UNIVERSIDAD EMPRESARIAL SIGLO 21

LA EVOLUCIÓN TECNOLÓGICA UTILIZADA COMO MEDIO DELICTIVO Y SU LEGISLACIÓN VIGENTE

Tesis para obtener el título de grado de la carrera Abogacía.

Elaborado por: Nicolás Francisco Bruno

LA PLATA, BUENOS AIRES 2016.

DEDICATORIA

Nicolás F. Bruno

A mi papa Rubén y mi mama Olga, en reconocimiento por todo su esfuerzo que en la vida han logrado con el fin de que sus hijos puedan progresar, por aquella educación que me han transmitido, los valores del esfuerzo, la honestidad, la humildad y perseverancia de que tarde o temprano se logran los objetivos.

A mi querido abuelo Miguel, quien me indicaba que nunca deje de estudiar, citando sus palabras como "hijo… nunca dejes de estudiar".

Y a mi amigo Don Carlos, siendo una gran persona que guiaba mi entusiasmo a estudiar, para que yo progrese tanto en lo personal, como también en lo profesional, aportando siempre su apoyo y aliento de nunca bajar los brazos.

A estas pocas personas que menciono… hoy les digo que soy Abogado y que sin la presencia de alguno de ellos, seria imposible obtener esta meta…

GRACIAS…

Introducción

Abstrac

En la presente investigación se tendrá en cuenta el estudio y el análisis de como la evolución de la tecnología, ha sido un elemento de gran utilidad para los delincuentes informáticos. Aprovechando que hoy en día la tecnología se encuentra al alcance de cualquier persona y que con una simple conexión a internet se puede mantener el tráfico de datos de cualquier tipo, los usuarios desconocen su vulnerabilidad frente a la peligrosidad que dicho tráfico puede producirles. En estas circunstancias, el riesgo está en que pueden aparecer personas inescrupulosas, capacitadas en informática, que se sientan atraídas por la falta de medidas de seguridad de dichos usuarios de internet y de esta manera pueden engañarlos, estafarlos, robarlos, o extorsionarlos, son los llamados ciberdelincuentes. Como consecuencia de estos delitos informáticos, en el presente trabajo, expondré la problemática en las investigaciones que presentan las fuerzas de seguridad como así también en el ámbito judicial, debido a que los modos para detectar la comisión de estos delitos son obsoletos, ya que deben ser investigados por personas con las mismas capacidades de aquellos que los cometen. Estas falencias son aprovechadas por los ciberdelincuentes que actúan con total impunidad al estar protegidos por el anonimato. Veremos los incidentes judiciales que se presentan en los procesos, en materia de los delitos que nos ocupan, como ser la manipulación de las pruebas digitales, y sus respectivas pericias, que siendo realizadas en la mayoría de los casos sin protocolos de actuaciones, resultan vislumbrar nulidades procesales, que son consecuencia de la falta de conocimiento del personal interviniente. Otro punto importante, será observar la gravedad futura que presenta el desinterés a la regulación actualizada de los delitos informáticos, que será uno de los delitos más graves en un futuro cercano y de más impunidad. Por último, se obtendrán las conclusiones finales del trabajo.

In the present investigation, it will take into account the study and the analysis of how technology evolution has been an element of great utility for the informatics delinquents. Today, the technology is easy to reach of each person with a simple connection to internet, and can support the traffic data of any type, the user don`t know their this conditions, the risk is that can appear malicious persons, quality in informatics, which will feel attack for absence of security measures and in this from, they can be deceive, defraud robber or extort. These persons are called cyber delinquents. In consequence, in this work, I will expose the problematic in investigations thet the security forces present in the juridical countow owing to the mode for detection the perform of these delicts are older and must be investigation for persons with the same capacity as the perpetrator. We will see jurical incidents present in the process, as the realized, in the most of cases. Without judicial records and result to glimpse process nullities as consequence the ungratefulness of the acting personal.Another important point, will be observe the future danger that present the disinterestednessto the actual regulation for informatics risk, that will be one of the most dangerous transgressions in the future with more impunity. In the end, we will get the finally conclusions of this work.

Introducción

La tecnología desde sus inicios se ha ido innovando constantemente, sin un fin que este delimitado. Es por eso, que el mundo actual sería imposible imaginarlo sin ella, ya que esta misma se aplica en los ámbitos laborales, personales, domésticos, automotriz, de navegación, en telecomunicaciones, etc., donde la tecnología ha llegado a transformar distancias de miles de kilómetros en comunicaciones de forma directa y en tiempo real entre personas.

En el momento de requerir información de cualquier tipo con solo utilizar un motor de búsqueda (conexión a intertet), podemos obtenerla de manera inmediata y casi completa, pudiendo realizar esta labor cualquier persona con meros conocimientos en informática. También ha influido en la evolución de la educación, pasando de profesores y alumnos en una aula, a las teleconferencias y trabajos prácticos realizados en forma virtual; podemos destacar como la tecnología nos puede pronosticar el estado del tránsito actual, las condiciones marítimas, climáticas, estados financieros, noticias actualizadas constantemente etc., todo esto, es propiciado de la manera del buen uso, es incondicional no contar con esta tecnología que hoy nos rodea constantemente.

La tecnología se ha convertido en una gran fuente de información y transferencia de datos, existiendo en estas instancias poco control sobre ello, lo que genera un ambiente propicio para aquellas personas que practican actividades con fines maliciosos o perjudiciales para otros.

Aquí podemos mencionar que las personas que se dedican a practicar esto actos delictivos, son los denominados hackers y crackers, que mas delante se mostrarán los conceptos de cada uno. Pero estas personas tienen en su poder una herramienta de magnitudes inimaginables siendo el manejo y conocimiento de los sistemas informáticos, donde uno de sus objetivos es dominar un sistema informático de un Estado, entidad privada, o ingresar a sitios de estricta restricción para tener el control sobre ello. Con el paso de los años, el mundo ha ido informatizando para todo tipo de actividad que una persona se imagine, donde el mundo es inimaginable sin la aplicación de la tecnología en las actividades que se desarrollan a diario.

Estamos ingresando a una era informática, donde estamos aprendiendo a manejar la información mediante la tecnología, pero no hay que olvidar los riesgos de la utilización de la tecnología, complementado con la legislación vigente que intenta aprender de ella para poder regularla correctamente.

El presente trabajo, consiste en observar como problema de investigación: ¿cuándo la legislación Argentina interactúa con los delitos informáticos y cómo impacta en el proceso de investigación judicial en la actualidad? Donde las consecuencias recaen sobre las nulidades judiciales, dejando a la sociedad sin justicia, y dando ventaja a los ciberdelincuentes.

Como objetivo general, la intención es analizar la comisión de delitos, utilizando las nuevas tecnologías, a su vez, cual es su marco jurídico actual en la Argentina, para concluir con los inconvenientes investigativos judiciales que se presentan ante esta nueva actividad delictiva.

Por otro lado, pretendo utilizar dentro del marco metodológico, al tipo de trabajo descriptivo, donde se realizarán descripciones de la legislación vigente Argentina en materia de Derecho Informático, como también en legislación Latinoamérica, donde un punto en común es la problemática investigativa y sus conflictos legales que en ocasiones se presentan. Acompañado del método cualitativo, intentando tener una apreciación mediante las experiencias vividas, a la hora de atravesar por un método improvisado de investigación dentro de las fuerzas de seguridad, como así también las partes que imparten justicia.

Para culminar y poder dar inicio al presente trabajo, sostengo que el delito informático, recién ha iniciado su camino delictual, con el presente pretendo mostrar su peligrosidad futura, generar conciencia a quienes legislan para poder algún día obtener una correcta, especifica legislación penal, y procesal, brindando así protección a los individuos de todo el territorio nacional, que en un futuro no muy lejano será ésta, una sociedad tecnológica en su totalidad.

➢ Capítulo 1: Antecedentes en materia tecnológica informática.

I. Antecedentes de la tecnología informática.

Para comenzar podemos indicar que la tecnológica informática tiene sus primeros inicios en el siglo XX, con la llegada de la Primera Guerra Mundial en 1914, donde las estrategias bélicas que incitaban al éxito de la batalla, solicitaban la necesidad de personas capacitadas para las investigaciones en desarrollos tecnológicos, como científicos, matemáticos, físicos, químicos, etc., con el objetivo de crear armamentos más efectivos.

Este tipo de accionar se ha ido implementando en el desarrollo de los vehículos, embarcaciones y personal militar que se dispersaba por los campos de combate, como por ejemplo los instrumentos de medición, radares, comunicaciones inalámbricas y armas. Este desarrollo tecnológico se ha multiplicado con el paso del tiempo, para volver a tener un impulso amplio con la Segunda Guerra Mundial, la cual se originó en el año 1939, teniendo más experiencia en la creación de elementos tecnológicos, la tecnología lograba su más importante progreso.

Finalizada la Segunda Guerra Mundial, los Estados que intervinieron en la guerra, sufrieron las consecuencias de victorias o derrotas, pero la ciencia de la tecnología fue desarrollándose para que poco a poco con los años siguientes, esos elementos tecnológicos fueran teniendo utilidad en la vida cotidiana de las personas, como por ejemplo la radio, el televisor, los automóviles, las comunicaciones.

Ya para los años sesenta, aparecía la palabra "computadora", que se la define como "Máquina electrónica capaz de realizar un tratamiento automático de la información y de resolver con gran rapidez problemas matemáticos y lógicos mediante programas informáticos". (Real Academia Española 2016, p. 1).

En el año 1961, un grupo de informáticos encabezado por Ray Tomlinson, quién se graduó como Ingeniero Informático en el año 1941, en la ciudad de Nueva York, trabajaba en un proyecto de transferencia de archivos entre una computadora y otra. Habiendo perfeccionado el sistema Arpanet, con un software llamado Cpynet, el cual permitía el tráfico de datos entre usuarios utilizando como símbolo genérico el arroba (@), de esta manera se organizó un grupo de personas que se dedicaban al estudio de la informática y cada uno con su computadora diagramaron un posible conexión entre cada

una de las máquinas, pudiendo así enviar y recibir datos, lo que más tarde conocemos como Email. (Jane, 2009).

Acontecimientos como estos han generado con el paso del tiempo una revolución del desarrollo tecnológico, que aún se mantiene presente en el, los días, meses y años, donde la tecnología genera un camino que no tiene final. Este emprendimiento que ha sido totalmente exitoso teniendo como fin, el intercambio de datos entre computadoras, no importando el lugar o la distancia donde estén, evolucionando hasta la actualidad, donde este tipo de interacción se la conoce como "internet".

La palabra internet, se la define como "Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación" (Real Academia Española 2016 p. 1).

Para brindar un clara explicación del funcionamiento de internet, pudiéndose explicar como una conexión hacia otras computadoras, las cuales se pueden realizar todo tipo de transferencia de datos, ya sean imágenes, textos, videos, etc., que a su vez estos archivos pueden ser colocados en la world wide web se entiende por estas siglas que a un sistema donde se distribuyen de documentos o datos de hipertexto o hipermedios entrelazados mediante internet. Donde por intermedio de un navegador web, un usuario visualizar distintos sitios web que contienen información de cualquier índole.

Como un ejemplo del funcionamiento de internet, podemos mencionar una cierta cantidad de computadoras distribuidas en todo el mundo donde con una conexión común entre ellas, inalámbrica o por cable (internet), donde se transfieren datos de forma inmediata, aun así estando a miles de kilómetros una computadora de otra.

Esta nueva forma de comunicación y tráfico de información ha generado un impacto mundial, provocando en un principio un impacto en los envíos de mensajes, sean cartas, resoluciones, protocolos, planos, etc., que eran enviados a través de personas llamadas correos, los cuales eran lentos y costosos, pasaron a ser obsoletos e innecesarios.

Jane, C. (2009). El Padre del Email. *El periódico.* (s/v). Recuperado de http://www.elperiodico.com/es/noticias/ciencia-y-tecnologia/20090617/ray-tomlinson-envio-primer-correo-electronico-1971/113183.shtml

Esta nueva forma de comunicación através de las computadoras mediante la conexión de internet, fue utilizada en principio por Estados y corporaciones que con respaldo económico, la utilizaron para insertar las nuevas tecnologías con fines militares, científicos, espionaje etc.

Con el paso del tiempo, la tecnología comenzó a tener múltiples funciones donde la sociedad podía obtener los beneficios de ella. De esta forma es que se fue insertando en la vida cotidiana de las personas de recursos económicos altos.

Pero esto ha ido cambiando, ya que con los años dejó de ser un fenómeno desconocido, bajaron los costos y hoy la tecnología se encuentra en la mano de cualquier persona, donde pasó de una computadora de tamaño considerable se ha convertido en una tableta, un GPS, un teléfono celular con sistemas operativos múltiplesetc., cumpliendo las mismas y mas funciones una computadora de los años sesenta.

II. Conceptos: informática, computadora, Internet, la Web.

Informática.

La informática, se la puede definir como el conjunto de datos que son transferidos de forma automática, entre computadoras u ordenadores donde existe un EMISOR y un RECEPTOR. Sosteniendo estas palabras mediante la "Ciencia que estudia el tratamiento automático de la información". (Rivera, 2006-2007, p. 1)

El científico K. Steinbuc, más conocido como el padre de la informática, tomo el concepto de procesamiento automático de la información, que partiendo de esa base luego con el paso de los años fue ampliándose pero siempre manteniendo las bases de Steinbuc, por ello, podemos apreciar el concepto de informática más actual, que es "la informática es una ciencia que estudia métodos, procesos, técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital. García J. (2015/13/11). La informática, conceptos básicos y datos históricos. [Etimología]. Recuperado de http://lainformaticayelcomputador.blogspot.com.ar/

Rivera, M. L. (2006-2007). Revista Jurídica. Obtenido de firma digital, consideraciones jurídicas: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20revista%20juridica/Revista%20Juridica%2006-07/articulos/02Firma.pdf

Por último, quiero citar el siguiente concepto, "ciencia del tratamiento racional, mediante máquinas automáticas, de la información, considerada como el soporte de los conocimientos humanos y de las comunicaciones de los campos técnico, social y económico." (Del Castillo Torres, 2005, p. 492).

Computadora

Se entiende por computadora, a una maquina con funciones electrónicas controladas por una persona, que con los elementos electrónicos internos de cálculos, lógica, se originan programas o resultados. En estas circunstancias una computadora es capaz de recibir y re direccionar ordenes, como así también almacenamientos de datos y transferencias de ellos.

Estas máquinas se encuentran compuestas por un hardware, siendo este la parte física, como un teclado, un monitor, una impresora, un C.P.U. etc., también tenemos el software, siendo el más importante ya que es la parte lógica de la máquina, el cerebro compuestos por algoritmos y números binarios que forman programas para que pueda funcionar una máquina. (Lugo Ramírez, s/f).

También se puede decir acompañando la definición antes citada, siendo un "conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras". (Cuapio, s/f, p. 2).

Es importante comprender que las computadoras están confeccionadas por sistemas operativos, los cuales están integrados por programas, llamados también software, complementando toda la parte lógica de la misma.

Del Castillo Torres, L. (2005). Manual Del Auxiliar Administrativo de Instituciones Sanitarias, {*versión electrónica*}. *Conceptos.* 3 (1) 492-492.

Lugo Ramírez, (s/f, p. 6). *Introducción a las computadoras*. Unidad de Servicios al Usuario (Vol. I). Recuperado de http://www.uprm.edu/cti/docs/manuales/manuales-espanol/vax-vms/manuales/Intcomp.pdf

Cuapio M. R. (s/f). A*ctualización judicial en el estado de Tlaxcala, dentro del marco del derecho informático y la informática jurídica en el siglo XXI. Marco Conceptual*. Recuperado de http://www.ordenjuridico.gob.mx/Congreso/pdf/172.pdf

Esta parte es esencial, ya que en la actualidad los sistemas operativos han evolucionado a la telefonía móvil que dejó de ser un simple aparato de llamadas telefónicas y mensajería de texto, para convertirse en teléfonos con las posibilidades de sacar fotografías, realizar videos, instalar programas de entretenimiento, aplicaciones, juegos, podernos utilizar GPS, transferir datos de un teléfono a otro a través de señales de bluetooth, rastreos satelitales, etc.

Una de las funciones principales que comparte esta tecnología es la conexión a internet que tienen los mismos, encontrándonos así con minis computadoras de mano portátiles.

Es por esto, que la posibilidad de poder a caer en manos de un ciberdelincuente, son muy altas, ya que desde temprana edad se comienza a utilizar este tipo de tecnología.

Como para tener una noción de las personas que utilizan hoy en día la telefonía móvil, con acceso a internet, como así también las computadoras, quiero citar un informe realizado por el I.N.D.E.C. en el cual nos indica que en los hogares donde hay personas con edades entre los 12 y 17 años de edad utilizan más de un teléfono celular, juntamente con una computadora con acceso a internet, que en los hogares que no existen integrantes de esas edades. Esto nos quiere decir, que desde la temprana edad ya se comienza a mantener contacto con la tecnología, y los accesos a internet. I.N.D.E.C. (2011). *Encuesta Nacional sobre Acceso y Uso de Tecnologías de la Información y de la Comunicación.* Informe preliminar sobre indicadores básicos de acceso y uso. Resultados de mayo-julio de 2015. (2). Recuperado de http://www.gobiernoabierto.gob.ar/multimedia/files/TICs_nacional.pdf

Por otro lado en nuestro país, las provincias que mayor contacto con la tecnología y acceso a internet son, Tierra del Fuego, Antártida e Islas del Atlántico Sur, Santa Cruz, Chubut y Ciudad Autónoma de Buenos Aires. Respecto a solamente los accesos a internet la población urbana de 10 años y mas utiliza internet con mucha frecuencia, y siendo un 95,6 % es utilizada todas las semanas. El 61,8 %, de las personas utilizan internet todos los días, para disminuir en un 33,8 %, en las conexiones de internet entre uno y cuatro días. I.N.D.E.C. (2011). *Encuesta Nacional sobre Acceso y Uso de Tecnologías de la Información y de la Comunicación.* Informe preliminar

sobre indicadores básicos de acceso y uso. Resultados de mayo-julio de 2015. (2). Recuperado de http://www.gobiernoabierto.gob.ar/multimedia/files/TICs_nacional.pdf

Atento a los relevamientos de datos nacionales realizados por el I.N.D.E.C., podemos decir que nos encontramos con una sociedad argentina tecnológica que recién esta comenzado a manipular las nuevas tecnologías acompañadas de los accesos a internet. Por consecuencia es que se deben mantener las medidas preventivas y de seguridad ante posibles daños colaterales por la utilización de la misma.

Internet

Internet, es una red que se encuentra conectada con computadoras u ordenadores en todo el mundo, lo que provoca el tráfico de información constante entre los usuarios conectados. En esta red, podemos encontrar tráficos de datos con fines laborales, académicas, personales, políticos, de seguridad, de salud, etc., estar conectado a una red nos genera grandes beneficios obteniendo información de todo tipo, sin tener la necesidad de permisos, salvo información confidencial o protegida jurídicamente.

Para que una computadora se conecte con otra, estas deben entablar los mismos canales de tráfico de información, esto se lo denomina protocolo y conocido en el mundo informático como TCP/IP, sin un protocolo una máquina no podría recibir ni enviar información a la otra. Lujambio, I., Martínez, L., Rodríguez, E. y Fernández, C. (2005). Guía práctica de internet. *{Versión electrónica} Acercando el uso de la Red a las Organizaciones Comunitarias* 2. (1). 17-19.

World Wide Web

La World Wide Web, conocida también como, WWW o Web es un sistema de información que tiene como fin distribuir los datos por internet, a través de una interface común para los datos que se transfieren, como los Hipertextos y los Hipermedias.

La comúnmente llamada Web, es el lugar en internet donde se colocan todos los enlaces para que cualquier usuario que se encuentre conectado a internet pueda acceder al mismo si lo desea e interactuar de la forma que desea, ya sea entretenimiento, laboral, económico, salud, interés, compras etc. Sin este sistema, el entrelazamientos de direcciones de páginas web, o también llamados URL, sería imposible navegar por el mundo virtual. Área de Tecnología de la Información y de las Comunicaciones

Aplicadas, (2011). Manual Básico de creación de páginas web. *Creación de páginas webs. 1* (1). Recuperado de https://www.um.es/atica/documentos/html.pdf

Para que funcione la Web es necesario un navegador web, que consiste en ser una aplicación que trabaja conjuntamente con internet y los sistemas operativos para que se pueda tener lectura de cualquier sitio que se publica en internet, como así también todo tipo de archivo, como por ejemplo, videos, fotográficas, textos, juegos, etc. [1]

III. Delitos informáticos

El delito informático aún no se encuentra con una definición universal única, pero autores atentos a las necesidades jurídicas, han intentado enmarcar a su criterio una definición que pueda responder a este tipo de delitos. Es por ello, que a continuación se mencionan Organismos como autores expertos en derecho informático.

La Asociación de Argentina de Derecho de Alta Tecnología, entiende atravez de la Organización para la Cooperación Económica y el Desarrollo (OCED), quien define al delito informático como, "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos. (Paterlini, Vega, Guerriero y Velázquez , s/f, p. 1)

También podemos tomar lo siguiente "El delito electrónico, también denominado informático, es la conducta típica, antijurídica y culpable, no ética o no autorizada, vinculada al procesador automático de datos y/o transmisiones de datos." (Ríos Patio, s/f, p. 2).

1. Menalkiawn. (2013). Manual básico de Seguridad Informática para activistas. *una guía para proteger nuestros ordenadores y a nosotras mismas hacer frente a la represión y extender una cultura de seguridad. 1*. (1). Recuperado de http://mexico.indymedia.org/IMG/pdf/libro_manual_seguridad_informa_tica_activistas.pdf
   Paterlini N., Vega C., Guerriero G. y Velázquez M. (s/f). Delitos Informáticos. *Antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos. 1*. (1). Recuperado de http://www.aadat.org/delitos_informaticos20.htm
   Dr. G. Ríos Patio. U.S.M.P. Facultad de Derecho, Revista Sapere. *Delitos Electrónicos.* (2-2). http://www.derecho.usmp.edu.pe/instituto/revista/articulos/DELITOS_ELECTRONICOS.pdf

Por último, mencionamos la cita de "Al que sin autorización obtenga, conozca, altere o destruya información confidencial en un sistema informático". (Montano, 2008, p. 157)

Atento a las definiciones presentadas es que me advierto a decir que los delitos informáticos, son aquellos en los cuales se observan conductas típicas, antijurídicas, que se concretan utilizando como medio para tal fin algún elemento reconocido por la tecnología o nuevas tecnologías.

Los delitos informáticos, como hemos dicho tienen relación con la tecnología ineludiblemente, que con el transcurso del tiempo se han cometido de forma silenciosa y han logrado tener mayor difusión con el paso de los años. Estos delitos se los puede clasificar de la siguiente manera:

IV. Clasificación de los delitos informáticos.

Según la Organización de las Naciones Unidas (O.N.U.) se clasifican en:

- Fraudes cometidos mediante manipulación de computadoras.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos computarizados.

Por otro lado, se pueden mostrar las conductas que pueden perjudicar a los usuarios de los sistemas informáticos como ser:

- Acceso no autorizado.
- Actos dañinos o circulación de material dañino.
- Intercepción no autorizada.

Montano Álvarez, A. A. (2008) La Problemática Jurídica en la Regulación de los Delitos Informáticos, *La Problemática Jurídica en la Regulación de los Delitos Informáticos. 1*. (1) recuperado de http://www.ordenjuridico.gob.mx/Publicaciones/Tesis2010/01_LDP_MONTANO.pdf

Una vez presentada las definiciones oportunas, es de tener en cuenta saber cómo se conoce esta actividad delictual cometida con la tecnología, el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos en el cual converge en citar a la palabra ciberdelincuencia, la cual se manifiesta como a las tecnologías globalizadas de la información y las comunicaciones, en particular a Internet, para la comisión de actos delictivos de alcance transnacional.[2]

Por otro lado, las personas que se dedican a esta actividad delictiva, han recibido la denominación de hackers, estas personas se dedican exclusivamente a la investigación de los sistemas informáticos, (Software), donde el trafico de información entre los ellos provocan un avanzado conocimiento en materia informática. En principio no resultan ser delincuentes, ya que los mismos pretenden mediante la investigación llegar a resultados desconocidos, lindando sobre lo ilegal, tienen como finalidad la creación de nuevas funciones sobre el software ya creados. También encontramos a los crackers conocidos como "vandálicos virtuales", que son aquellas personas que su finalidad es romper o dañar los sistemas de seguridad de bases de datos, empresas, policiales, políticas, judiciales etc. Aquí nos encontramos con personas que incurren en los actos de ilegalidad e forma directa. (Sain, 2010, p. 92-93).

Un informe elaborado por el F.B.I. demuestra que con la aparición de internet, la sociedad comenzó a tener manejo de esta tecnología, aparecieron los delitos del robo de identidad, de estafa para luego con el paso del tiempo evolucionar a la extorsión.

Este tipo de delitos provocaban grandes perjuicios económicos, y daño a los Derechos personales, donde las victimas sufrían perdidas generosas de dinero, y muchas veces intervenían en determinados casos los profesionales como psicólogos, médicos, etc.

El delito de robo de identidad, interactúa con la figura legal de la extorsión, donde el robo de una fotografía y datos traen resultados inesperados y el victimario tenía la ventaja de permanecer en el anonimato por siempre.

2. Saín, G. (1994). *Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos.* (43-44). Argentina, Rustica.
   Saín, G. (2010). *El fenómeno del cibercrimen en Internet y la World Wide Web, una mirada criminológica.* (92-93). Argentina, Rustica.

El esfuerzo y el interés del F.B.I., por regular, prevenir y combatir estas actividades delictivas para un futuro más seguro, y viendo la gravedad de los hechos que podrían acontecer mediante el desarrollo tecnológico, se vió obligado a hacer públicos, informes criminalísticos y a cooperar entre Estados para combatir a estos ciberdelincuentes. F.B.I. (2015). *Internet Crime Complaint Center.* E.E.U.U. Recuperado de www.fbi.gov/about-us/investigate/cyber

➢ Capítulo 2: Los delitos informáticos en el mundo y la legislación comparada.

I. Acontecimientos mundiales y la concienciación de los delitos informáticos.

La proliferación de los delitos informáticos en las últimas décadas ha sido asombrosa, donde los países más desarrollados como Estados Unidos, Francia, España, Alemania, Israel entre tantos, pero en Sudamérica se destaca a Puerto Rico, que todos ellos tuvieron que visualizar esta problemática a futuro y sus consecuencias, si no existe legislación y regulación, donde se llega a opinar que la tercer guerra mundial podría realizarse a través de los ordenadores.

Esta guerra fue llamada ciberguerra, donde no habría militares enfrentados, sino todo tipo de personas con conocimientos de informática con fines de destrucción, daños, o perjuicios a otros Estados. La gravedad de esta posible guerra, se expande mediante el desarrollo a diario de la tecnología, quedando siempre un paso atrás de aquellas personas que pretenden mantener un orden o evitar una posible guerra cibernética. M. Rogers, La NSA se prepara para la guerra mundial cibernética. (Muller, 2015, p.1).

Un ejemplo claro y actual de lo antes expuesto, son los acontecimientos gravísimos que han azotado al mundo, como los atentados terroristas que fueron víctimas los ciudadanos franceses en su país. Muchas personas, Estados, Organizaciones han repudiado estos delitos.

Muller, E. (2015). Internacional. *La NSA se prepara para la guerra mundial cibernética, según Der Spiegel.* (10-10). Recuperado de http://internacional.elpais.com/internacional/2015/01/17/actualidad/1421500678_347192.html

Ante ello, existe una organización no gubernamental, sin fines de lucro, que ante el repudio de los atentados en Francia, anunció utilizando los medios de comunicación, una venganza mediante una ciberguerra contra el Estado Islámico, (autores de los atentados terroristas en Francia), también en su anuncio refieren que se iniciarán ciberataques masivos.

Esta organización de nombre Anonnimus, más conocida por la máscara blanca de Fawkes Guy, que sus representantes utilizan para darse a conocer, resultan ser personas de amplios conocimientos informáticos, siendo la mayor red de activistas y de hackers del mundo. El Día (2015). *Annonimus declaró la guerra cibernética*. (10-10).

Es por este tipo de acontecimiento que en Sudamérica, se tomó como ejemplo en este trabajo la legislación de Puerto Rico, siendo una de las más avanzadas en materia de delitos informáticos, con una problemática actual controlada, que se encuentra rodeada de legisladores con conocimiento en la materia, y de la gravedad que puede desencadenarse con un delito informático, propiciando impunidad y anonimato en los ciberdelincuentes, si existe desinterés y falta de conocimiento a la hora de legislar una Ley.

También, en Tel Aviv, Israel tienen un gran objetivo que es la guerra contra el cibercrimen, donde como punto principal de los actos delictivos, es el fraude en internet el cual se desparrama por todo el mundo.

La O.P.C. (organización Policial Internacional), más conocida en el mundo como Interpol donde se mantuvo una reunión en Francia con cuarenta y nueve países de Europa, que tienen como prioridad máxima el combate contra el cibercrimen, siendo que se está distribuyendo por todo el mundo, donde aún hay muchos países que no se encuentran con las medidas de seguridad informáticas, como tampoco tiene una legislación acorde a la temática del delito informático. También en la misma reunión se publicó un informe de la Universidad Metropolitana de Londres, donde se vislumbra que el 80% de los delitos en línea, o sea con conexión a internet están vinculados con bandas que interactúan con otros miembros del mundo.

Una nueva generación de bandas organizadas está afectando Israel, donde se comienza con el reclutamiento de miembros otros países, que no tienen vinculación diplomática. De esta manera es que se manejan desde distintos puntos del mundo un líder de una ciberbanda de crimen organizado, tomando decisiones desde cualquier

lugar, para que luego los miembros de la organización los efectivicen. La ventaja que les ha concebido internet, ha promovido su migración hacia la tecnología del tráfico de datos, que como hemos mencionado en el presente trabajo, otorgan seguridad de impunidad a los ciberdelincuentes.

Un ejemplo de este caso de ciberbandas organizadas, es el arresto que concretó la policía de Malaya de unos doscientos ciberdelincuentes de nacionalidad China y Taiwanesa, que cometían fraude por internet integrado por dos bandas siendo un único líder un jefe taiwanés. Esta banda utilizaba lugares temporales en distintos puntos de Oriente, una vez instalados los hackers embolsaban miles de millones de dólares por medio de fraude a tarjetas de crédito y cuentas bancarias, aprovechando sitios de fútbol y apuestas.

En Israel tiene una estadística de mil ataques a la red global, provocando así una pérdida económica de millones de dólares, en consecuencia mediante las fuertes políticas de prevención y combate contra los ciberdelincuentes la O.C.P, ha propuesto que se cree un establecimiento en Singapur a los fines de entrenar a las policías del mundo ante el delito informático.[3]

En España, la Jefatura de Estado, ha confeccionado una Ley en la cual brinda protección a las instalaciones específicas del país, donde prevé la posibilidad de ataques físicos como cibernéticos. Para mencionar un ejemplo, sería de carácter catastrófico que se cometa un ciberataque a los sistemas de hidráulica del país, donde se abriesen todas las represas, la cantidad de muertes y consecuencias económicas. También podemos tener en cuenta un ciberataque a los sistemas de tráfico vehicular, como aeronáuticos, donde los resultados de ellos serian impactantes. Ante posibles y en algunos casos ciber ataques ya provocados.

Siguiendo con el país europeo el cual presenta Ley 8/2011, donde en su Preámbulo y noveno párrafo refiere que es necesario crear una norma cuyo objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo, tanto de carácter físico como cibernético.[4]

3. Khoo Boon Huim, (2012), Interpol le declara la guerra al cibercrimen , *Fraude y Cibercrimen*, (1-1). Recuperado de https://haddensecurity.wordpress.com/2012/page/84/ https://haddensecurity.wordpress.com/2012/page/84/
4. Ley 8/2011, (2011), Medidas para la Protección de las Infraestructuras Críticas. Jefatura del Estado, España.

En China, en el Ejército Popular de Liberación al observar la gravedad y complejidad que presenta una prevención y una posterior investigaciones para el combate del cibercrimen, preparan las fuerzas de seguridad para el combate y enfrentamientos informáticos. Los cuales contarán con tecnología de excelencia, unidades especiales en tecnología digital, donde China observa a futuro una problemática mundial de una ciberguerra, que se hace presente ante las crecientes presiones internacionales por los ataques informáticos realizados por hackers. Infobae, (2013), Política. *China entrena a sus militares para una ciberguerra*. *1* (1). Recuperado de http://www.infobae.com/2013/05/29/1072314-china-entrena-sus-militares-una-ciberguerra

En Estados Unidos se la conoce como la "Cool War" o la "Guerra Fría cibernética", donde la principal amenaza consta de computadoras con conexión a internet, teniendo esos dos elementos estamos en condiciones de experimentar los posibles efectos que podría causar un hackers.

La Agencia de seguridad Mandiant, realizó un informe ante una señal de alerta donde se practicaba espionaje cibernético, donde se imputan los hechos a países como China. Muchas entidades del mundo han sufrido ataques por ciberdelincuentes, o hackers, donde se pudo establecer mediante investigaciones que los ataques provenían de un edificio en Shangi, donde se emplaza la sede de operaciones de la unidad 61398 del Ejército de Liberación Popular, donde el objetivo de estos ciberdelincuentes era robar todo tipo de información militar, económica y tecnológica

Atento a lo expuesto en la República Argentina, no existe para las fuerzas de seguridad una posible ciberguerra, o ciberataque, pero hasta que punto nos encontramos fuera de los objetivos de los ciberdelincuentes.

En los últimos tiempos hemos tenido amenazas hacia la presidencia de la Nación, a través de emails, recibidos a las distintas casillas de correos gubernamentales y de fuerzas de seguridad, en donde se ponía en riesgo la vida de misma, con mensajes amenazantes y con hechos de muertes adjudicados por parte del Estado Islámico.

Por tal razón, es que se reunieron todas las fuerzas federales y provinciales a los fines de poder dilucidar un posible inicio de investigación, lo cual era desconocido para todos. Ahora ante estos acontecimientos ¿cuáles son las medidas preventivas o métodos investigativos a seguir? No existe una respuesta clara, ya que no se advierte forma

alguna de cómo iniciar una investigación en contra de una o más personas con conocimientos en materia informática.

En el hecho mencionado, se utilizó un navegador web llamado Red Tor, la cual su única finalidad es brindar anonimato a cualquier persona que navega por internet. Este anonimato se realiza mediante el enmascaramiento de la Dirección IP original de conexión, otorgando una al azar ubicada en cualquier parte del mundo. Por lo tanto, realizar una amenaza a través de la RedTor, resultaría imposible para las policías de la República Argentina esclarecer un hecho.

Como posible solución se realizan investigaciones con la colaboración de personas civiles que conocen la temática de la programación informática, donde hasta a ellos mismo les resulta imposible llegar al autor de la amenaza. Esta es una herramienta de excelencia la cual se puede descargar de forma gratuita, sin mediar trámite engorroso alguno, pero las consecuencias con el uso delictivo pueden ser calamitosas. [5]

II. Convención de Budapest, convenio sobre la Ciberdelincuencia

En materia de delitos informáticos, poco se encuentra legislado en el mundo siendo un delito novedoso de difícil investigación, y pocas herramientas para la prevención. Atento al desarrollo tecnológico masivo de los últimos años, y el crecimiento de la actividad delictiva con utilización de la tecnología, ha generado que se redactara el Convenio de Budapest, siendo uno de los motores impulsores en materia legislativa para el resto de los Estados para adecuar su propia legislación mediante el modelo del Convenio.

El Convenio tiene su origen en Europa, siendo una de las regiones donde más se ha desarrollado la cultura de cooperación jurídica y policial internacional para el combate de todo tipo de delincuencia. Este convenio fue firmado en Budapest en el año 2001, entrando en vigencia el 1 de julio del año 2004, y persigue dos objetivos, en primer lugar tiene como su objetivo mantener cubiertas todas las ramas del Derecho Penal y Procesal, cuando estos se vean interactuando con los delitos informáticos.

5. División Contraterrorismo, (2015), Dirección Cibercrimen, Policía de la Provincia de Buenos Aires Causa FLM 104/2014.

En segundo lugar, pretende servir como ejemplo legislativo para el resto de los Estados, y observar la gravedad delictiva que asisten los delitos informáticos y por último, es mantener una cooperación entre los Estados para la prevención y combate del Delito Informático.

El Convenio que se encontraba destinado a armonizar las legislaciones en los Estados que firmaron el acuerdo, siendo 47 países, con la posibilidad que se puedan insertar los restantes.

El presente está integrado por un Preámbulo en el cual, hace mención de la fructífera función del mismo con una visión a futuro: "convencidos de la necesidad de aplicar, con carácter prioritario, una política común con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular y mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional."[6]

Para lograr una uniformidad legislativa mundial en delitos informáticos respecto al Derecho Penal, el Convenio dió inicio a su lección con conceptos claves que los podemos encontrar en el Artículo 2 al Artículo 9.

En ellos, se adoptan los sistemas informáticos y los sistemas de datos, falsificación informática, fraude informático; uso de la tecnología computacional para crear, distribuir o procesar pornografía infantil y el uso de la tecnología computacional para cometer infracciones a la propiedad intelectual.[7]

Las actividades delictivas que tienen en la mira a los sistemas informáticos y a los datos son: obtener acceso no autorizado a ellos, daño y abuso de dispositivos. Pero también la Convención ha tratado el Derecho Procesal, teniendo en cuenta la problemática investigativa, a los fines de poder facilitar la ejecución de las diligencias judiciales mediando las garantías constitucionales de cada Estado, en tal sentido el Convenio en sus Artículos 16 hasta el Articulo 21, encontramos el tratamiento que se le otorga a la preservación y producción de la prueba digital, o evidencia virtual; solicitudes de búsquedas para el secuestro de los sistemas informáticos, con la autorización del poder judicial para diligenciar las medidas protocolares.[8]

6. Convención de Budapest, (2001). Preámbulo, 4to. Párrafo.
7. Convención de Budapest, (2001). Preámbulo, Artículo 2-9.
8. Convención de Budapest, (2001). Preámbulo, Artículo16-21.

Luego en los Artículos 23 al Artículo 24, menciona el colaborar con la información obtenida, preservar, interceptar y revelar datos de tráfico y el contenido del mismo, también brinda tratamiento a la extradición de los ciberdelincuentes.

El objetivo procesal, pretende agilizar los procesos judiciales en materia de delito informático, habiendo países que utilizan la legislación vigente para realizar procedimientos de resguardo de prueba digital, cuando el tratamiento que merece es totalmente diferente, acarreando consecuencias gravísimas con la nulidad de una investigación.

III. Declaración del Fortalecimiento de la Seguridad Cibernética en las Américas.

La tecnología es interpretada como una preocupación mundial donde se intenta mediante la coordinación y cooperación de los Estados la posibilidad de poder prevenir y combatir los delitos informáticos. En tal magnitud nos encontramos que en el desarrollo tecnológico a nivel mundial se comienza a insertar la figura del delito de terrorismo mediante el uso de la tecnología.

En este caso se pretende lograr la prevención, como así también el combate. Ocupándonos de la Declaración del Fortalecimiento de la Seguridad Cibernética en las Américas, la cual entiende que los acontecimientos delictuales producidos por el desarrollo tecnológico y el impacto que puede tener en un futuro con consecuencias de desestabilizad hacia un Estado y también a nivel mundial.

La Declaración reconoce los ataques de alto riesgo social y mundial en materia de delitos cibernéticos en los cuales el delito de terrorismo es el eje de la Declaración; la intención de la Declaración es el reconocimiento del delito de terrorismo mediante el uso de las nuevas tecnologías, por ello se busca poder prevenir y combatir los actos terroristas mediante el uso de las nuevas tecnología, también refleja la cooperación entre Estados miembros, por último quiero citar uno de sus párrafos donde reza, "La importancia de reforzar la seguridad y la resistencia de tecnologías de infraestructura crítica de información y comunicaciones (TIC) ante las ciber amenazas, con especial énfasis en las instituciones gubernamentales críticas así como en los sectores críticos para la seguridad nacional, incluyendo los sistemas de energía, financieros, transporte y telecomunicaciones." [9]

9. Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas. (2012).

Quiero mencionar la actitud de la República Argentina de haber firmado la Declaración en vísperas de "prevenir, impedir y atenuar las consecuencias de posibles amenazas a la infraestructura crítica y de estar preparados para responder a tales amenazas, así como de garantizar la seguridad de las instalaciones y de quienes las ocupan como asimismo la necesidad de alentar a los Estados Miembros a estrechar vínculos con el sector privado y la sociedad civil, cuando corresponda, en sus respectivos países, para desarrollar programas de fomento de la capacidad preventiva y de protección contra las amenazas a la infraestructura crítica."[10]

Esta Convención es importante en relación al delito informático, el cual dispone en sus articulados legislación en materia de Derecho Penal citando sus artículos titulados, "Acceso Ilícito, Interceptación Ilícita", "Ataque a la integridad de datos", "Ataque a la integridad de sistemas", "Abuso de dispositivos", "Falsificación informática", "Fraude informático"; dentro de los delitos relacionados con el contenido, en este Convenio nos encontramos con "Delitos de relacionados con la pornografía infantil", "Delitos con infracciones de la propiedad intelectual y de derechos afines", (Art. 2, Art. 3, Art. 4, Art. 5, Art. 6, Art. 7, Art. 8, Art. 9 y Art. 10.[11]

Por otro lado brinda regulación en materia de Derecho Procesal, (Art. 14. Convención de Budapest sobre Ciberdelincuencia, 2001). Por último, quiero destacar los artículos relacionados a la regulación de los procedimientos que entienden en materia de prueba y resguardo judicial, siendo los siguientes artículos titulados como, "Condiciones y salvaguardia", "Ámbito de aplicación de las disposiciones de procedimiento", "conservación rápida de datos informáticos almacenados", "Conservación y revelación parcial rápida de los datos relativos al tráfico", (Art.15, Art. 16, Art. 17.[12]

10. Disposición Nº 2/2013, Jefatura de Gabinete de Ministros Secretaria de Gabinete y Coordinación Administrativa Subsecretaria de Tecnologías de Gestión Oficina Nacional de Tecnologías de Información.
11. Convención de Budapest, (2001).
12. Convención de Budapest, (2001).

IV. Legislación Comparada en Latinoamérica

La intención de observar la legislación comparada, de algunos de los países de Latinoamérica, es para tener en cuenta, como dependiendo del Estado existe una legislación clara, especifica, y de prioridad en delitos informáticos. También veremos como otros Estados, hacen mención en escasos artículos, haciendo ambigua una posible conducta delictiva cibernética. Para luego culminar a mí entender con una legislación ejemplar, que sería de gran aporte para la protección jurídica de los ciudadanos Argentinos.

Ley 19223, Ley de Delitos Informáticos, Chile.

En Chile, tenemos la Ley 19223, que respecto a los delitos informáticos, refiere en escasos artículos la tipificación delictiva.

En su Artículo 1º.- hace mención de la destrucción, o hacer inutilizar un sistema operativo, que impida su funcionamiento, en este caso resulta ambiguo el relato de la tipificación, dejando vacios legales.

Por otro lado tenemos el Artículo 2º, que hace mención al apoderamiento, usar o dar a conocer información indebida que se encuentre contenida en un sistema operativo. Luego habla de interceptación o interfiera o accesos. De igual forma que el artículo nº 1, aquí observamos la vulnerabilidad que presenta al no especificar la temática delictiva.

Por otro lado en el Artículo 3º, encontramos las acciones de alterar, dañar o destruir datos de un sistema operativo. Y por último en el Artículo 4º, encontramos la revelación y difusión de datos. [13]

Luego en años posteriores, se sancionó la Ley La Ley 20.009, la cual como fin único es la de regular las responsabilidades cuando las conductas delictivas sean de características de robo, hurto, o extravió de tarjetas de créditos. [14]

13. Ley 19223, Delitos Informáticos, Chile. (1993).
14. Ley 20.009, Limita la Responsabilidad de los Usuarios De Tarjetas de Crédito por operaciones realizadas con Tarjetas Extraviadas, Hurtadas o Robadas. (2005).

Por último, con la última actualización en materia de delitos informáticos, Chile presento la Ley 18.168, la cual regula de una forma amplia las telecomunicaciones, y aquí se aprecia la incorporación de las tipificaciones de la interferencia, captación ilegitima de las señales de telecomunicaciones.[15]

Resumiendo en el país vecino de Chile, encontramos una ley escasa ambigua, con una problemática de no encontrar la conducta típica de la pornográfica infantil en su legislación, también presenta con muchos vacios legales que brindan ventajas a los ciberdelincuentes y desprotección jurídica a los ciudadanos.

Ley Nº 1.160/97, Delitos Informáticos, Paraguay

En Paraguay encontramos legislación en materia de delitos informáticos a partir del año 1997, en la cual se tipifican conductas, ampliando el espectro de conductas delictivas en comparación con la Ley 19223 de Chile. En principio debemos mencionar que el Código Penal Paraguayo, reconoce los delitos de:

- Violación del secreto de la comunicación
- Alteración de datos Sabotaje de computadoras
- Operaciones fraudulentas por computadora
- Aprovechamiento clandestino de una prestación
- Perturbación de instalaciones de telecomunicaciones
- Pornografía infantil
- Intercepción, secuestro, apertura y examen de correspondencia
- Intervención de comunicaciones [16]

15. Ley 18168, Ley General de Telecomunicaciones, Chile. (2002).
16. Ley Nº. 1.160/97, Delitos Informáticos, Paraguay, Artículos (144, 146, 173, 174, 175, 188, 189, 220). (1997).

En Paraguay apreciamos como desde hace ya varios años, se realizo una compleja legislación en materia de los delitos informáticos, abarcando gran cantidad de conductas delictivas como ser la de Pornografía Infantil, y las Operaciones Fraudulentas, (estafas, con compras, tarjetas de crédito, debito, falsificaciones de las mismas etc.), que servirán para otros Estados de ejemplo para adecuar a sus legislaciones.

Para destacar de la presente Ley Paraguaya, quiero citar el Artículo 188°, el cual incorpora una tipificación específica llamada "Operaciones fraudulentas por computadora". En este punto hace referencia al procesamiento de datos de un ajeno, con el objeto de obtener un beneficio patrimonial. En otras palabras, lo podemos interpretar como las acciones de falsificación de programas o software, la utilización de datos falsos o incompletos, o la utilización de datos indebida.[17]

Por otro lado, vemos como la LEY N° 2861/2006, trata de forma completa la pornografía infantil, donde castiga la exhibición, la reproducción, difusión. Pero quiero mencionar que el Artículo 6º, tipifica la posesión de pornografía infantil y el consumo de la misma. Dando una protección extrema a los niños ante este delito.[18]

Ley 12.737 Delitos Informáticos, Brasil.

La presente Ley resulta de actual vigencia, sancionada en el año 2012, donde mediante una actualización, dispone la tipificación criminal de los delitos informáticos. Uno de los Artículos más importantes es el 154 A. el cual tipifica las conductas de adulteración, destrucción de datos, la instalación de virus, o programas con el objeto de vulnerar la seguridad de un sistema informático. Por otro lado, también hace mención a la venta y distribución, o disposición de los dispositivos que estén fabricados a los fines de vulnerar un sistema informático.

17. Ley Nº. 1.160/97, Delitos Informáticos, Paraguay, (1997). Artículo 188, inc. 1, 2, 3, 4.
18. Ley N° 2861/06,Represión el comercio y la difusión comercial o no comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces (2006).

En sus párrafos, encontramos también tipificaciones de la violación o interceptación de las comunicaciones privadas, y como novedoso, hace mención al control de dispositivos a distancia, con un agravante de la divulgación o comercialización de esa información obtenida si es una persona del alto mando del Estado.

El Artículo 266, fue modificado para aprehender de forma inmediata quien realice una interrupción o perturbación de servicio telemático o informático, como también a aquel que impida su restablecimiento.

Por último, en el Artículo 298, encontramos como se equipara a calificación de documento particular a las tarjetas de crédito o debito, protegiendo de esta forma los datos personales que la misma tiene.

En Brasil encontramos, la complementación legislativa con la Ley 11.829, la cual presenta una regulación del Estatuto de la Niñez y la Adolescencia. Esta ley tiene por objeto brindar protección jurídica más eficaz a los niños quienes son víctimas de la pornográfica infantil, através de la producción, venta y distribución. No puedo dejar de mencionar que se tipifican las conductas de la adquisición, posesión del material pornográfico infantil. [19]

Ley 1.768, Delitos Informáticos, Bolivia.

En el Código Penal de Bolivia, aparece con la reforma mediante la Ley 1.768 la cual realiza una reforma en gran parte del Código, pero atento a la temática que nos incumbe, nos enfocaremos en el Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el cual refiere a los Delitos Informáticos.

En esta reforma encontramos una escasa legislación en esta temática, incorporando solo dos Artículos, el 363 bis, titulado manipulación informática, el cual trata las intenciones de obtener de forma indebida un beneficio para sí o un tercero. También menciona la manipulación del procesamiento o transferencias de datos (internet) que tenga como fin una actividad incorrecta, como para citar un ejemplo una transferencia de dinero a una cuenta falsa.

19. Ley 11.829, Delitos Informáticos, Brasil. (2008).

Luego en el Artículo 363 ter. encontramos las conductas que sin autorización se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

En este apartado, vemos lo escaso y lo apropiado que puede ser el país vecino victima de delitos informáticos, atento a que no tipifica con especificad la problemática de los delitos informáticos, encontrándose tanto los ciudadanos, como el Estado vulnerable ante los ciberdelincuentes. [20]

Ley 27309, Delitos Informáticos. Perú.

La Ley 27309 incorpora al Código Penal del Perú, los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, introduciendo allí los artículos 207, A, el cual refiere a la utilización e ingreso indebido de una base de datos, o sistemas de red de computadoras, con la finalidad de alterar, ejecutar, interferir, interceptar, copiar información en tránsito (internet), o que se encuentre en la base de datos.

Por otro lado, en el Artículo 207, B, encontramos la tipificación de daños o destrucción.

En otro orden, la Ley 28.251, mediante su actualización se incorporó los delitos contra la integridad sexual, referida a la pornografía infantil, a través de la modificación del art 183-A.

Por último, encontramos en la Ley 28.493 de, año 2005, la cual tiene por objeto la regulación de la utilización de los correos electrónicos, más específicamente los de spam, o los correos no deseados.

Observamos como en Perú, incorpora a su cuerpo legislativo la regulación de los correos electrónicos, que hasta el momento aún no se han presentado en los países ya citados.[21]

20. Ley 1.768, Delitos Informáticos, Bolivia. (1997). Artículos el 363 bis y Articulo 363 ter.-

21. Ley 27309, Delitos Informáticos. Perú. (2005).

Ley Nº 53-07 2007. República Dominica, Delitos Informáticos.

La Ley nº 53-07, que trata sobre crímenes y delitos de alta tecnología, sancionada en el año 2007, en República Dominicana. Ley que ejemplifica y ha utilizado los términos en materia de derecho Penal y Procesal del Convenio de Budapest, pero también ha agregado en su legislación objetividad sobre las conductas de los ciberdelincuentes.

Está en una Ley se creó con el fin de brindar dar protección a de los usuarios, las bases de datos y las transferencia de datos. La misma en sus párrafos nos menciona los fundamentos de su proyección, como ser el alto desarrollo tecnológico, crea nuevas modalidades delictivas que no se encuentran tipificadas, también que al no estar tipificadas estas conductas, las mismas otorgan un vacío legal a los infractores haciéndolos inimputable.

Por otro lado, nos muestra el interés internacional que existe ante esta nueva forma de cometer delitos y como descansan los fundamentos de su creación en bases jurídicas internacionales.[22]

Articulo 4 y destacados

El Artículo 4 de la presente Ley, con una introducción de conceptos de componentes que integran la tecnología se va sumergiendo en la materia de los delitos informáticos y así poder tener una clara interpretación de la Ley al finalizar la lectura de la misma, haciendo que una persona que no sea idónea en materia informática, pueda comprender las conductas ilícitas que se presentan. Por ello, nos menciona definiciones de computadora, código malicioso, datos, dispositivo, dispositivo de acceso, documento digital, red informática, sistema de información, sistema electrónico, sistema informático, criptografía, sistema de telecomunicaciones, sistema telemático; para luego pasar por las acciones posibles que se pueden desarrollar mediante la informática, como por ejemplo, clonación, acceso ilícito, afectar, delito de alta tecnología, desvió de facili-

22. Ley Nº 53-07. Delitos Informáticos. República Dominicana (2007).

-dades contratadas, desvió de servicios, interceptación, pornografía infantil, señal de disparo, sin autorización, transferencia electrónica de fondos, y por último a los individuos, sujeto activo, sujeto pasivo y usuario.

Este artículo destaca la presente en todo Sudamérica, por el motivo de una breve descripción de cada uno de los elementos, como así también las conductas posibles que se realizan mediante el uso de la tecnología.

Para continuar con la descripción de las figuras legales con sus respectivas sanciones, podemos indicar que la presente, tiene una variedad generosa en especificación de las conductas típicas a que en muchos otros Estados no lo es, el capítulo I, el cual se titula como Crímenes y Delito contra la Confidencialidad, Integridad y Disponibilidad de datos y sistema de información, mantiene un formato de descripción de conductas típicas similares a las del resto del mundo como Acceso Ilícito, Códigos de Accesos, Uso de Datos por Acceso Ilícito, Clonación de Dispositivos de Acceso, Acceso Ilícito para Servicios de Terceros, Explotación Ilegitima de Acceso Inintencional, dispositivos fraudulentos, Interceptación e Intervención de Datos o Señales, Beneficios de Actividades de un Tercero, Sabotaje, Daño o Alteración de Datos.

En el Capítulo II, menciona las figuras legales de Atentado contra la vida de la persona, robo mediante la utilización de Alta tecnología, obtención ilícita de fondos, chantaje, robo de identidad, uso de equipos para la invasión de la intimidad, difamación, atentado sexual.

Pero en el capítulo V, encontramos las figuras legales de los crímenes, delitos contra la nación y actos de terrorismo. Por otro lado, se establece la creación de Organismos Judiciales y de las fuerzas de seguridad con los fines de combatir el delito informático, como también de prevenirlo y como función más importante es la de velar por la actualización de la Ley, cuando los motivos se justifiquen.

Es por ello, que la Ley 53-07, ha sido creada por los legisladores con conocimientos profundos en materia de delitos informáticos, haciendo de esta una de las Leyes más complejas, por su redacción de las conductas típicas, como sus de sus conceptos, pero también de la fácil comprensión de las mismas destacándose notoriamente de el resto del mundo.[23]

23. Ley Nº 53-07, Delitos Informáticos. (2007).Articulo 4, República Dominicana.

Por otro lado en la presente Ley encontramos como se crean y confeccionan las unidades específicas de investigaciones de delitos informáticos. Haciendo a mí entender una Ley ejemplar y de creación a conciencia de la problemática existente.

Iniciando por el Artículo 36, en el cual Puerto Rico, mediante fuerza de Ley crea un Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología, bajo las siglas DICAT. La cual tiene la función específica de combatir los delitos cometidos mediante las nuevas tecnologías, también realizado tareas de prevención, y la posterior investigación. Conformada en su totalidad por personal altamente capacitado, partiendo de la base de juristas y efectivos de las fuerzas de seguridad.

En su artículo 37, nos indica como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología, prestará apoyo a la justicia ante las investigaciones.

Por último en el Artículo 38 una de las funciones principales del Departamento de Investigación de Crímenes y Delitos de Alta Tecnología, es la de velar por el buen funcionamiento y ejecución de las disposiciones de la presente Ley. También se encarga de la investigación de cada una de las denuncias recibidas en materia de delitos informáticos. Y por otro lado, el Departamento descansando en el espíritu de la Ley, deberá contar con el personal especifico en la materia de delitos informáticos, velando por el correcto entrenamiento del personal de la unidad de investigación.

En el Artículo 43, se crea una División temática, siendo la de Investigaciones de Delitos Informáticos identificada por sus siglas como D.I.D.I. Esta División se encargará de la investigación de los delitos relacionados a los crímenes contra la humanidad.

Artículo 44.- Investigación y Sometimiento. La División de Investigación de Delitos Informáticos (DIDI) trabajará los casos relacionados a: crímenes contra la humanidad; crímenes, delitos contra la Nación, el Estado y la paz pública; amenazas o ataques contra el Estado dominicano, la seguridad nacional o que involucren la figura del presidente de la República, secretarios de Estado o funcionarios electos.

Dentro de sus funciones que se encuadran en el Artículo 45, será la de velar por las disposiciones de la presente Ley, investigar las denuncias de crímenes o delitos considerados de alta tecnología; responder con capacidad investigativa a todas las amenazas y ataques al Estado. También por otro lado, deberá desarrollar análisis ante

las amenazas informáticas y velar por el correcto entrenamiento y capacitación del personal.

Esta legislación presenta un gran interés e importancia en la formación de una institución especifica, con personal idóneo en delitos de alta tecnología, por ello es de destacar como los legisladores han confeccionado esta Ley, pudiendo someterse a modo de ejemplificación para ser aplicable en la República Argentina.

➢ Capítulo 3: La Legislación vigente Argentina.

En el presente capítulo, recorreremos la legislación en materia de los delitos informáticos en la República Argentina, con la finalidad de tener una noción de las Leyes que existen y que tipo de conductas delictivas tipifican. A continuación se detallan las siguientes:

I. Ley 26.388. Delitos Informáticos.

En la Argentina con la aparición de las nuevas conductas delictivas donde intervenía la utilización de la tecnología se encontraba en un vacío legal dentro del Derecho Penal, lo cual hacía imposible tener una sanción. También en este tipo de conductas delictivas se observaba la intervención del Derecho Constitucional, ya que una conducta ilícita violaba los principios de Privacidad de las personas.

La Ley fue sancionada en el Año 2008, actualizando algunos artículos en el Código Penal, tipificando conductas relacionadas a los delitos informáticos.

La misma ha agregado artículos, como así también ha modificado los que se encontraban ya incorporados en el Código Penal argentino en el año 2008. Para hacer un repaso de los puntos que trasluce esta Ley podemos decir que son los siguientes:

- Tenencia con fines de distribución por Internet; u otros medios electrónicos de pornografía infantil
- Violación, apoderamiento y desvío de comunicación electrónica;
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones;
- Interrupción de las comunicaciones electrónicas
- 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. Bendinelli M. (2014).

Uno de los Artículos más importantes y que es tema de actualidad, respecto a los menores de edad y su protección de la integridad sexual de los mismos ante la exposición y uso de internet. Estas conductas inocentes por menores de edad, se adjudican ante la vulnerabilidad, manipulación de los terceros que intervienen en el intercambio de información entre ellos. [24]

Por ello, y descansando los fundamentos de su creación tomando fundamentos jurídicos emanados por el Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.

Donde asiste un crecimiento de las apariciones de pornografía infantil dentro de los sitios de internet, donde pretende sanciona toda producción, distribución, importación, exportación y transmisión, posesión intencional y propaganda que refiera a la temática mencionada, para en complemento con los Estados para la prevención. U.N.I.C.E.F. (2006). *Protocolo facultativo de la Convención sobre los Derechos del Niño*. Argentina.

Bendinelli M. (2014). Delitos informáticos. *La importancia de la prueba digital en el proceso judicial.* (1-1). Recuperado de: http://aldiaargentina.microjuris.com/2014/12/03/delitos-informaticos-la-importancia-de-la-prueba-digital-en-el-proceso-judicial/

24. Ley 26.388 Ley de Delitos Informáticos. Argentina. (2008).

El reflejo de lo mencionado en la presente Ley, es el Artículo 128 el cual nos dice, "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".

Otras de las modificaciones ha sido en razón a la utilización de la internet, la creación de cuentas de correos, como así también cuentas personales, laborales, y de distinto índole, donde se brinda protección jurídica contra el acceso ilegitimo y cualquier otro tipo desviación de la información hacia otra cuenta.

El presente Artículo 153 se presenta como, "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".

Para continuar, nos dirigimos hacia la protección de las bases de datos, sean estatales o privadas, donde las personas que aportan cierta información debe prestar su conformidad. No obstante ello, la presente Ley, otorga protección jurídica frente al acceso ilegitimo de las bases de datos, como así también, la difusión de la información o la inserción de datos que modifiquen información de las bases de datos sin consentimiento.

El Artículo 157 bis, "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", este artículo ya fue incorporado por la Ley 25.326 de Protección de Datos Personales, pero sufrió sus modificaciones por la Ley 26.388) el artículo, 173 inc. 16, nos demuestra la regulación mediante la defraudación, o técnicas de manipulación de los sistemas informáticos, el mismo dice,

“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”.

Para ir concluyendo me remito a citar el Artículo 183, en su segundo párrafo, brinda protección jurídica atento a la alteración, destrucción, y que ello, genere un daño. El mismo reza, “…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 delito con las nuevas tecnologías ha generado una problemática procesal investigativa, donde sus principales defectos los encontramos en la falta de conocimiento, de capacitación, de personal idóneos en la materia, hacen que fuere conflictivo aplicar la ley.

La tecnología ha presentado inconvenientes legales, tales como si un teléfono celular, debe ser tenido en cuenta como tal o tiene que ser considerado una computadora, donde aparecen garantías constitucionales que protegen nuestros Derechos, como ser el de la intimidad o privacidad entre otros y debe ser analizado por los juristas de una manera precisa para que pueda ser efectiva.

Esta Ley no es una ley especial, solo se encarga de modificar, sustituir e incorporar figuras típicas al Código Penal que se encuentra actualmente en vigencia, y que tiene como fin único regular las conductas desarrolladas en consecuencia del uso de las nuevas tecnologías como medios para la comisión de delitos.

Las penas que presenta la Ley 26.388, corresponde a prisión, inhabilitación y multa.

Podemos mencionar como punto importante en la presente, el Artículo 10 que incorpora al Artículo 183 del Código Penal de la Nación, el siguiente texto, “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”.

Ahora bien pero para interpretarlo mejor tenemos que citar el Artículo 183 del Código Penal de la Nación que tipifica el delito de daño en general, donde los posibles daños corresponden a las cosas materiales, ahora bien que sucede cuando se daña un

software, este artículo no podría encuadrar tal conducta, de igual manera sucede si se dañan los datos que se encuentran en las bases de datos. En estas circunstancias quedaríamos frente a un vacío legal que en la actualidad encontramos bases de datos en cualquier ámbito de la vida cotidiana, sean comercios, bancos, aseguradoras, etc.

Para mantener una mejor ilustración de lo mencionado sobre este Artículo, a continuación se cita el presente que reza lo siguiente "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".

Ante la normativa descripta que corresponde al daño, mediante la incorporación de la Ley 26.388, amplia a la figura legal, hacia los caminos de las nuevas tecnologías, donde tenemos un amplio espectro de conductas que se desarrollan con la finalidad del daño informático.

Por último, podemos mencionar que el texto del Código Penal de la Nación sufrió un amplio cambio en sus líneas quedando redactado de la siguiente manera "Se impondrá prisión de un mes a dos años, al que, por cualquier medio, destruyere en todo o en parte, borrare, alterare en forma temporal o permanente, o de cualquier manera impidiere la utilización de datos o programas, cualquiera sea el soporte en que estén contenidos durante un proceso de comunicación electrónica. La misma pena se aplicará a quien vendiere, distribuyere o de cualquier manera hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños de los descriptos en el párrafo anterior, en los programas de computación o en los datos contenidos en cualquier tipo de sistema informático y de telecomunicaciones". Artículo 183 del Código Penal de la Nación.

En el presente se encuentra una redacción solemne que trae aparejados confusiones donde pudiera interpretarse que el delitos de daño informático, se estaría cometiendo siempre que alguien introduzca algún tipo de software o programa en un sistema informático, o también en otro programa que pudiera traer aparejado consecuencias potenciales de conflictos para las personas ideales que comercializan software, aquí encontramos una contradicción donde el Artículo 11 el cual reza "las partes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores

en relación con el ejercicio de sus derechos en virtud del presente Tratado o del Convenio de Viena y que, respecto de sus obras, restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la Ley", Artículo 5 del Tratado de la OMPI sobre Derechos de Autor de 1996, vigente desde el 06/03/2002, y aprobado por Argentina en 1999.

También ante estas consecuencias puedo mencionar un Dictamen de la Cámara de Senadores, ante el Artículo 153, que nos dice el elemento normativo incorporado al tipo "Con respecto al actual artículo 153 del Código Penal, última parte del primer párrafo …suprimiere o desviare de su destino una correspondencia que no le esté dirigida.

Es de menester la presente valoración de la Cámara ya que la propuesta de origen de incorporar la expresión indebidamente en la figura legal, con el objeto de que no queden dudas para la persona deba interpretar con respecto a requerir la finalidad de la responsabilidad dolosa del autor del delito.

La importancia de la ley sancionada nos muestra un gran avance en materia de los delitos informáticos, siendo una actualización única para el Código Penal de la Nación, rigiendo en materia de penal los principios de legalidad, donde una conducta no ilícita si no se está expresamente tipificada en el cuerpo normativo. Quedando prohibida las acciones de la analogía, donde no se puede sancionar una conducta que no se encuentra tipificada, con otra similar. Ante estas circunstancias se hacen imprescindible la sanción de la presente Ley, donde precisa conductas típicas, donde acompaña la evolución de la tecnología, si bien aún queda mucho mas por hacer, es un buen comienzo, pero que no debe quedar estacionado en el tiempo, ya que la tecnología se renueva constantemente y hoy el mundo se caracteriza por ser de una sociedad tecnológica.

Resumiendo la Ley 26.388, se redactó ante los grandes inconvenientes jurídicos que se suscitaban y las victimas que se encontraban en desprotección jurídica, pudiendo decir en principio que ya están resueltas, como así también de concretar compromisos internacionales asumidos por nuestro país.

En algunas oportunidades la justicia penal ha resueltos casos de ilicitud a partir de la adopción de figuras típicas penales existentes. Algunos casos sometidos a la justicia penal han sido resueltos favorablemente a partir de la adopción de figuras

penales existentes. A partir de ahora, tanto las personas físicas, como las personas de existencia ideal, deberán tomar todas las medidas de seguridad necesarias para no comprometer los bienes jurídicos, tanto como la responsabilidad o imagen en la comisión de delitos sobre los que, hasta el día de hoy la jurisprudencia Argentina se había pronunciado, pero que a partir de esta Ley la justicia podrá sancionar las conductas típicas con fundamentos legales específicos.

Habiendo comentado la Ley 26.388, no puedo dejar de mencionar la importancia del apoyo de la Convención de Budapest, siendo desarrollado el Convenio sobre ciberdelincuencia. En este acontecimiento la República Argentina, se adhirió luego de presentar la Ley 26.388, donde fue analizada por los especialistas de la Convención, siendo aceptada y en consecuencia se firmó la aceptación y adhesión de la Argentina al presente Convenio. [25]

A los fines de interpretar la jurisprudencia Argentina respecto a la materia de los delitos informáticos, si bien resulta escasa en la actualidad, podemos citar casos donde observamos cómo interactúan las leyes vigentes en un proceso judicial, donde encontramos incidentes procesales, resultantes de la aplicación de las leyes que se encuentran vigentes, resultan obsoletas, no encuadrando la figura legal como debería. Es por ello, que la Ley 26.388, se presenta como una solución a estos inconvenientes legales.

En un primer caso, observamos como la legislación actual se aplica, y en consecuencia nos encontramos con un incidente de nulidad por el mal menester por parte de una de los actores, violando garantías constitucionales consecuencia del desconocimiento y la manipulación de la tecnología. Ver sentencia de la Sala II del Tribunal Constitucional de España (Sentencia 173/2011, del 7/11/11) y Fallo del Juzgado de Instrucción Penal N° 49 "Camus Hacker".

Es por ello, que con los fines de mantener la actualización de la Ley 26.388, se confeccionó un Proyecto de Ley en el año 2014, donde se cuestionaron la mayor parte los errores, o lagunas legales que se presentaban dentro del Código Penal de la Nación, ante la presencia de un delito informático, que daban origen a nulidades o se encontraban con ausencias de fundamentos para redactas un auto de imputación.

25. Convención de Budapest. (2001).

En este Proyecto de Ley, que pretende actualizar e insertar nuevas figuras legales se fundamentaba en la solución otorgada a los problemas del ejercicio de la acción penal, que no cumplimentaba con la tipificación posible, y que tampoco fue lo suficientemente completa y abarcativa ante la legitimidad de los bancos de datos personales. También es de destacar el problema de la falsificación de instrumentos públicos digitales, donde la ley 26.388, nunca fundamentó las posibles consecuencias ante la presencia de una falsificación de una orden de allanamiento digital. En este Anteproyecto que aún continua en discusión, sería un gran aporte a la conformidad de los delitos informáticos.

Para la conformación de los Proyectos de Ley de sancionó el Decreto 678/12 donde el mismo pretende organizar mediante un organigrama de funcionarios que participen en los distintos acontecimientos que sea menester. En consecuencia se crea la Comisión para la Elaboración del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación. Atento a que el Código de la Nación su estructura y lineamientos principales fueron confeccionados en el año 1921, lo cual merece tener un tratamiento por profesionales a los fines de lograr una armoniosa actualización en materia de conductas ilícitas, acompañado del desarrollo de las nuevas tecnologías.

II. Ley 25.326 Protección de Datos Personales.

En la República Argentina comenzó a tener vigencia como novedosa la Ley 25.326 la cual en principio se basa en el Convenio de Budapest. Aquí el legislador pretende brindar protección de los datos personales de las personas que se encuentran en bases de datos, o cualquier otro destino del cual la información sea automática, ya sea en entidades públicas o privadas. Uno de los Derechos que se pretende resguardar es el Honor y la Intimidad.

Su contenido se inicia con conceptos de los que son los datos y bases de datos en general, pasando por el usuario y el titular de esos datos. Luego continuamos con disposiciones que tiene el titular sobre esos datos almacenados en una base, y a su vez quien es administrador o titular de la base de datos. Por último, hace mención de los Derechos que tiene un titular de los datos.

Donde esta Ley nos indica que brinda protección sobre los datos de los individuos que aportan por motivos de contratos laborales o de distinta índole en la vida cotidiana, los cuales se transforman en bases de datos. A partir de la implementación de la presente Ley, encontramos la protección de los datos aportados por las personas de acuerdo a cada una de las circunstancias particulares.

En su contenido podemos observar la regulación de los "datos informatizados", "archivos o banco de datos", "datos de usuarios", (Ley 25.326 de Protección de Datos Personales, 2000) como para destacar. Aquí la tecnología ha encontrado en su evolución tecnológica los vacios legales respecto a las bases de datos, que llevan a la vulneración de los mismos. Esta Ley se presenta en razón de brindar seguridad a aquellas personas físicas o jurídicas que aportan sus datos al realizar cualquier tipo de contrato, donde los datos descansan en bases de datos informatizadas; resguardando así los principios de la Intimidad, el Principió al Honor etc.

Atento al contenido de la misma, se destacan algunos Artículos de mi interés para indicar la presencia de las actualizaciones legislativas que evocan a la presente, como ser el Artículo 2, el cual contiene algunas definiciones que complementan a la Ley 26.388, partiendo del inicio de los Datos Personales, donde entiende que será toda información de cualquier índole correspondientes a personas físicas o jurídicas. Luego tenemos que una sub definición que corresponde a los Datos Sensibles, donde la Ley expresa que son los datos de índole personal, como ser filiatorios, historias clínicas o de referencia sexual.

Una definición destacables es la de Archivo, registro, base o banco de datos, aquí nos sitiamos ya en la parte técnica del cuerpo tecnológico, donde indica a una serie de sistemas de ordenamiento de información de los datos personales. Otras de las definiciones corresponde al Tratamiento de datos, el cual resulta de las operaciones y procedimientos sistemáticos, pudiendo ser electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relaciona-miento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias y por último, para concluir con la parte física de las nuevas tecnologías, encontramos a los Datos informatizados, que son aquellos datos que se utilizan para el tratamiento electrónico o automatizado.

Por otro lado, encontramos dentro de las definiciones del presente Artículo, las responsabilidades de las personas físicas o jurídicas titulares de las bases de datos, ya sean en el ámbito privado o público.[26] Luego tenemos al titular de los datos, que como antes mencionamos solo deben contener dentro de su identificación un domicilio legal o delegaciones, sucursales en el territorio nacional. Por último, la Ley individualiza al usuario de los datos, entendiéndolo como toda persona pública o privada, que realice tratamientos de datos.

En el Artículo 3 hace mención al los tipos de datos que representan a licitud mientas se encuentren debidamente inscriptos. [27]

El Artículo siguiente nos representa en la calidad de los datos donde estos hacen referencia a la veracidad de los datos inscriptos, y la finalidad de dichas inscripciones, también menciona la recolección de datos mediantes medios legales sin la comisión de fraudes o conductas contrarias a la ley. Estos datos deben ser puntuales, específicos, sin lugar a ambigüedades y en caso de ser necesarios deben ser actualizados.

Ante la inconsistencia de alguna de las anomalías detectadas, los datos deberán ser suprimidos, sustituidos, o completados por el responsable de la base de datos cuando detecte la anomalía, teniendo siempre en cuenta los Derechos del titular establecidos en la presente Ley en su Artículo 16. También el titular de los datos podrá tener acceso a los datos insertados en una base de datos, y el caso de que estos datos dejen de cumplir una función específica deberá ser destruido. [28]

Atento a lo antes expuesto, uno de los Derechos principales que menciona la presente, refiere a que toda persona puede solicitar al organismo de control relativo a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita. [29]

Los datos ingresados en las bases de datos, tienen que ser protegidos ya sea por la legislación, y a su vez se debe tener en cuenta las medidas de seguridad físicas que prometen un resguardo ante la posible violación los Derechos de los titulares de aportan dicha información.

26. Ley 25.326 Ley de Protección de Datos Personales. (2000).Argentina, Artículo 2.
27. Ley 25.326 Ley de Protección de Datos Personales. . (2000).Argentina. Artículo 16.
28. Ley 25.326 Ley de Protección de Datos Personales. (2000).Argentina. Artículo 26.
29. Ley 25.326 Ley de Protección de Datos Personales. (2000).Argentina. Artículo 9.

Como ser el responsable o usuario del archivo de datos tendrá que adoptar medidas físicas técnicas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Los datos podrán ser de conocimiento y transferencia ante un requerimiento judicial fundado, donde el responsable deberá prestar colaboración con el aporte de los mismos. También existe la transferencia de datos cuando por ejemplo se presentan ante un tratamiento médico de un afectado, o de un investigado ante una epidemia, siempre y cuando teniendo en cuenta lo escrito en la presente Ley.

Las transferencias podrán realizarse siempre y cuando se encuentren de acuerdo a la Ley, como ser las entidades bancarias y transferencias de carácter internacional, ante la cooperación entre estados donde tiene como objeto el combate del crimen organizado, el terrorismo y el narcotráfico.

La Ley ha tenido en cuenta al titular de los datos personales que se encuentran en las bases de datos, dándole protección como así también, derechos sobre los mismos, con la capacidad de disponer de los datos a criterio de cada titular. Por eso dedica un artículo extenso a tales fines, como ser el titular habiéndose acreditado correctamente tiene derecho de solicitar y obtener la información que se encuentra en las bases de datos, sean públicos y privados.

En consecuencia el responsable de la administración de esos datos tiene la obligación de informar al titular dentro de los 10 días la información solicitada, concluido el tiempo mencionado la Ley interactúa ante la protección de datos personales o de habeas data prevista. En sus últimas líneas del Artículo hace referencia a los titulares de los datos en caso de fallecimiento donde la Ley lo resuelve de forma clara, sin vericuetos siendo los sucesores universales los que continúan ejerciendo el Derecho legítimos del titular.

Respecto a las sanciones penales, la presente Ley incorpora penas que van desde un mes a dos de prisión al que insertara datos falsos en una base de datos. También la pena aumenta ante la presencia de aquel que proporcione a un tercero a sabiendas información falsa para ser insertada en una base de datos.

Cuando el hecho incurre en un perjuicio a la persona la pena aumentará a la mitad del mínimo y del máximo. Por último, cuando la intervención en un hecho delictivo descripto por la presente Ley, sea de un funcionario público en ejercicio de sus funciones se aplicará la accesoria de inhabilitación para sus cargos por el tiempo de la condena.

Por otro lado se incorpora al Código Penal de la Nación, la pena de un mes a dos años de prisión a quien a sabiendas e ilegítimamente o violando sistemas de seguridad respecto a las bases de datos. También quien revelare información registrada en una base de datos, teniendo la misma pena si incurre un funcionario público en ejercicio de sus funciones, con inhabilitación de 1 a 4 años en su cargo.

A modo de comentario, se puede mantener que la Ley de Protección de Datos Personales, ha confeccionado una regulación de posibles conductas ilícitas como así también, derechos de los titulares de los datos. Siendo una redacción clara y completa en relación a los aportes de datos, en cualquier ámbito de la vida cotidiana, donde sin conocer a quienes se los otorgamos de igual manera existe una Ley clara que nos brinda protección sobre la información personal que brindamos. Ver fallo, Tanus Gustavo Daniel c/ Cosa Carlos Alberto y otros/ Habeas Data (art. 43 C.N.).

Esta Ley pretende brindar protección a los datos personales que se encuentran en archivos, registros, bases de datos, u otros medios técnicos de almacenamiento de datos, pudiendo ser públicos o privados donde se deberá garantizar la no violación del derecho al honor y a la intimidad de las personas.

V. Ley 26.904, Groming, o Ciberhostigamiento.

Por otro lado, la utilización de las nuevas tecnologías donde se vieron agraviados los Derechos de las personas, provocando una vulnerabilidad mayor cuando interactúan menores de edad con los elementos electrónicos y el uso de las comunicaciones mediante el uso de la internet.

La palabra, groom en el vocablo inglés hace referencia a preparación o acicalamiento de algo, también las conductas definidas como la pedofilia, el término groom inmediatamente se asocia con acciones que tienen como fin socavar la moral o psicológicamente de un menor de edad a los fines de obtener el control emocional, para luego concluir con el acto sexual. Motivo por el cual, dió origen a delitos que aún

habían sido tipificado en la Argentina, pero si en el mundo eran reconocidos como Grooming.

En este tipo de actividades llamada en Argentina como Ciber acoso, esta figura legal se manifiesta mediante acciones por parte de un adulto, con la finalidad de generar una confianza en la persona menor de edad, aprovechándose de la inocencia, y la inexperiencia del menor. El objetivo de esta actividad es la de lograr un intercambio de información, donde aparecen las extorsiones, para obtener por último un acercamiento de índole sexual.

Según UNICEF, indica que "es toda acción deliberada de un adulto de acosar sexualmente a un niño o niña mediante el uso de Internet.[30]

Según la O.N.G Argentina Cibersegura, quien ha impulsado la sanción de la presente, define al Grooming como el Ciberhostigamiento, siendo acciones deliberadamente emprendidas por un mayor de edad con el objeto de lograr la amistad de un menor de edad, con el fin de disminuir las inhibiciones del niño e incentivarlo para que realice conductas de índole sexual. O.N.G. (2013). Argentina Cibersegura, *Ley de Grooming* (1-1). Recuperado de: https://www.argentinacibersegura.org/leygroomingya/

Habiendo mencionado algunos conceptos de las más importantes y prestigiosas Organizaciones, podemos acotar que el Grooming, transmite estas inquietudes a la sociedad, donde los locales que brindaban acceso a internet (ciber), carecían de regulación sobre el ingreso y el servicio que prestaban, no existiendo ningún tipo de control sobre el acceso de los menores de edad y las acciones que realizaban en el mismo, pudiendo ingresar a sitios web prohibidos en otros países del mundo o los chats, donde provocaba una vulnerabilidad hacia la integridad física como psicológica de los mismos.

En consecuencia, es ejemplificadora la Ley en la Ciudad Autónoma de Buenos Aires, que se llevó a cabo la sanción de una Ley específica que regulara el acceso de los menores de edad y el uso de internet dentro de los comercios habilitados a tal fin, restringiendo determinados portales de internet.

30. Convención Sobre Los Derechos Del Niño, UNICEF. (2006).

En el Artículo 1º se indica que "Los establecimientos comerciales que, en el ámbito de la Ciudad Autónoma de Buenos Aires, brinden acceso a Internet, deben instalar y activar en todas las computadoras que se encuentren a disposición del público, filtros de contenido sobre páginas pornográficas."[31]

También la presente otorga facultades al titular del local comercial, de restringir el acceso a determinados sitios de internet prohibidos por la Ley, a través de filtro. Y por último hace mención a las sanciones que le corresponde al titular del local ante el incumplimiento de la presente Ley. [32]

La utilización de las nuevas tecnologías donde se vieron agraviados los Derechos de las personas, provocando así una vulnerabilidad mayor cuando interactúan menores de edad, con los elementos electrónicos y el uso de las comunicaciones mediante el uso de la internet.

Motivo por el cual, dió origen a delitos que aun habían sido tipificado en la Argentina, pero si en el mundo eran reconocidos como Grooming. En este tipo de actividades llamada en Argentina como Ciber acoso, esta figura legal se manifiesta mediante acciones por parte de un adulto, con la finalidad de generar una confianza en la persona menor de edad, aprovechándose de la inocencia, y la inexperiencia del menor. El objetivo de esta actividad es la de lograr un intercambio de información, donde aparecen las extorsiones, para obtener por último una acercamiento de índole sexual.

En el delito de grooming podemos describir las etapas de contemplación del delito, donde todo se inicia con el lazo de amistad, donde el menor de edad engañado por posibles falsas personalidades, que podrían ser niños o niñas manteniendo contactos esporádicos, para luego ir aumentando de a poco con el tiempo a los fines ir obteniendo la confianza y el manejo psicológico del menor.

31. Ley 863, Artículo 1, Ley de Establecimiento Comerciales. (2003).
32. Ley 863, Artículo 2-3, Ley de Establecimiento Comerciales. (2003).

Luego de haber ganado la confianza suficiente, donde el ciber delincuente ya en estos momentos ha obtenido gran cantidad de información personal del menor como así también de su familia, prepara al menor de edad para pasar a la etapa de afectación, siendo esta una etapa donde consiste en seducir al menor mediante diálogos de índole sexual.

Por último, se llega a la etapa de la extorsión donde el menor por miedo a contar lo sucedido, y habiendo sido manipulado mentalmente por el ciber delincuente, intenta obtener pornografía infantil, y en su defecto poder tener el contacto físico.

El análisis de la conducta típica que prohíbe, ante la sanción de una pena por el hecho de contactar menores de edad a través de medios electrónicos, como ser computadoras o cualquier elemento que contemple las nuevas tecnologías, con el objeto de trasgredir la integridad sexual.

Habiendo mencionado una breve introducción al delito del grooming, o ciber acoso, se transmite todas estas inquietudes a la sociedad, donde carecían de regularidad los locales que brindaban acceso a internet, como ser los ciber, donde no existía ningún tipo de control sobre los accesos a la pornografía, provocando así una vulnerabilidad hacia los menores que se hacían presentes en los locales comerciales.

Esto llevo a que se sancione una Ley específica que regulara el acceso de los menores de edad y el uso de internet, donde se restringen determinados portales de internet, el mismo nos indica "Artículo 1º Los establecimientos comerciales que, en el ámbito de la Ciudad Autónoma de Buenos Aires, brinden acceso a Internet, deben instalar y activar en todas las computadoras que se encuentren a disposición del público, filtros de contenido sobre páginas pornográficas", (Ley 863. 2003).

En consecuencia se la cual incorpora la siguiente figura legal al Código Penal de la Nación, "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".

Para poder mencionar la legislación comparada del Código Penal de Chile donde regula las conductas típicas a través del artículo 366 quater, donde encontramos una gran diferencia ante la legislación Argentina.[33]

33. Código Penal de Chile, Artículo 366 quater.

El presente Artículo tipifica la conducta, que se realice por intermedio de cualquier medio electrónico. Respecto a las sanciones vemos que son más severas y especificando varias conductas en relación al grooming.

En sus puntos mencionan:

- Quien para procurar excitación sexual realiza acciones de significado sexual ante un menor de 14 años, lo hace ver o escuchar pornografía.
- Quien, para el mismo fin, determina al menor a realizar tales acciones.
- Quien lo hace con un menor de más de 14 años mediante amenazas.

También, la Ley prevé que las sanciones que se aplican aún así, si se comenten a distancia, a través del uso de cualquier elemento que se integre las nuevas tecnologías, de esta manera la Ley entiende que no es necesario el contacto físico con el menor de edad, sino que con el solo hecho de mantener una conversación sin importar la distancia que los separe, atento a las fases antes mencionadas, esta conducta se encuentra tipificada claramente en la Ley Chilena. Por último, la legislación se convierte en más gravosa aun, cuando existe la falsedad de identidad, o los falsos datos aportados a la víctima.

También destaca la presente la edad de 14 años para diferenciar la mayor o menor gravedad de las conductas prohibidas, donde se exige la materialización de amenazas cuando hay intervención con victimas de mayor a 14 años. Ver fallo, 1."F. ,L. N. s/ corrupción de menores agravada" (Expte. T.C. Nº 4924-0244).

VI. Ley 27.078 Tecnologías de la Información y las Comunicaciones.

En otro orden, menciono la Ley de Tecnologías de la Información y las Comunicaciones, donde fue sancionada en el año 2014, donde presenta una regulación de la actividad de de los proveedores de los servicios de internet, como ser la explotación, licencias, precios etc. Teniendo como objeto, declarar como interés el desarrollo de la tecnología, como así también de la información, brindando protección de los Derechos de los consumidores de los servicios ponderados.

En principio es para destacar el Articulo 5, que hace referencia a la inviolabilidad de las comunicaciones, como el correo electrónico, el tráfico de datos realizados por los medio de las redes y servicios de telecomunicaciones, donde solo la interceptación de las mismas será únicamente ante el pedido de un Juez.

La presente regulariza a los proveedores de servicios, dando inicio desde el otorgamiento de las licencias con sus respectivos requisitos administrativos, pasando por el las sanciones ante el incumplimiento de su reglamentación. Por otro lado, detalla la calidad del servicio a ofrecer, como así también las intercomunicaciones deberán ser de calidad y precio justo.[34]

Luego en su Artículo 6, nos hace referencia a conceptos claves, como "Autoridad de Aplicación"; "Recursos Asociados"; "Servicio Básico Telefónico"; "Servicio de las Tecnologías de la Información y las Comunicaciones", este concepto se entiende por aquellos sistemas que transportan y distribuyen señales o datos entre usuarios, mediante redes de telecomunicaciones, donde cada servicio tendrá su regulación dentro de su marco jurídico.

Aquí observamos como la Ley de Tecnologías de la Información y las Comunicaciones comienza a interactuar con el tráfico de datos mediante la utilización de redes con señales inalámbricas o por cable. Luego tenemos un concepto de las "Tecnologías de la información y las comunicaciones", siendo un conjunto de recursos, programas informáticos, redes, aplicaciones que permiten el compilado, procesamiento, almacenamiento y transmisión de información.[35]

Por último vemos en su Artículo 7, como los conceptos específicos brinda una complementación a la Ley 26.388 de Delitos Informáticos, ya que la misma carece de conceptos claves en su desarrollo. Atento a lo mencionado podemos citar el concepto de "Acceso", "Arquitectura Abierta", "Interconexión" la cual nos dice que es aquella conexión física y lógica de las redes de telecomunicaciones de forma tal que los usuarios puedan comunicarse entre sí, también pudiendo acceder a los servicios de otros usuarios.

34. Ley 27.078 Artículo 5, Tecnologías de la Información y las Comunicaciones. (2014).
35. Ley 27.078 Artículo 6 Tecnologías de la Información y las Comunicaciones. (2014).

Continuando con “Red de Telecomunicaciones” siendo los sistemas de transmisión mediante cables, o señales inalámbricas o satelitales, terrestres; “Red Local” concepto clave en las conexiones de interfaces, siendo una sistema de redes, incluyendo software y hardware, para poder concluir con una conexión de un punto al otro; “Usuario de Servicios TIC” que es la persona física o jurídica que utiliza un servicio para sí. Todo esto, complementa a la legislación que regula la actividad delictiva informática.[36] Ver Fallo, “Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios".

VII. Ley 25.506 Ley de Firma Digital.

En la actualidad se desarrollan varios métodos para poder firmar determinados documentos físicos, pero también acompañado de la tecnología nos encontramos con documentos digitales y sus firmas. Donde estas firmas no son una firma como cuando utilizamos una lapicera, sino que la firma digital, se confecciones atreves de caracteres binarios que conforman una imagen. Para poder citar un ejemplo, se puede decir que un documento firmado con una lapicera que este a la vez es escaneado, su resultado es una imagen impresa en un papel.

Esto resulta valido como para la firma, ya que para que tenga validez jurídica se deberá verificar la identidad del firmante.

Este tipo de firmas digitales es utilizada en la administración pública y yendo poco a poco en los sectores del ámbito privado.

Uno de los objetivos que nos muestra la firma digital, es que tenga la misma validez que la firma holográfica, que también trae aparejado el beneficio de facilitar la veracidad a distancia entre las partes que intervienen, siendo que estas no se conocen físicamente. Pudiendo así, ampliar el desarrollo comercial tecnológico en internet.

El hecho de que internacionalmente halla una coordinación de validez jurídica de las firmas digitales, promueven la comunicación y la actividad empresarial, con el resto del mundo.

36. Ley 27.078 Artículo 7 Tecnologías de la Información y las Comunicaciones. (2014).

Hay países que se encuentran en sintonía ante las firmas digitales, donde existe una Ley modelo de comercio electrónico sancionada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, que fue aprobada en Nueva York en el año 1996, por la asamblea General de las Naciones Unidas.

También dentro de la Unión Europea nos encontramos con la Directiva de la Unión Europea sobre Comercio Electrónico, celebrado en el año 1997.

En los Estados Unidos, se encuentra en vigencia la Ley de Firma Digital, siendo este uno de los primeros países en legislar en materia comercial el uso de las firmas.

Esta Ley regula prevé estándares con otros países, con la finalidad de promocionar el comercio electrónico, siendo una Ley muy beneficiosa para los empresarios de los Estados Unidos.

En casi todo el mundo se encuentra legislada la Ley de Firma Digital, como se en Estados Unidos, Canadá, Francia, Italia, España, Reino Unido, Australia, Colombia, Japón, Corea, entre otros.

Dentro del territorio nacional podemos encontrar algunos antecedentes la Ley de Firma Digital, que regulan los contenidos y el uso de internet, pero que sirvieron como modelo la presente Ley. Estos antecedentes fueron el Decreto 554/97, donde refiere a declarar de interés Nacional el acceso de los Habitantes de la República Argentina a la red mundial de internet.

Luego podemos mencionar la resolución 1616/98, la cual adopta el procedimiento de Audiencia Pública, donde se presenta con la finalidad de que la sociedad mencione los distintos motivos de disconformidad relacionados a internet.

También tenemos la resolución 2226/2000, la cual hace referencia a los nombres de los dominios de internet.

Por último, quiero mencionar al Proyecto de la Unificación del Código Civil y Comercial, en el cual se hace referencia a las normas que regulan la prueba de los actos jurídicos, y se tratan los temas en relación a las firmas digitales.

La presente Ley sancionada en el año 2001, además de regular la firma digital nos brinda una definición de la misma. Uno de los pasos importantes que se generaron con esta Ley, fue la de haber modificado el ordenamiento jurídico, donde también se encontraba el Código Civil, donde hacen hincapié en la existencia de las firmas digitales y los documentos digitales. No se puede dejar de mencionar que es un elemento esencial

que se complemento con la sociedad y las nuevas tecnologías, que brinda así una expansión del comercio digital.

En su Artículo 1, la Ley establece que tiene como objetivo, reconocer el uso de la firma electrónica y de la firma digital, teniendo encuentra la eficiencia jurídica en las condiciones preestablecidas por la presente Ley.[37]

Dentro de las acciones que tenemos respecto a la firma digital, la criptografía, o clave pública, siendo una de las formas más seguras y con las características únicas de la firma holográfica.

La criptografía es una ciencia que estudia las medidas de seguridad de la privacidad y de la integridad de la información.

Es materia de las matemáticas que tiene como fin resguardar la confidencialidad de los textos, también la integridad de los datos, como así también la identidad de los contratantes.

Esta ciencia funciona estudiando la conversión de los textos desde su estado original, al estado de encriptado. Esta transformación se realiza mediante una operación de cifrado electrónica que procura que solo las personas que intervienen tengan la capacidad de poder leer la información enviada o recibida.

Esta operación se la denomina encriptación, que se la puede definir como insertar un algoritmo, que mediante la utilización de una clave, lo convierte en un texto incomprensible, e imposible de tomar lectura. La única opción de poder tomar lectura del texto es solo con la obtención de la clave.

La clave, es una llave que complementa a los algoritmos, que convierten en legibles o ilegibles los textos o archivos.

Otro de las firmas digitales que reconoce la presente Ley es la utilización de los valores Hash, que es una función algorítmica que convierte a un documento digital, en una cadena de bits, dejando al documento que contiene números y palabras, pasa a ser un resumen numérico llamado valor Hash. Este mensaje resumido y encriptado con una llave privada son reconocidos como una firma digital.

37. Ley 25.506 Ley de Firma Digital. Artículo 1. (2001).

A lo que respecta a la firma, nos encontramos con la llamada Firma holográfica, que es la firma realizada de puño y letra de una persona. Luego tenemos la Firma no holográfica, que son todas las firmas realizadas por cualquier medio que no sea de puño y letra. Atento a esta ultima definición, nos encontramos con una subdivisión siendo la firma no holográfica no electrónica, que resulta será toda firma realizada con cualquier medio que no electrónico. Para citar un ejemplo de esta clase de firmas podemos mencionar un sello.

Por último, encontramos la firma no holográfica electrónica, que en este caso, resulta ser toda firma que se realiza por intermedio de un elemento electrónico. Para que una firma sea electrónica o no, debe contener tres requisitos indispensables, como se la identifica, siendo esta que individualiza a la persona firmante; la presunción de autoría, esta presunción se toma a todos los documentos que se encuentren firmados, donde quién firmo se lo interpreta como el autor.

También, tenemos a la conformidad del texto que antecede, esto quiere decir que con la firma ubicada al final de texto, estamos ante la aceptación de la conformidad de la redacción e interpretación del texto.

Una vez aclarado como se conceptualizan, y componen los objetivos de estas, estamos en condiciones de citar la definición de la presente Ley, que nos indica que la firma digital es el resultado de la aplicación a un documento digital con un procedimiento matemático que solo el autor de la firma es quien mantiene el control del documento. Para que todo ello, tenga valor jurídico estas formas deberán ser pasibles de ser verificadas. [38]

Además la presente Ley nos menciona las presunciones como ser la de autoría, donde salvo prueba en contrario toda firma pertenece al titular del certificado digital, que permite la verificación de dicha firma. [39]

En otro de los artículos, encontramos la presunción de integridad, que quiere decir si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero. Siempre haciendo la salvedad de que exista prueba en contrario.

38. Ley 25.506 Ley de Firma Digital. Artículo 7. (2001).
39. Ley 25.506 Ley de Firma Digital. Artículo 2. (2001).

Una firma digital se presume verdadera mientras esta no haya sido modificada desde el momento de su firma, y esto se debe a que si el valor hash no ha cambiado es válida la firma. En uno de los casos en que el documento digital que se envía con la firma digital a un destinatario, y este lo recibe la Ley presume que el documento es firmado por el remitente, siempre que existe la prueba en contrario.[40]

Asimismo la Ley indica los requisitos que debe contener la firma digital para que esta sea válida, siendo cuando se ha creado en el tiempo de vigencia del certificado digital con validez del firmante.

Que la misma pudiera ser verificada. Será apreciada en referencia a los datos de verificación de la firma digital, indicando en el certificado.

Por otro lado, la ley establece las disposiciones en que no es aplicable la firma digital. Ante ello, se mencionan las siguientes:

- Por causa de muerte.
- Los actos jurídicos del derecho de familia.
- Los actos personalísimos en general.
- Los actos que tengan que ser instrumentados bajo las exigencias de la firma digital, siempre mediante las disposiciones que se encuentren con acuerdo entre las partes.

Ver Fallos "G.D.E.C/C. S.A. S/DILIGENCIA PRELIMINAR" Juzgado Nacional de 1º Instancia en lo Criminal nº18- Sec.nº 36- 23/10/2001. Buenos Aires y el de la C.N. Criminal y Correccional, Sala VI, en marzo 4 de 1999, caratulada "Jorge Lanata".

40. Ley 25.506 Ley de Firma Digital. Artículo 10. (2001).

VIII. Anteproyecto de Ley año 2014, Argentina.

En la República Argentina, en los últimos años, más precisamente en 2014, se intentó redactar un Anteproyecto de Ley en la materia que tratamos, escrito con gran esfuerzo, entre personas de gran conocimiento en materia informática, como así también en delitos informáticos, que tiene como finalidad la actualización legislativa, siendo impulsado por el Fiscal Ricardo Sáenz y acompañado de su equipo profesional.

Por otro lado y situándonos en el siglo XXI, la sociedad se encuentra definida y caracterizada con la tecnología y el tráfico de información como las comunicaciones, que todo en su conjunto ha llegado a modificar cada una de las actividades de una sociedad influyendo, en todas las ramas como la científica, la economía, la política, la educación, jurídica, medicina, etc.

Teniendo en cuenta la influencia, como el impacto que generan las nuevas tecnologías en la sociedad, y sosteniendo que nos encontramos en el inicio de un siglo que se pretende caracterizar por el desarrollo tecnológico, sería imposible hoy en día pensar en un mundo sin internet, olvidándonos de la tecnología sobre las computadoras, teléfonos celulares inteligentes, vehículos inteligentes, aeronaves inteligentes entre otros. Donde podemos mantener una comunicación de internet desde una computadora, o un vehículo, tarjetas de crédito, tarjetas S.U.B.E., o un celular, convirtiendo el tráfico de datos en vulnerables ante la ciberdelincuencia. Ver Fallo "G.D.E.C/C. S.A. S/DILIGENCIA PRELIMINAR" Juzgado Nacional de 1º Instancia en lo Criminal nº18- Sec.nº 36- 23/10/2001.

Los puntos principales del presente se suscitan en destacar que se mantienen los delitos de referencia a las comunicaciones electrónicas, también los accesos ilegítimos, los daños como así también el fraude informático y se incorpora el robo de identidad, siendo este uno de los delitos más comunes dentro de las redes sociales, con fines gravísimos de violación a los Derechos del Honor, la Intimidad, entre otros.

Uno de los puntos a tratar en este anteproyecto fue la del delito de distribución de pornografía infantil, donde se le aumenta la pena y desaparece la figura de tenencia de pornografía infantil con fines de distribución o comercialización. Otro de los puntos que el presente Anteproyecto es la de suprimir la descripción del tipo penal de la supuesta representación de las partes genitales del niño con fines predominantemente sexuales. Aquí se presenta una irregularidad de mala interpretación a mi entender de la

definición de pornografía infantil que fue citada descansando los fundamentos de la ley 26.388 que tiene su origen en el Protocolo Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía, que complementa y asiste a la Convención de las Naciones Unidas sobre los Derechos del Niño.

Otro de los puntos a tratar en el presente Anteproyecto, es la regulación del delito de grooming, en donde pretende disminuir la edad de cobertura legal hasta los menores de 13 años de edad. También teniendo en cuenta el delito de Trata de menores de edad donde en la actualidad se encuentra previsto una pena de 10 hasta 15 años de prisión, según el Artículo 145 ter del Código Penal de la Nación, introducido por la Ley 26.842. En el presente Anteproyecto se realiza un exhaustivo análisis de la edad en los menores de edad y la desdobla para luego fijar una pena más importante siendo de 4 hasta 15 años de prisión si se trata de menores de edad, pero se la aumenta desde 8 años el mínimo cuando la víctima fuese menor de 13 años de edad.

También teniendo en cuenta la prueba digital en materia procesal se analizó reformar el Código Procesal de la Nación, teniendo como objeto tratamientos sobre la prueba digital, donde se incorporan las acciones de los jueces y los fiscales para que se interioricen en materia de investigación sobre delitos informáticos. Destaco así, que esta regulación que se propuso toma como espíritu del ámbito de los principios de legalidad, y ante la anuencia de las líneas redactadas en la Convención de Budapest.

Una de las ideas que se plasmaron en el Proyecto fue la de cómo indicarle a un proveedor de servicios de internet, o de servicios de mensajería instantánea, que congele una cuenta, o que diligencie los datos del usuario o contractuales para quedar a disposición de la Justicia.

El proyecto también tiene en cuenta la potestad de que solo los jueces deben solicitar determinada información con el fin de obtener los datos contractuales de las conexiones de las comunicaciones electrónicas y el contenido proprio en tiempo real. Todo esto, en la actualidad se desempeña mediante la utilización de normas análogas que corresponden a la prueba física, normas que en materia de delitos informáticos resultan obsoletas, desarrollando así un proceso judicial en el límite de las nulidades y sanciones procesales a los que intervienen en dicho proceso.

Uno de los puntos principales de la prueba digital es la mantención de la cadena de custodia, la cual descansan los principios de legalidad y del debido proceso. El Estado es quien debe brindar la protección de las garantías constitucionales, del

imputado ante la presencia de pruebas digitales, que son vulnerables de cualquier tipo de alteración fácilmente, siendo manipuladas solo por personas capacitadas a tales fines, con el objeto de llegar a la etapa de juicio oral, la prueba se mantenga intacta, validado las pericias judiciales practicadas sobre la misma, otorgando transparencia, legalidad, y profesionalidad a los procesos judiciales sin violar ninguna garantía constitucional del o los imputados.

➢ Capítulo 4: Problemática en los Procesos Investigativos.

I. Conflictos en las investigaciones en tiempos pasados y actuales

A mi entender una problemática actual en materia de investigación y legalidad, donde hacer frente a la investigación de los delitos informáticos, habiendo precoz regulación donde nos lleva muchas veces a los conflictos con la legalidad de los procesos judiciales. El desarrollo tecnológico se configura a diario, donde el personal que interviene en este tipo de delitos debe estar capacitado y actualizado a todo momento.

Esto en la actualidad no sucede, por ello nos encontramos con falencias investigativas, originado nulidades, o falsa imputaciones, por no entender en materia de investigación y manipulación de la tecnología utilizada como medio delictivo. En la Ciudad Autónoma de Buenos Aires, se ha creado la Fiscalía Especializada en Delitos Informáticos, donde con su reciente aparición ha contemplado amplios resultados positivos en materia de investigación. La misma contempla amplios recursos de personal profesional capacitado específicamente, como así también en materia de recursos logísticos para poder llevar a cabo cada una de las investigaciones que desarrollan. También cuenta con capacitaciones constante para su personal dándole un prestigio de excelencia en materia de delitos informáticos.

En la Provincia de Buenos Aires, como en muchas otra no existe un protocolo de actuaciones frente a la intervención judicial de un elemento tecnológico. Por ello, como ejemplo en la Ciudad Autónoma de Buenos Aires, la promoción de un recurso de nulidad sobre la prueba, donde el Fiscal interviniente, entiende que no existe un protocolo de actuación sobre asuntos de peritajes informáticos, "que la evidencia obtenida por los profesionales de la UBA -en concreto, los correos electrónicos que

constituyen la evidencia probatoria para este y otros expedientes- no sufrió alteración alguna con posterioridad a su secuestro".

Al mismo tiempo, destacó que más allá de las buenas prácticas forenses no existe un protocolo de actuación que prevea la observancia obligatoria de aquellas para realizar peritajes sobre material informático".[41]

Casos como este se dan a diario donde la falta de un protocolo de procedimientos judiciales sobre elementos electrónicos, acarrean como consecuencia la nulidad del acto jurídico. Por tal motivo se presentan para las Fuerzas de Seguridad una metodología en la cual se inician las investigaciones informáticas redactadas en la obra llamada El Rastro Digital del Crimen, presentando así un método investigativo.

Partiendo de la identificación, donde se debe conocer todos los elementos pasibles de comprender la prueba digital, una preparación en la cual se debe tener conocimiento de las herramientas a utilizar, como así también los recaudos jurídicos para mantener la legalidad de los actos jurídicos, por otro lado se debe desarrollar una planificación estratégica, donde se debe plantear todas las condiciones físicas que intervienen alrededor de la futura prueba digital, mantener la ubicación del lugar del hecho seguro de toda intervención ajena, que pueda destruir o modificar o contaminar la futura prueba digital; luego se realiza la recogida de la prueba digital, es de especial atención el reconocimiento de esta prueba, su posterior levantamiento, manipulación, y embalaje.

En países como Estados Unidos se presentan las llamadas "guías", reconocidas en nuestro territorio como los protocolos de actuación, donde el Departamento de Justicia publicó la guía, en la cual nos presenta un protocolo de actuación ante delitos informáticos. Departamento de Justicia de los Estados Unidos, Oficina de Programas de Justicia. (2008). Investigación de la Escena del Crimen. Estados Unidos.

Desde el Departamento de Cooperación Jurídica, el cual es dependiente de la Secretaría de Asuntos Jurídicos, de la Organización de los Estados Americanos, en la cual dentro de su organigrama existe una unidad que se dedica exclusivamente al estudio de las investigaciones de los Delitos Cibernéticos.

41. Causa n° 46.744 "Fiscal s/ apela declaración de nulidad de informe pericial".

Esto nos quiere decir, como los Organismos internacionales prestan mucha atención a la comisión de los delitos informativos. Teniendo en cuenta siempre, las consecuencias posibles que se pueden desencadenar ante un ataque cibernético, sería poco serio que países no contemplen un protocolo de procedimientos ante la comisión de delitos informáticos, también teniendo en cuenta al personal, siendo siempre idóneos en la materia.

La tecnología ha logrado que cualquier persona pueda tener al alcance de su mano un elemento electrónico, donde podemos manipular en toda hora, teniendo acceso a Internet, logrando así comunicaciones instantáneas a nivel mundial. En todas estas actividades la sociedad aún no ha tomado conciencia de de la magnitud del uso de internet, como así también la vulnerabilidad, en la que nos encontramos cuando utilizamos la tecnología. Ahora bien, a la hora de encontrarnos frente a un elemento electrónico se nos despiertan una gran cantidad de interrogantes, ya que debemos mantener la legalidad del proceso judicial que existe para ser víctimas de un delito informático.

II. Prueba digital

Para dar inicio a este tema, quiero mencionar que dentro de las medidas preventivas de los métodos de investigación, encontramos a la informática forense, la cual se desprende como una disciplina de la criminalística, que presenta como fin la investigación de los sistemas informáticos dentro de una investigación judicial.

Esta informática desarrolla técnicas para reproducir y analizar evidencias digitales

En la informática forense, encontramos cuatro normas que rigen todo actuar ante la manipulación de la prueba digital siendo:

- Preservar la evidencia original
- Establecer y mantener la Cadena de Custodia
- Documentar todo hecho
- NO EXTRALIMITARSE
    1. Conocimientos personales.
    2. Leyes, Normas, Procedimientos.

La complejidad de las investigaciones en relación a lo delitos informáticos, tenemos que destacar el elemento fundamental que sostiene un proceso judicial, donde

será la protagonista en la sentencia que se dicte. Temas Avanzados en Seguridad y Sociedad de la Información. (2013). *Informática Forense*. (11-11). Recuperado de: http://www.criptored.upm.es/descarga/ConferenciaJavierPagesTASSI2013.pdf

Este elemento es la prueba, que en procesos ordinarios respecto a los delitos cometidos con pruebas físicas, como el robo, podemos encontrar elementos para forzar determinados accesos, o en el hurto podríamos tener como prueba una huella digital o entre otros el homicidio, donde aparecerían pruebas como elementos contundentes, o punzo cortantes o armas de fuego etc. Pero ¿cómo nos referimos a las pruebas donde se cometen delitos informáticos?

En los Estados Unidos de Norteamérica, atiende con gran importancia los conflictos ante la prueba digital, que al haber una regulación particular para este tipo de pruebas, los juristas han aplicado las normas previstas para las pruebas físicas, y aquí es donde se inician los conflictos legales del debido proceso.[42]

Tomando como referencia a los Estados Unidos de América donde, los Jueces Federales han unificado criterios a los fines de confeccionar un modelo de actuación ante los procedimientos de materia de delitos informáticos, donde si bien cada uno de los Estados que componen los Estados Unidos, confeccionaron un protocolo de procedimientos ante los peritajes informáticos, resguardo de la prueba digital, cadenas de custodias, recolección de la prueba digital entre otros.

El Departamento de Justicia, ha confeccionado una serie de protocolos de actuaciones ante la presencia de la prueba digital, a los fines de brindar información a las fuerzas de seguridad que intervienen en materia de delitos informáticos para la recopilar evidencia, con una variedad de alternativas técnicas para recabar y conservar prueba contenida en medios electrónicos. Uno de los manuales más utilizados por las fuerzas de seguridad Estadounidenses es un manual llamado "Evaluación Forense de Información Digital" (Forensic Examination of Digital Evidence: A Guidefor Law Enforcement).[43]

42. F.B.I. (2010). *Internet Crime Schemes*, (2-2). Recuperado de www.fbi.gov/stats-services/publications/mortgage-fraud-2010
43. F.B.I. (2003). *Forensic Examination of Digital Evidence: A Guidefor Law Enforcement* (44-46). Recuperado de https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

En el manual se destacan los tres pilares fundamentales ante la intervención de las pruebas digitales, siendo el proceso de recopilación, la custodia y el peritaje de la prueba digital.

En la Argentina aún no se encuentra un manual de unificación de protocolos de actuación de intervención ante la presencia de pruebas digitales, que al intervenir sobre elementos electrónicos considerados como prueba digital, debemos tener presente siempre, que no cualquier persona puede manipular una prueba digital, ya que la misma ante sus características físicas, solo personal capacitado y especializado debe manipular la misma.

La intervención directa de personal no capacitado y con desconocimientos sobre estos elementos nos puede incurrir en la violación al Principio de la Privacidad, o el Principio de la Intimidad, al Honor etc., donde cualquier acto que obtenga este resultado no remite a la nulidad del acto jurídico. Atento al esfuerzo por el personal de las fuerzas de seguridad y judiciales de capacitarse por voluntad propia o participando de los escasos cursos de capacitación que se brindan, con los fines garantizar la legalidad correspondiente a los procesos judiciales.

Un modelo de protocolo de actuación ante la presencia de pruebas digitales, existe en la provincia de Neuquén, donde juristas especializados y personal especializado en materia informática han confeccionado el llamado "Protocolo de actuación para Pericias Informáticas". Este protocolo se presenta como una guía de actuaciones, garantizando los Derechos y Garantías Constitucionales de las personas, ante un proceso judicial, ante una imputación o siendo víctima de un delito informático.

Una forma de realizar las diligencias judiciales sin trasgredir los Derechos de los individuos que son titulares de los mismos es garantizar en principio son las cadenas de custodias de las pruebas digitales, como así también las etapas periciales de los mismos que mantengan la no violación del los principios del debido proceso. Este protocolo nos indica partiendo desde la realización de un secuestro de un elemento electrónico, identificar y como preservar la prueba, la aparición de la prioridad en casos urgentes, como así también el traslado y recepción de los elementos electrónicos, etc. López, D. L. (s/f). *Protocolo de Actuaciones para Pericias Informáticas*. Neuquén.

Para observar como la prueba digital se presenta como un elemento que dependiendo de cómo se aporta, resulta una ventaja judicial o no. Tal es el caso en que se presenta un conflicto legal entre dos personas, donde una de ellas encuentra mensajes

de características eróticas, como así también mails de mismo tenor. Una de las personas resulta ser de estado civil casada. Más allá que el Tribunal, entiende que no es prueba de la existencia de infidelidad, ni una relación entre sí, el intercambio de mensajes de texto o emails. La resolución dictada por el Tribunal, entendió que las pruebas presentadas no eran suficientes como para comprobar la existencia de las causales de divorcio. Ahora bien, pero respecto a las pruebas presentadas, los magistrados manifestaron que "No basta con el intercambio de palabras o mensajes cargados de erotismo y de fantasías entre los dos polos de comunicación de la red, pues la infidelidad virtual, en tanto no pase a 3D, no llega a consumar el encuentro carnal que configuraría el adulterio".[44]

Aquí vemos como un Tribunal adopta los elementos electrónicos como prueba dentro del proceso judicial, siguiendo la reforma del Código Penal, como se incorpora como elemento de prueba, la tecnología. Hoy en día la prueba informática se presenta en los conflictos jurídicos como prueba esencial y de primera instancia.

Mientras tanto, un Tribunal de la justicia Chubutense, entiende ante las pruebas electrónicas, no admitió la validez de la mensajería de texto como prueba ante el advertimiento de infidelidad. En este caso, la parte actora reviso el teléfono celular de la otra parte, encontrando mensajes de texto que posiblemente atendía a una infidelidad. Pero sin advertir que se pronunciaba una violación de los principios de privacidad y de intimidad, que la parte actora provoco al revisar el teléfono celular de la parte demandada. Según el Dr. Naudin, quien menciona que muchas veces la invalidez de la prueba resulta pertinente de acuerdo como se presenta, en estos casos un Tribunal acepta una prueba digital, mientras que otro entiende que existe una violación de los principios de privacidad y de intimidad. Himitian, E. Diario La Nación. (2011). *Los Mails eróticos no son prueba de infidelidad.* (1-1).

44. Fallo, de la Sala “M” de la Cámara Nacional de Apelaciones en lo Civil, “V., E. O. c/P., M. L. s/ divorcio art. 214 inc. 2do. Código Civil”.

III. Intervención de las fuerzas de seguridad y personal judicial

Como punto de inicio se debe mencionar que en la República Argentina, no se encuentra ninguna normativa de capacitación del personal judicial, y de las fuerzas de seguridad ante la presencia de los delitos informáticos. Muchos de ellos, logran capacitaciones desde su ámbito particular, partiendo de su propio interés. Haciendo escaso personal idóneo en materia de investigaciones de delitos informáticos, como así también en materia pericial informática.

Para ello, es que voy a mencionar como la legislación internacional atiende a los delitos informáticos, desde la importancia que tiene la capacitación del personal que interviene a tales fines.

Teniendo en cuenta la Ley 53/07 de República Dominicana, donde desde la legislación internacional se toma en cuenta la importancia en circunstancias de delitos informáticos para su investigación, donde debo remarcar el Artículo 35, donde tiene en cuenta la capacitación del personal interviniente ante la presencia de los delitos informáticos. El mismo se presenta con la creación de una institución llamada Instituto Tecnológico de las Américas, el cual se encargará de la capacitación de los funcionarios.

En algunos países de Latinoamérica existen instituciones específicas al solo efecto de la investigación de los delitos informáticos, como ser los siguientes:

- Bolivia, existe la División Delitos Informáticos que es parte de la Fuerza Especial de Lucha Contra el Crimen. FELCC de la Policía Nacional.
- Colombia, existe el grupo de delitos informáticos de la SIJIN (Policía Nacional) quien tiene varios laboratorios de computación forense, y el DAS (Departamento Administrativo de Seguridad) que tiene una unidad específica de delitos informáticos, además de varias entidades investigativas privadas que colaboran con los agentes nacionales.
- Uruguay, existe la sección Delitos Informáticos del Departamento de Delitos Complejos, de la Dirección de Investigaciones de la Jefatura de Policía.
- Ecuador, existe la DIDAT, Departamento de Investigación de Alta Tecnología de la Policía Judicial del Ecuador, y la Fiscalía General del Estado existe el Departamento de Investigación y Análisis Forense.

- México, la Policía Cibernética de la Secretaría de Seguridad Pública Federal, trabaja en temas de delitos informáticos, llevando a cabo campañas de prevención del delito informático a través de la radio y cursos en instituciones públicas y privadas.

En la República Argentina existen varios cuerpos policiales de investigación pero que no son instituciones específicas en el tratamiento de los delitos informáticos, sino que con el paso del tiempo, estas fuerzas se han visto obligadas a confeccionar organismos de investigaciones, con personal idóneo para poder incurrir en el combate de los delitos informáticos, un ejemplo claro es la División de Delitos en Tecnología y Análisis Criminal de la Policía Federal. Pero ello, no basta con la ausencia de organizaciones específicas que tendrías que integran también el ámbito judicial. Esta es una ausencia de materia investigativa, que fue demarcada por el Procurador General de la Nación y de los participantes del segundo curso intensivo sobre "Delitos informáticos, investigación y prueba digital" a cargo del fiscal Ricardo Sáenz. Sáenz, R. (2012). El problema de la investigación de los delitos informáticos. [*Versión electrónica*], *Revista Digital, El Derecho Informático*, (6-6).

Siguiendo los lineamientos del Fiscal Ricardo Sáenz, especialista en materia de delitos informáticos, la problemática de la capacitación de los intervinientes desde el sistema judicial, hasta el policial, siendo esta una necesidad importante a la hora de realizar una investigación, que interactúa entre la tecnología e internet. Esta es una herramienta fundamental a la hora de progresar en un proceso judicial y poder llegar a la autoría de una conducta típica.

La República Argentina debe comprometerse en este sentido, a los fines de posibilitar la más adecuada capacitación de sus fuerzas de la ley, para ponerla a la altura de los ciberdelincuentes para poder afrontar los conflictos. R. Sáenz, (2012), Panorama del combate contra el Ciberdelito, [*Versión electrónica*], *Red Iberoamericana El Derecho Informático.* (3-3).

En nuestro país se puede mencionar que en la Policía de la Provincia de Buenos Aires, tiene una Dirección temática llamada Dirección Cibercrimen, la cual fue creada hace pocos años. Su origen se advierte ante las numerosas denuncias en relación a delitos informáticos, que se recibían en las comisarias, y demás dependencias policiales, donde muchas veces las denuncias no prosperaban ante la falta de conocimiento de los

efectivos policiales al momento de la recepción de la denuncia tipificado el delito, o ya en la investigación.

Es por esto, que mediante un análisis realizado por el Estado de la problemática y la amenaza que refería el delito informático, en el año 2009 se crea la Dirección de Cibercrimen, donde descansan los fundamentos de su funcionalidad ante la AG/RES. 1939 (XXXIII-O/03).

En la mencionada resolución, establece que el Comité Directivo Permanente de la Comisión Interamericana de Telecomunicaciones, enuncia la "creación de una cultura de ciberseguridad para proteger la infraestructura de las telecomunicaciones aumentando la conciencia entre todos los participantes de las Américas en las redes y sistemas de información relacionados con el riesgo de dichos sistemas y desarrollando las medidas necesarias para hacer frente a los riesgos de seguridad respondiendo rápidamente a los ciber-incidentes".[45]

Esta resolución encarece a los Estados miembros, tener en cuenta a través de La Comisión interamericana de Telecomunicaciones y del Grupo de Expertos Gubernamentales sobre Delito Cibernético de la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas, que se dio inicio al desarrollo de un proyecto a los fines combatir al ciberdelincuencia, mediante la multidiciplina de la prevención.[46]

Ante lo expuesto es que en la Provincia de Buenos Aires, por intermedio del Ministerio de Seguridad, se publicó en el boletín oficial del Ministerio de Seguridad de la Provincia, la función específica que abarca la Dirección, donde se realizarán tareas de reunión de información, teniendo en cuenta las nuevas tecnologías en la investigación; mantener actualizado los métodos investigativos de los delitos informáticos; hacer conocer la nueva temática delictiva, y generar medidas preventivas y de combate ante los delitos presentados y por último, trabajar en conjunto con los Ministerios Públicos y demás fuerzas de seguridad a los fines de desarrollar investigaciones referentes a la temática.

45. Ag/res. 1939 (xxxiii-o/03) Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética. (2003).
46. Ag/res. 1939 (xxxiii-o/03) Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética resolución 2. (2003).

Esta Dirección se encuentra compuesta por la División Seguridad de las Personas, la División Pornografía Infantil, y la División Procedimientos Electrónicos, lugar este donde se realizan todo tipo de pericias electrónicas. [47]

A Nivel nacional tenemos la Policía Federal Argentina, donde presenta desde hace unos ocho años a la División Delitos Tecnológicos, la cual resulta ser una unidad especializada en la temática de los delitos informáticos. Desde sus inicios se mantuvo la problemática de los métodos investigativos en materia de delitos utilizando las tecnologías, donde con el paso del tiempo, se incluyeron personal civil con conocimientos en programas y utilización de la informática, para capacitar de manera informal y a criterio de la superioridad, (sin protocolos algunos), al personal de las fuerza de seguridad.

Se han planteado muchos inconvenientes investigativos y también procesales, que para citar podemos decir una sentencia de nulidad, donde la División Delitos Informáticos, ha confeccionado una investigación donde se solicitaron llamadas entrantes y saliente de un abonado telefónico, pero la parte investigada se vió agraviada, ya que considera que mediante el sustento del la causa Halabi, 270.KLII, del 24 de febrero del año 2009, donde sostiene que las intervenciones telefónicas resultan ser autorizadas por el Juez de intervención.

En este caso, las comunicaciones entrantes y salientes, se igualan al tipo de una intervención telefónica, por tal motivo es que se solicita la pronunciación de un Juez. Es por ello, que aquí observamos como los desconocimientos del proceder ante los elementos tecnológicos llevan a resultados de nulidades procesales.[48]

Luego en la Ciudad Autónoma de Buenos Aires, encontramos a la Policía Metropolitana, donde con poca antigüedad en funcionamiento resulta ser una de las fuerzas más especializadas y con más tecnología aplicada a las investigaciones informáticas. En esta policía se presenta con el Área Especial de Investigaciones Telemáticos, como dijimos su reciente creación ha concebido en la incorporación de personal de seguridad ya capacitado en la temática de los delitos informáticos.

47. Ministerio de Seguridad de la Provincia de Buenos Aires. Boletín Informativo Nº 61. Recuperado http://www.mseg.gba.gov.ar/Boletin%20Informativo/ordenes/his_pdf/BoletinInformativoM,JyS2011/BI-61-11.ACTUAL.pdf
48. Causa Nº 135 “M. O., L. L. s/procesamiento Interlocutoria Sala de Feria “B” (17).- Juzgado de Instrucción Nº 30.

Todo esto, acompañado de la tecnología implementada y con el apoyo de la Fiscalía Especializada en Delitos Informáticos hace una excelencia en la práctica investigativa y procesos judiciales.

En el año 2012, en la Ciudad Autónoma de Buenos Aires, se crea mediante la Resolución501/12, la Fiscalía General, donde por intermedio de ella, se hace una prueba piloto por un tiempo determinado de un Equipo de Fiscales Especializados en Delitos y Contravenciones Informáticas, teniendo completa jurisdicción en la Ciudad Autónoma de Buenos Aires, con el objeto de investigar los delitos informáticos que incurren una compleja investigaciones judicial, con una enorme dificultad a la hora de individualizar al autor del delito.

Para esta Fiscalía Especializada la cual interpreta que los métodos de investigación resultan muy diferentes a las investigaciones tradicionales, ya que es necesaria la utilización de las mismas herramientas con las que se cometen los ilícitos, ósea las nuevas tecnologías, pudiendo de esta forma detectar, recolectar y preservar la evidencia digital, que es un elemento nuevo en el proceso judicial. D. Dupuy, T. Vaccarezza, M. Kiefer y C. Neme, (2012), *Informe Final Cibercrimen* C.A.B.A. (1-1).

IV. Conclusiones finales

Habiendo presentado la temática de los Delitos Informáticos, su impacto jurídico en la República Argentina y el mundo, resulta indispensable una legislación apropiada, especifica, y de constante actualización, que debe ser tratada por juristas especializados en la temática.

En principio entiendo que sería imprescindible tener un organismo integrado especialistas informáticos, que se dediquen al estudio del desarrollo tecnológico y como podría ser utilizado para delinquir, advirtiendo mediante informes a los legisladores para que estos puedan apreciar una actualización adecuada, pudiendo de esta forma hacer efectivas las medidas preventivas de seguridad.

Respecto a este tipo de delitos donde los índices delictivos se incrementan con el paso de cortos periodos de tiempo, tenemos presente que en nuestro país contamos entre

otras, con la Ley 26.388, la cual ha sido muy importante en la legislación vigente, pero que aun no es suficiente.

A mi entender y habiendo realizado el presente trabajo, sería necesario actualizar el Código Penal, con conductas delictivas más específicas, como por ejemplo, la tipificación del robo de identidad dentro de los sistemas informáticos, siendo este un delito común en estos días. También la calificación legal de estafa, resulta inapropiada en la actualidad, ya que en los sistemas informáticos existen distintas formas de estafa que otros países han tipificado, como ser el phishing, vishing y pharming.

También el Código Procesal debería contemplar modificaciones que otorguen resguardo a las garantías procesales cuando se realiza una investigación. No olvidemos que también se efectúan investigaciones cibernéticas, y existe el contacto de las pruebas digitales que sus diligencias son adaptadas mediante una normativa antigua. Con una adecuada legislación procesal evitaremos caer en nulidades judiciales, dejando sin justicia a las víctimas.

Otro punto a tener en cuenta, es que la justicia pueda utilizar sus facultades investigativas ante las prestatarias de servicios de internet, ampliando el espectro para que no solo se informen datos contractuales, sino también se pueda ejercer mediante la Ley, el resguardo de la información o proceder a un congelamiento de la misma ante una urgencia judicial.

Respecto a los recursos humanos, es indispensable coordinar un esfuerzo de capacitación del Poder Judicial y fuerzas de seguridad, a los fines de poder inmediatamente identificar un delito informático, preceder a su investigación y eficiente individualización del o los imputados.

Debemos tomar conciencia de la peligrosidad que los delitos informáticos y estar preparados.

V. Bibliografía.

- Ag/res. 1939 (xxxiii-o/03) Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética. (2003).
- Ag/res. 1939 (xxxiii-o/03) Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética resolución 2. (2003).
- Área de Tecnología de la Información y de las Comunicaciones Aplicadas, (2011). Manual Básico de creación de páginas web. *Creación de páginas webs. 1* (1). Recuperado de https://www.um.es/atica/documentos/html.pdf
- Bendinelli M. (2014). Delitos informáticos. *La importancia de la prueba digital en el proceso judicial.* (1-1). Recuperado de: http://aldiaargentina.microjuris.com/2014/12/03/delitos-informaticos-la-importancia-de-la-prueba-digital-en-el-proceso-judicial/
- Causa Nº 135 "M. O., L. L. s/procesamiento Interlocutoria Sala de Feria "B" (17).- Juzgado de Instrucción Nº 30.
- Causa n° 46.744 "Fiscal s/ apela declaración de nulidad de informe pericial".
- Convención de Budapest, (2001).
- Convención de Budapest, (2001). Preámbulo, 4to. Párrafo.
- Convención de Budapest, (2001). Preámbulo, Artículo 2-9.
- Convención de Budapest, (2001). Preámbulo, Artículo16-21.
- Convención de Budapest, (2001).
- Convención Sobre Los Derechos Del Niño, UNICEF. (2006).
- Cuapio M. R. (s/f). A*ctualización judicial en el estado de Tlaxcala, dentro del marco del derecho informático y la informática jurídica en el siglo XXI. Marco Conceptual*. Recuperado de http://www.ordenjuridico.gob.mx/Congreso/pdf/172.pdf
- Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas. (2012).
- Del Castillo Torres, L. (2005). Manual Del Auxiliar Administrativo de Instituciones Sanitarias, *{versión electrónica}. Conceptos. 3* (1) 492-492.
- Disposición Nº 2/2013, Jefatura de Gabinete de Ministros Secretaria de Gabinete y Coordinación Administrativa Subsecretaria de Tecnologías de Gestión Oficina Nacional de Tecnologías de Información.

- División Contraterrorismo, (2015), Dirección Cibercrimen, Policía de la Provincia de Buenos Aires. Causa FLM 104/2014.
- Dr. G. Ríos Patio. U.S.M.P. Facultad de Derecho, Revista Sapere. *Delitos Electrónicos.* (2-2). http://www.derecho.usmp.edu.pe/instituto/revista/articulos/DELITOS_ELECTRONICOS.pdf
- Dr. Montano Álvarez, A. A. (2008) La Problemática Jurídica en la Regulación de los Delitos Informáticos, *La Problemática Jurídica en la Regulación de los Delitos Informáticos. 1*. (1) recuperado de http://www.ordenjuridico.gob.mx/Publicaciones/Tesis2010/01_LDP_MONTANO.pdf
- Dupuy, D. T. Vaccarezza, M. Kiefer y C. Neme, (2012), *Informe Final Cibercrimen* C.A.B.A. (1-1).
- Fallo, de la Sala "M" de la Cámara Nacional de Apelaciones en lo Civil, "V., E. O. c/P., M. L. s/ divorcio art. 214 inc. 2do. Código Civil".
- F.B.I. (2003). *Forensic Examination of Digital Evidence: A Guidefor Law Enforcement* (44-46). Recuperado de https://www.ncjrs.gov/pdffiles1/nij/199408.pdf
- F.B.I. (2010). *Internet Crime Schemes*, (2-2). Recuperado de www.fbi.gov/stats-services/publications/mortgage-fraud-2010
- F.B.I. (2015). *Internet Crime Complaint Center.* E.E.U.U. Recuperado de www.fbi.gov/about-us/investigate/cyber
- García J. (2015/13/11). La informática, conceptos básicos y datos históricos. [Etimología]. Recuperado de http://lainformaticayelcomputador.blogspot.com.ar/
- Himitian, E. Diario La Nación. (2011). *Los Mails eróticos no son prueba de infidelidad.* (1-1).
- I.N.D.E.C. (2011). *Encuesta Nacional sobre Acceso y Uso de Tecnologías de la Información y de la Comunicación.* Informe preliminar sobre indicadores básicos de acceso y uso. Resultados de mayo-julio de 2015. (2). Recuperado de http://www.gobiernoabierto.gob.ar/multimedia/files/TICs_nacional.pdf

- Jane, C. (2009). El Padre del Email. El periódico. (s/v). Recuperado de http://www.elperiodico.com/es/noticias/ciencia-y-tecnologia/20090617/ray-tomlinson-envio-primer-correo-electronico-1971/113183.shtml
- Khoo Boon Huim, (2012), Interpol le declara la guerra al cibercrimen , *Fraude y Cibercrimen,* (1-1). Recuperado de https://haddensecurity.wordpress.com/2012/page/84/
- Ley 8/2011, (2011), Medidas para la Protección de las Infraestructuras Críticas. Jefatura del Estado, España.
- Ley 19223, Delitos Informáticos, Chile. (1993).
- Ley 20.009, Limita la Responsabilidad de los Usuarios De Tarjetas de Crédito por operaciones realizadas con Tarjetas Extraviadas, Hurtadas o Robadas. (2005).
- Ley 18168, Ley General de Telecomunicaciones, Chile.(2002).
- Ley 1.160/97, Delitos Informáticos, Paraguay, Artículos (144, 146, 173, 174, 175, 188, 189, 220). (1997).
- Ley 1.160/97, Delitos Informáticos, Paraguay, (1997). Artículo 188, inc. 1, 2, 3, 4.
- Ley N° 2861/06,Represión el comercio y la difusión comercial o no comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces (2006).
- Ley 11.829, Delitos Informáticos, Brasil. (2008).
- Ley 1.768, Delitos Informáticos, Bolivia. (1997). Artículos el 363 bis y Articulo 363 ter.-
- Ley 27309, Delitos Informáticos. Perú. (2005).
- Ley Nº 53-07. Delitos Informáticos. República Dominicana (2007).
- Ley Nº 53-07, Delitos Informáticos. (2007).Articulo 4, República Dominicana.
- Ley 26.388 Ley de Delitos Informáticos. Argentina. (2008).
- Ley 25.326 Ley de Protección de Datos Personales. (2000).Argentina, Artículo 2.
- Ley 25.326 Ley de Protección de Datos Personales. . (2000).Argentina. Artículo 16.
- Ley 25.326 Ley de Protección de Datos Personales. (2000).Argentina. Artículo 26.

- Ley 25.326 Ley de Protección de Datos Personales. (2000).Argentina. Artículo 9.
- Ley 863, Artículo 1, Ley de Establecimiento Comerciales. (2003).
- Ley 863, Artículo 2-3, Ley de Establecimiento Comerciales. (2003).
- Código Penal de Chile, Artículo 366 quater.
- Ley 27.078 Artículo 5, Tecnologías de la Información y las Comunicaciones. (2014).
- Ley 27.078 Artículo 6 Tecnologías de la Información y las Comunicaciones. (2014).
- Ley 27.078 Artículo 7 Tecnologías de la Información y las Comunicaciones. (2014).
- Ley 25.506 Ley de Firma Digital. Artículo 1. (2001).
- Ley 25.506 Ley de Firma Digital. Artículo 7. (2001).
- Ley 25.506 Ley de Firma Digital. Artículo 2. (2001
- Ley 25.506 Ley de Firma Digital. Artículo 10. (2001).
- López, D. L. (s/f). *Protocolo de Actuaciones para Pericias Informáticas*. Neuquén.
- Lugo Ramírez, I. (s/f). *Introducción a las computadoras*. Unidad de Servicios al Usuario (Vol. I). Recuperado de http://www.uprm.edu/cti/docs/manuales/manuales-espanol/vax-vms/manuales/Intcomp.pdf
- Lujambio, I., Martínez, L., Rodríguez, E. y Fernández, C. (2005). Guía practica de internet. *{Versión electrónica} Acercando el uso de la Red a las Organizaciones Comunitarias* 2. (1). 17-19.
- Menalkiawn. (2013). Manual básico de Seguridad Informática para activistas. *una guía para proteger nuestros ordenadores y a nosotras mismas hacer frente a la represión y extender una cultura de seguridad. 1*. (1). Recuperado de http://mexico.indymedia.org/IMG/pdf/libro_manual_seguridad_informa_tica_activistas.pdf
- Ministerio de Seguridad de la Provincia de Buenos Aires. Boletín Informativo Nº 61. Recuperado http://www.mseg.gba.gov.ar/Boletin%20Informativo/ordenes/his_pdf/BoletinInformativoM,JyS2011/BI-61-11.ACTUAL.pd

- Muller, E. (2015). Internacional. *La NSA se prepara para la guerra mundial cibernética, según Der Spiegel.* (10-10). Recuperado de http://internacional.elpais.com/internacional/2015/01/17/actualidad/1421500678_347192.html
- Paterlini N., Vega C., Guerriero G. y Velázquez M. (s/f). Delitos Informáticos. *Antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos. 1*. (1). Recuperado de http://www.aadat.org/delitos_informaticos20.htm
- Rivera, M. L. (2006-2007). Revista Jurídica. Obtenido de firma digital, consideraciones jurídicas: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20revista%20juridica/Revista%20Juridica%2006-07/articulos/02Firma.pdf
- Sáenz, R. (2012). El problema de la investigación de los delitos informáticos. [*Versión electrónica*], *Revista Digital, El Derecho Informático,* (6-6).
- Sáenz, R. (2012), Panorama del combate contra el Ciberdelito, [*Versión electrónica*], *Red Iberoamericana El Derecho Informático.* (3-3).
- Saín, G. (1994). *Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos.*1994, (43-44). Argentina, Rustica.

AUTORIZACIÓN PARA PUBLICAR Y DIFUNDIRTESIS DE POSGRADO O GRADOA LA UNIVERIDAD SIGLO 21

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

Autor-tesista	BRUNO NICOLAS FRANCISCO
DNI	29577900
Título y subtítulo	LA EVOLUCIÓN TECNOLÓGICA UTILIZADA COMO MEDIO DELICTIVO Y SU LEGISLACIÓN VIGENTE
Correo electrónico	NN_FF_BB@YAHOO.COM.AR
Unidad Académica	Universidad Siglo 21
Datos de edición:	SIN DATOS

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

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

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

Lugar y fecha LA PLATA, BUENOS AIRES, JUNIO 2016

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

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

Firma Autoridad	Aclaración Autoridad

Sello de la Secretaría/Departamento de Posgrado

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