digital, entendiendo por tal al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular."
En síntesis, tanto la firma como el certificado le dan autenticidad a la identidad del que envía un mensaje a través de la web, asegurando que su contenido original no ha sido alterado.-

Delitos contra la integridad sexual

Art. 2°.-*Sustitúyase el artículo 128 del Código Penal, por el siguiente:*
Artículo 128.- *Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho*

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 meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años."
El artículo 2 de la Ley 26.388, que reemplaza al artículo 128 del Código Penal reprime a quien intervenga en la producción, financiación, ofrecimiento, comercialización, publicación, facilitación, divulgación, distribución y la organización de eventos o espectáculos de representaciones sexuales explícitas de menores.- Condena la participación en todas sus formas no dejando lugar a dudas de las responsabilidades que a cada uno de los actores le corresponde.- Reprime, asimismo no solamente a quien tuviere en su poder, con fines de comercialización los elementos o representaciones sino también a quien permita el ingreso o suministre material a menores de 14 años.- Serán pasibles de sanción penal quienes hubieren actuado con dolo. Este delito no admite tentativa.-
Este artículo sanciona a quienes intervengan en la etapa de preparación, a quienes suministren dinero para la creación o desarrollo, a quien ponga a disposición del público, quien muestre y/o presente, a quien compre, venda y/o permute con fines lucrativos; a quien difunda el material, quien haga fácil y/o posible la propagación, quien la publique y quien reparta o haga lo posible para que llegue a los consumidores y a quien prepare la realización de actos, espectáculos con menores de edad en representaciones sexuales explícitas.-
El legislador se orientó a sancionar a todas aquellas acciones típicas que en su conjunto o separadas lleven a la explotación de menores de edad.-
Relacionado a este tema tan delicado y preocupante a nivel mundial, el Convenio sobre cibercriminalidad de Budapest del 23 de Noviembre del año 2001, en su Artículo noveno estableció que son infracciones relativas a la pornografía infantil tanto el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático, como la difusión, transmisión o la procuración para sí como para otros de pornografía infantil o la simple posesión en cualquier sistema informático y amplía diciendo que pornografía infantil comprende cualquier material pornográfico representado en forma visual de " un menor adoptando un comportamiento sexualmente explícito; una persona que aparece como un menor adoptando un comportamiento sexualmente explícito y unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito".-

"Violación de Secretos y de la Privacidad."

Art. 3°.- *Sustituyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente.-*
Es importante la modificación ya que incorpora e incluye a la privacidad como bien jurídico protegido.
Art. 4°.-Sustitúyase el artículo 153 del Código Penal, por el siguiente: "**Artículo 153**.- *Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté*

dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena."

Previo a la sanción de la ley de delitos informáticos, el correo electrónico no se encontraba equiparado al correo postal por lo que todas las acciones que se planteaban judicialmente eran rechazadas por inexistencia de delitos, lo cual hasta ese momento era así.-

El artículo 153 reprime a quien por cualquier medio ingresa a un correo electrónico que no le esté dirigido y sobre el efectúe cualquier tipo de acción de distribución y/o modificación y por ello podrá ser condenado a una pena entre 15 días y 6 meses y se incrementará de un mes a un año en el caso que el autor publicare o comunicare el contenido.-

Art. 5°.- *Incorporase como artículo 153 bis del Código Penal, el siguiente*:

"**Artículo 153 bis**.- *Será reprimido con prisión de quince días a seis 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 mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."*

El artículo 153 bis reprime a quien accediere por cualquier medio a un sistema informático, a sabiendas, es decir, conociendo la situación en carácter previo a realizar la acción. El término "a sabiendas" nos indica claramente que estamos bajo una figura que únicamente acepta el dolo, desestimando la negligencia.- Del mismo modo, al referirse a "acceso restringido", se refiere a sistemas en los cuales el ingreso no sea libre, de acceso gratuito a través de Internet. Citando al Dr. Pablo Palazzi dice "El texto legal hace referencia a un "sistema o dato informático de acceso restringido" puesto que no se prohíbe acceder a sistemas o redes abiertas, o al contenido publicado en un sitio de Internet público (como son la gran mayoría).-

El término "a sabiendas" no deja lugar a dudas que quien ingresa en ese archivo o dato lo está haciendo en clara situación que quien ingresa lo hace con intención de hacerlo y que el sitio no requiere de contraseñas o de nombres de usuarios previamente otorgados al individuo. Las empresas proveedoras de servicios de Internet han mostrado su inquietud, comentarios y preocupación al respecto. Los proveedores de Internet brindan servicios de navegación, correo electrónico, alojamiento de web, entre otros que lógicamente permite la navegación por la red. Esa navegación se realiza en las denominadas redes abiertas o libres, en las cuales no existe restricción alguna para poder "navegar" por los contenidos. Muy

diferente son las redes "cerradas" en las cuales no se puede ingresar sin contar con una autorización expresa o nombre de usuario o contraseña. Entonces, el término "a sabiendas" se refiere a este punto en particular; es decir separa la navegación libre que no requiere autorización alguna de cualquier acceso limitado a un sistema o dato informático que requiere de autorización para ingresar. Hay que tener presente que quien ingresa en un lugar cerrado "franqueando la entrada", es decir, "hacheando una clave" será considerada actividad ilegal por parte de quien lo realice. Esos usuarios para cometer el delito requieren de un servicio de Internet y es por ello la preocupación de los proveedores, ya que indirectamente podrían ser partícipes necesarios. "La conducta típica se basa en el acceso ilegítimo a un sistema informático, cuyo acceso es restringido."

Art. 6°.- *Sustitúyase el artículo 155 del Código Penal, por el siguiente*:

Artículo 155.- *Será reprimido con multa de pesos un mil quinientos ($1.500) a pesos cien mil ($100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público."*

El nuevo artículo 155 aplica una multa a quien encontrándose en posesión de una comunicación electrónica, un e-mail o similar lo hiciere publicar indebidamente, no siendo esta comunicación destinada a publicidad y supedita la multa si la publicación ocasione o pudiere ocasionar un daño.- Exime de responsabilidad a quien lo hace en virtud de la protección de un bien público.- Estamos en presencia de una acción dolosa. No admite culpa. Ello queda ratificado con la incorporación de la palabra "indebido" con la cual el legislador contempla únicamente la acción dolosa descartando la culpa.-

Nos encontramos en presencia de una nueva forma de forma de una comunicación; la comunicación electrónica, la cual, mediante esta ley, ya hemos dicho, es equiparable a la correspondencia postal, el correo electrónico.-

Ha de preguntarnos si las comunicaciones por chat, messenger, Black Berry Messenger, por WhatsUp, entre otros son también comunicaciones electrónicas.-

Si partimos del principio que las comunicaciones entre individuos son privadas, salvo que permitan su difusión, nos encontramos con que tanto el correo electrónico como cualquier otra comunicación electrónica o mediante medios electrónicos, la publicación sin la debida autorización violaría el presente artículo, lo cual incorpora toda nueva forma recomunicación mediante medios electrónicos, ya sea actuales como nuevos que en el futuro puedan crearse.-

El delito se configura al dar a publicidad el contenido de una comunicación no destinada a ello y sin autorización expresa del remitente o emisor y que tal comunicación ocasione o pueda ocasionar daños a terceros. Con relación a ello y de acuerdo con Lucero y Kohen "1..el tipo penal exige que se pudiera ocasionar perjuicios a terceros, alcanzando con que éste pueda ser al menos potencial; es decir que no se requiere un perjuicio efectivamente causado, sino que es suficiente la posibilidad cierta de causarlo…"

La doctrina colabora con la cuestión y dice que la "correspondencia debe proceder de un remitente determinado para que exista delito por ausencia del bien jurídico

protegido", el cual en este caso es la protección de la privacidad de la correspondencia.-

Art. 7°.- *Sustituyese el artículo 157 del Código Penal, por el siguiente:*

"**Artículo 157.-** *Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos*."

El Legislador, siguiendo el criterio de incorporación de las figuras tecnológicas en la ley que estamos analizando, ha incorporado los "datos", con el fin de proteger aquella información almacenada en sistema digital y que los datos tengan el carácter de secretos.-

Se denomina datos a "Cualquier medio de información ya sea electrónica, en soporte papel y/o cualquier otro soporte idóneo. El llamado dato electrónico abarca a bases, archivos, documentos de texto, imágenes, voz y video codificados en forma digital". Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Con el mismo criterio este artículo protege como bien jurídico, también a la privacidad de los datos.- El sujeto activo de la acción, tal lo establecido en el texto de la norma es un funcionario público y que se encuentre en la obligación de guardar un secreto. Por ello el agravante en la pena si lo comparamos con el artículo anterior y el pasivo aquel al cual se le deben proteger esos datos.-

Nos encontramos en una figura que requiere de conocimiento de que el dato es secreto y que su divulgación se encuentra prohibida, por lo cual no puede tratarse de otra que una figura dolosa, por lo cual acepta también la tentativa.-

La tentativa en este delito, al igual que en todos los delitos en los cuales el bien jurídico es la privacidad, la prueba en el grado de tentativa es sumamente difícil comprobarlo. El porqué de tal afirmación se debe a que la tentativa se produce al momento en que un tercero toma conocimiento del secreto aunque no se produzca el daño, porque si se produce el daño salimos de la figura de la tentativa. Desde este punto de vista, si el secreto "continua guardado" en el tercero que no debe conocerlo y de ninguna manera se puede probar que ese secreto fue suministrado por el funcionario público, entonces es imposible probar el delito.-

Art. 8°.- *Sustitúyase el artículo 157 bis del Código Penal, por el siguiente*:

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

El presente artículo tal su redacción, reprime a quien ingrese a un banco de datos personales sin autorización ni permiso alguno; a quien revelare secretos o archivos registrada en ese banco de datos y a quien las modifique por cualquier medio. Se agrava la pena si el sujeto activo es un funcionario público.-

Esta figura está íntimamente relacionada con la protección de datos personales establecidos en la ley 25326 que incorporó las figuras del acceso ilegítimo a un banco de datos y revelación ilegítima de información.-
El bien jurídico protegido, al igual que en los artículos anteriores es la privacidad, se trata de una conducta dolosa y acepta la tentativa, al igual que el artículo anterior.-
Lógicamente quien ingresa a sistemas seguros a los cuales no tiene autorización, o violando los ingresos o franqueando las contraseñas, realiza su conducta a sabiendas que lo está realizando y sin duda alguna ese ingreso será ilegítimo. El criterio es similar a la violación del correo electrónico pero hace referencia a los datos personales, protege la intimidad o el secreto no ya del email sino de una base de datos privada y cerrada y cualquier violación a ella es considerada delito.-
Del mismo modo, reprime no solamente a quien ingresa ilegalmente sino a quien participa de la información allí registrada a terceros, pero en este caso se detiene la norma en que la prohibición de esa revelación se encuentre establecida por ley: *"…cuyo secreto estuviere obligado a preservar por disposición de la ley…"* .-
Entonces la pregunta a formularse es: ¿si no está establecida por ley, la revelación de la información guardada en una base de datos no será considerada delito?. Desde el punto de vista y de acuerdo la redacción del artículo presente, la respuesta es negativa. Si no está prohibida por ley no será delito.-
La lógica del artículo, además de reprimir a quien ingresa in debidamente, a quien revela la información allí almacenada, reprime a quien modifica el contenido de dicha base de datos., agregando, cambiando, modificando, suprimiendo el contenido de la información.-
El sujeto activo será cualquier persona que ingrese indebidamente a una base de datos sin autorización, y el sujeto pasivo no será simplemente el dueño o titular de esa base de datos sino también quien tenga la responsabilidad de proteger y resguardar la base de datos.-
Se trata de una figura que requiere dolo, tal lo que he manifestado anteriormente en los tres incisos que componen este artículo, por lo cual acepta también la tentativa y agrava la pena si el sujeto es un funcionario público.-

Estafa Informática. Fraude informático

Art. 9°.- *Incorporase como inciso 16 del artículo 173 del Código Penal, el siguiente:*

"Inciso 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."*

Nos encontramos con una nueva figura del delito de estafa establecido en el Código penal Argentino. Previamente el 21 de setiembre de 2004 la ley 25930 incorporó la defraudación mediante el uso de tarjetas de créditos o débitos.-
La incorporación del delito de defraudación informática en el Código Penal, llevó a los legisladores a grandes debates. Las discusiones parlamentarias se dividían en dos grandes sectores, aquellos que consideraban que se debía encuadrar a la apropiación de bienes informáticos en la figura de defraudación mediante la utilización de medios informáticos y aquellos que consideraban que tal apropiación debería ser hurto mediante medios informáticos.- Finalmente se ha incorporado la figura de fraude informático dentro del artículo 173 del Código Penal, tal lo

realizado por diferentes países europeos –Inglaterra, España, Italia, Alemania, entre otros y los Estados Unidos de Norte América.-
Al definir a la defraudación informática nos referimos a un nuevo sistema de estafa la cual se lleva a cabo mediante la manipulación de cualquier sistema informático que afecte al patrimonio y/o a la propiedad.-
Generalmente es muy difícil que este tipo de delitos los cometan sujetos no familiarizados con los sistemas. No es común ver que una estafa informática haya sido cometida por personas sin conocimiento en informática justamente porque se requiere de conocimientos específicos para poder manipular los sistemas o una transmisión de datos utilizando cualquier tipo de ardid que lleve a la víctima a cometer un error y que ese error lo lleve a un perjuicio económico que a su vez beneficie económicamente al autor del delito.-
Este delito está creciendo exponencialmente donde gran cantidad de personas han sido estafadas producto del robo o sustracción de su identidad, mediante el cual sus datos personales son utilizados ilegalmente. Los datos generalmente son facilitados por los propios damnificados mediante encuestas, llamados telefónicos que simulan ser del banco para verificar datos, mismo sistema por correo electrónico, mediante sorteos simulados en supermercados o en la vía pública o bien a partir del hurto o robo de documentos y tarjetas de crédito, cupones de sorteos, y cualquier credencial que contenga datos propios. Generalmente el damnificado se entera del robo de su identidad una vez que recibe intimaciones a cancelar deudas o juicios ejecutivos y hasta pedidos de detención, los cuales se llevan a cabo generalmente cuando la víctima desea salir del país por algún motivo.-
Cualquier persona puede generar el denominado perfil y allí compartir con quien desee información propia y ajena. Pero está la situación en que un sujeto haciéndose pasar por otro, genera un perfil haciéndose pasar por éste. ¿Podría llamarse robo de identidad?. Sin duda será un tema para un futuro trabajo.-
Se trata de un delito doloso de acción pública que admite la tentativa.

Daño informático. Daño informático agravado.-

Art. 10.- *Incorporase como segundo párrafo del artículo 183 del Código Penal, el siguiente: "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños."*

El artículo 183 del Código Penal, el cual reprime con quince días a un año, al 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, e incorpora como segundo párrafo el definido en el párrafo anterior.-
Se incorpora al Código Penal el daño informático mediante esta figura. Con el primer párrafo quedaba un vacío legal en cuanto a la informática y los daños que su uso podía ocasionar incluso la distribución de virus a través de la red. Los verbos típicos son alterare, destruyere, inutilizare, vendiere, distribuyere. No merecen demasiado análisis pero sí es importante destacar que tanto el alterar, destruir como inutilizar serán acciones definitivas que no puedan ser reparadas de

ningún modo, es decir que no pueda regresarse al estado anterior a la acción típica, de lo contrario estaríamos en el grado de tentativa.
El problema inicial consistió en que no se consideraba como cosa a los documentos o programas o datos informáticos, entonces mal podría recaer sobre estos daño alguno por tratarse de bienes intangibles.
Los verbos típicos "vendiere" y "distribuyere" se refieren específicamente a la facilitación mediante diferentes medios de virus o programas destinados a causar daños informáticos.- La ley sanciona a quien los venda o distribuya por cualquier medio, no a quien los tiene en su poder.
El bien jurídico protegido, indudablemente es la propiedad, requiere de dolo directo de querer dañar los programas o documentos o sistemas informáticos.
Art. 11.- *Sustitúyase el artículo 184 del Código Penal, por el siguiente:*
"Art. 184.- *La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes: 1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones; 2. Producir infección o contagio en aves u otros animales domésticos; 3. Emplear substancias venenosas o corrosivas; 4. Cometer el delito en despoblado y en banda*; 5. Ejecutarlo en archivos, registros*, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público."*
Con la incorporación a la última parte del inciso 5 e inciso 6 del artículo 184 del Código Penal de la figura de daño a los sistemas informáticos se han solucionado un grave vacío legal, al cual ya me he referido anteriormente.-
El inciso sexto y el quinto última parte establecen que quien ejecuta un daño en sistemas informáticos destinados a servicios públicos y en los sistemas destinados a la prestación de servicios de salud o comunicaciones, energía, transporte u otro servicio público será pasible de una sanción.-
De ello se desprende que el bien jurídico tutelado es la propiedad de los datos, sistemas informáticos, documentos informáticos destinados a prestar servicios públicos, siendo el sujeto activo cualquier sujeto que altere, destruya, inutilice los datos o sistemas y el sujeto pasivo en principio es el titular del dato, pero siguiendo el criterio de artículos anteriores es no solamente éste sino también aquel responsable de esos documentos.-
Con la figura incorporada, en el presente artículo se agrava la pena a quien daña los sistemas informáticos públicos, sabiendo que lo son, considerando que el daño a un sistema informático de salud, comunicaciones, transporte, energía, etc. es un daño grave que perjudica no solo al titular del documento sino potencialmente a la sociedad toda.- "Sabiendo que lo son", significa que quien comete el daño a los sistemas debe conocer que esos datos corresponden a los servicios públicos, de lo contrario nos encontraríamos en la figura del artículo anterior.- Atento ello nos encontramos en la figura del dolo directo.-
Más allá del agravante de la pena, el cual es a todas luces necesario, la pena que establece este artículo no tiene razón de ser ni remotamente equivalente al daño

que un nuevo virus puede ocasionar. Al respecto Lucero y Kohen dicen que "… el Legislador, al entender que existe un mayor grado de culpabilidad, optó por agravar el daño informático, cuando éste se ejecuta en sistemas informáticos destinados a la prestación de servicios de salud, comunicaciones, provisión o transporte de energía, de medios de transporte u otro servicio público..". y agrega Palazzi, "el agravante se refiere a sistemas informáticos, pero no de datos o programas de ordenador contenidos en ellos. Entendemos que la redacción los incluye ya que es muy difícil afectar directamente el hardware de un equipo mediante ataques externos, más bien lo que se estropeará será el software, los datos o los medios de comunicación…"

Delitos contra la seguridad del tránsito y de los medios de transporte y de comunicación.-

Art. 12.- *Sustitúyase el artículo 197 del Código Penal, por el siguiente:*
***"Art. 197**.- Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida."*

El capítulo segundo del Código Penal, debería agregar a continuación de comunicación, el término comunicación electrónica. Más allá de ello, los Legisladores al redactar la modificación del 197 incorporaron la frase "o de otra naturaleza" en lugar de comunicación electrónica o a través de medios electrónicos abarcando de este modo cualquier tipo de comunicación mediante los sistemas y equipos actuales como los que se creen en el futuro.-

El artículo reprime a quien entorpeciere o interrumpiere la comunicación…o resistiere el restablecimiento y de este modo mantiene la línea con lo establecido en el artículo analizado anteriormente pero ampliando la protección a todas las comunicaciones que se cursen tanto públicas como privadas y sanciona no sólo el entorpecimiento o la interrupción sino también la resistencia del autor al restablecimiento de la comunicación interrumpida.-

Con relación a este último punto es importante destacar que tal conducta –el resistir violentamente el restablecimiento- debería ser un agravante a la figura principal de interrumpir o entorpecer. El fundamento se basa en que el delito se comete con los dos primeros verbos típicos, pero el hecho de "resistir que la comunicación se restablezca" quiere decir que quien cometió el delito se encuentra "trabajando" para que quien o quienes intentan restablecerlo se encuentren con más impedimentos sucesivos. Esa conducta de mantener la interrupción debería ser agravada cuanto menos en las interrupciones de comunicaciones públicas y siguiendo la lógica del artículo anterior, este delito sería más cercano a los estragos que a la propia interrupción de las comunicaciones

Si tenemos en cuenta que en el delito de robo, si el mismo se produce mediante el uso de armas o violencia, el mismo es agravado, entonces siguiendo el mismo criterio, si el artículo establece la violencia en el modo utilizado para que se proceda a la restitución del servicio, ninguna duda cabe que la última parte debería ser la figura agravada y por consiguiente un aumento en la pena a aplicarse.-

El bien jurídico protegido son las comunicaciones en general pudiendo ser el sujeto activo cualquier persona que interrumpa o interfiera las comunicaciones y el sujeto pasivo el titular de dichas comunicaciones, se trata de un delito doloso y lógicamente no admite el grado de tentativa toda vez que el delito se consuma una vez interrumpida la comunicación.-

Alteración de medios probatorios

Art. 13.- *Sustitúyase el artículo 255 del Código Penal, por el siguiente*: "Art. 255*.- Será reprimido con prisión de un mes a cuatro años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de setecientos cincuenta a doce mil quinientos pesos.."*

De la redacción del presente, el cual protege a los medios de prueba no ha sufrido demasiadas modificaciones con la ley 26388 a excepción de la incorporación del verbo *alterar, en todo o en parte y público (al funcionario)* y a la palabra *culpable* la modificó por *autor.* El verbo *alterar* fue incorporado con el fin de proteger a los sistemas informáticos de cualquier tipo de modificación tal lo manifestado en este mismo trabajo anteriormente. Al tratarse de prueba digitales, por ejemplo, la misma con el sólo hecho de alterarlo o modificarlo mediante cualquier técnica de manipulación informática estaría variando el elemento probatorio.- El término *"en todo o en parte",* tal lo visto, un sistema o prueba informática puede ser modificado o alterada en todo el contenido del archivo o parte de éste teniendo presente que cualquier modificación debe ser definitiva. El término *"culpable"* ha sido reemplazado por *autor*, siendo ello lógico toda vez que muy distinto es ser autor de un hecho que culpable del mismo. Desde el punto de vista de la informática quien modifica un archivo o una base de datos o sistemas puede ser autor material del hecho sin ser el culpable. Hemos dicho que quien comete un delito informático, dependiendo el delito de que se trate, debe ser una persona idónea en sistemas. No cualquier sujeto puede ingresar a una base de datos y alterar su contenido, violando contraseñas o permisos de ingreso sin contar con una experiencia importante en la materia.-

Es un delito doloso, ya que quien altera, sustrae, daña lo hace conociendo el carácter de medios probatorios de los elementos en custodia; admite la tentativa ya que si la alteración permite su recuperación la prueba seguiría intacta.- El sujeto pasivo es aquel que tiene la custodia de los elementos de prueba, sujeto activo es cualquier sujeto que altere, dañe, sustraiga la cosa y continua el articulado agravando la pena al depositario de la cosa si por su negligencia se comete el hecho.-

Art. 14.- *Derogase el artículo 78 bis y el inciso 1° del artículo 117 bis del Código Penal.-*

El presente artículo deroga el artículo 178 bis del Código Penal el cual antes de la Ley 26388 definía los términos firma y suscripción, comprenden la firma digital, la creación de una forma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado

digitalmente.- El inciso 1 del art. 117 bis decía antes de la reforma: "será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales…"
En los últimos párrafos del artículo 77 del Código Penal en el cual se definen los conceptos empleados en el propio código, nos encontramos con la definición de documento, firma, suscripción, instrumento privado y certificado. El común denominador es la referencia al término digital ya sea expresa como tácitamente. De no haberse derogado los artículos mencionados el código hubiese sido redundante definiendo los mismos términos en artículos diferentes.

Ley 26.904 (2013)

Incorpora el delito de "Grooming" o Ciberacoso, estableciendo en el 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".
La captación o el acoso de menores por internet con fines sexuales (conocido en inglés como grooming) consiste en la creación de perfiles falsos en las redes sociales y en otros servicios de comunicación digital, donde el acosador busca crear lazos de confianza o una supuesta amistad que a lo largo del tiempo comienza a tornarse extorsiva y abusiva. En el peor de los casos, aunque no siempre llega a suceder, se intenta concretar un encuentro físico para abusar sexualmente de los menores.

IV. SITUACION MUNDIAL

En los inicios de Internet no se buscaba su regulación legal ya que al tratarse de una red mundial de consultas y comunicación su esencia era la libertad de acción, lo cierto que con el paso del tiempo y con los ataques terroristas los cuales utilizaban la red justamente para esa comunicación, esa primera idea quedó sin efecto y los estados tuvieron que poner manos a la obra con el fin de controlar todo aquello que circula por la red.-
Es así que a raíz del aumento de los delitos cometidos por medios electrónicos y la falta de legislación a los países a elaborar un convenio internacional con el fin de regularlo. Es así que en la Ciudad de Budapest en el mes de Noviembre de 2001, se firmó un Convenio sobre cibercriminalidad en el cual varios países entre ellos Albania, Croacia, Estonia, Hungría, Lituania, Rumania, Eslovenia y Macedonia se comprometieron a contar con un mayor control en la utilización y seguridad en Internet.- Argentina adhirió al convenio en el año 2010, aún no es miembro firmante.-

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

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

Los principales objetivos de este tratado son los siguientes:

- La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.
- La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.
- Establecimiento de un régimen rápido y eficaz de la cooperación internacional.7

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

Asimismo, se exponen cuestiones de derecho procesal como la preservación expeditiva de los datos almacenados, la preservación expeditiva y divulgación parcial de los datos de tráfico, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido. Además, el Convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua (con consentimiento o disponibles al público) y prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las Partes Colaboradoras.

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

V. CONCLUSION

Para concluir con este trabajo, que abarca un tema de gran interés y preocupación en estos tiempos ya sea a nivel nacional como internacional, y debido a que en sí, no hay un concepto universal y genérico de lo que es un DELITO INFORMATICO, tomando como punta los diversos conceptos de varios autores anteriormente mencionados, podemos decir que un delito informático es una conducta o actividad no ética, ilícita, inadecuada o no autorizada en la cual la computadora y demás artículos tecnológicos han estado involucrados como material, objeto o como medio de la acción contraproducente. O sea, que lo importante es que la acción se dé por vías informáticas o que tenga como objetivo destruir y dañar artículos tecnológicos, medios electrónicos y redes de Internet: eso lo convierte en delito informático, más allá del tipo de crimen del que hablemos, ya sea hackeo, sabotaje, piratería, modificación de datos, entre otros.

Por otro lado, la falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, ya que cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

En cuanto al problema de este tipo de delitos, si bien son muchos los casos que se presentan, pocas son las denuncias, o mejor dicho las soluciones encontradas a este tipo de inconvenientes, y esto es debido a la gran dificultad de comprobación del delito y también a la falta de regulación por parte del Derecho, porque la tecnología se mueve más rápido que la legislación y existen conductas criminales por vías informáticas que no pueden considerarse como delito, ya sea por no cumplir con las etapas de la "Teoría del delito" como por no estar tipificadas en un texto legal. En Argentina se sancionó en el año 2008 la Ley 26.388 que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones. Pero si bien, ésta se sancionó para llenar un vacío legal que había hasta ese momento, también es verdad que esta ley es, digamos, de escasa utilidad por ejemplo, por las penas que se establecen en caso de que se cometa el quebrantamiento, como bien se ve en el art. 128 de la ley, ya que las penas y las multas deberían ser mayores y/o equivalentes a la gravedad y perjuicios que ocasionen los delitos, y que haya un grado de exposición para los culpables.

Por último, la ocurrencia de los delitos informáticos, no debe impedir los beneficios que proveen las tecnologías, sino por el contrario, esta situación debe servir como un desafío a los especialistas de informática y tecnología, como así también al Estado, para realizar esfuerzos encaminados a fortalecer y consolidar los aspectos de regulación, controles, límites al uso, seguridad, e integridad de la información.

VI. BIBLIOGRAFIA

- GIANNANTONIO, Ettore; "El valor jurídico del documento electrónico"; en Informática y derecho"; Ed. Depalma, 1987

- LUCERO Y KOHEN. “Delitos informáticos”

- PABLO PALAZZI . Análisis de la ley Argentina 26.388/2008

- Video de Marcos Salt: TEDxBuenosAires : https://www.youtube.com/watch?v=7xzbi9DHT9M

- Pagina de Asociación Argentina de Derecho de Alta Tecnología: http://www.aadat.org/delitos_informaticos20.htm

- Foro de Profesionales Latinoamericanos de Seguridad: http://www.segu-info.com.ar/delitos/tiposdelito.htm

INTEGRANTES:

- Agustín Nicolás Bambini
- Constanza Noel Casal
- Rocío Belén Coronel