TRABAJO FINAL DE GRADUACIÓN

LA PROTECCIÓN PENAL ANTE EL AVANCE TECNOLÓGICO Y LA DELINCUENCIA CIBERNÉTICA

"Dado el carácter transnacional ¿es suficiente la normativa penal existente para impedir el avance de la ciberdelincuencia?

Jorge Enrique Horianski

VABG48193

ABOGACÍA

AGRADECIMIENTOS

Cuando se llega a este momento, vienen a la mente muchas personas que de alguna u otra manera colaboraron para poder llegar a este logro, personas que con su ayuda desinteresada hicieron posible que alcance una de mis metas más preciadas.

Sé que es imposible nombrar a todas, pero también es verdad que hay otras a los que no puedo dejar de mencionar a mi esposa Graciela que nunca dejó de creer en mí, ella siempre supo que iba a llegar este momento; mis ocho hijos: Mariana, Daniela, Alejandro, Tatiana, Emiliana, Milagros, Graciano y David que vivieron mi experiencia con un gran apoyo, siendo para mí una gran fuerza motivadora; a mis amigos y compañeros de estudio que han cooperado de manera generosa sabiendo que estamos todos juntos en esta misma senda.

Por último, y no por ello menos importante, agradezco a la Universidad que nos ofrece a muchos una oportunidad para cumplir nuestros sueños y a los profesores que son quienes nos transmiten sus conocimientos para que el día de mañana seamos profesionales.

Muchas gracias a todos.

Jorge Enrique Horianski

RESUMEN

LA PROTECCIÓN PENAL ANTE EL PROGRESO DE LA TECNOLOGÍA Y DEL DELITO CIBERNÉTICO.

En el presente Trabajo Final de Graduación, se llevará a cabo una investigación de un nuevo tipo de crímenes nacidos en las últimas décadas del siglo XX que la doctrina los denomina "delitos informáticos".

Para ello buscamos identificar cómo se configura el delito informático, cómo se regula en Argentina e internacionalmente y cuáles son las lagunas que todavía no se han legislado.

Para alcanzar los objetivos establecidos, era necesario conceptualizar los crímenes informáticos, definir el perfil criminológico de quienes cometieron delitos informáticos, caracterizar las particularidades de estos delitos, tipología, activos protegidos, formas, métodos de comisión, características y funciones.

Para encontrar la efectividad de las normas actuales argentinas y extranjeras, fue necesario detectar si existe coherencia entre la jurisprudencia, la doctrina y los escritos profesionales específicos sobre el tema en estudio con las normas vigentes. Por eso se describe si las disposiciones de los instrumentos internacionales, los tratados y los acuerdos regionales son aplicables por los Estados.

Con el conocimiento de los actuales procedimientos penales relacionados con los delitos cibernéticos, se describen las soluciones propuestas por los juristas, ofreciendo posibles remedios legales y prácticas para detener el avance de los cibercrímenes.

Palabras Claves: delito penal – ciberdelitos – efectividad normativa – soluciones – impacto social – seguridad informática.

ABSTRACT

THE CRIMINAL PROTECTION AGAINST THE PROGRESS OF CYBER TECHNOLOGY AND CRIME.

In this present Final Paper Graduation, an investigation of a new type of crimes born in the last decades of the twentieth century that the doctrine denominates "computer crimes" will be carried out.

To this end, we seek to identify how computer crime is configured, how it is regulated in Argentina and internationally, and what are the gaps that have not yet been legislated.

In order to reach the established objectives, it was necessary to conceptualize computer crimes, define the criminological profile of those who committed computer crimes, characterize the particularities of these crimes, typology, protected assets, forms, commission methods, characteristics and functions.

In order to find the effectiveness of current Argentine and foreign norms, it was necessary to detect whether there is coherence between jurisprudence, doctrine and specific professional writings on the subject under study with the current norms. That is why it describes whether the provisions of international instruments, treaties and regional agreements are applicable by States.

With the knowledge of the current criminal procedures related to cyber crimes, the solutions proposed by lawyers are described, offering possible legal remedies and practices to stop the advance of cybercrime.

Keywords: criminal offense - cybercrime - normative effectiveness - solutions - social impact - computer security.

ÍNDICE GENERAL

CONCEPTOS	PAGINA
Agradecimientos.	2
Resumen.	3
Abstract.	4
Índice General.	5
Introducción.	7
Metodología.	9
PRIMERA PARTE: La informatización y el delito.	11
Capítulo I: Introducción al fenómeno informático.	13
I.1: Lineamientos generales del delito informático.	13
I.2: Existencia del delito informático.	15
I.3: El Derecho Informático.	16
Capítulo II: Configuración y características de los ciberdelitos.	18
II.1: Conceptualización doctrinaria.	18
II.2: Caracteres de los delitos informáticos.	19
II.3: Caracterización criminológica de los ciberdelincuentes.	20
II.4: Sujetos intervinientes.	20
II.5: Clasificaciones.	21
SEGUNDA PARTE: Regulación de los crímenes en informática	25
Capítulo III: Regulación de los delitos informáticos en el Derecho Argentino y en el Derecho Comparado.	27
III.1: Delitos informáticos en el Derecho Argentino.	27
III.1.1: Ley de Delitos Informáticos Nº 26.388 y sus implicancias.	28
III.1.2: Ley de Piratería de Software Nº 25.036.	35
III.1.3: Aportes de la Ley de Despenalización de Calumnias e Injurias en Asuntos de Interés Público Nº 26.551 y otras normativas locales relacionadas con delitos informáticos.	37
III.1.4: Principios de aplicación. Las Garantías Constitucionales en el Proceso Penal. Otros recursos.	39
III.1.5: Los ciberdelitos en la Provincia de Córdoba.	42
III.2: Los ciberdelitos en el Derecho Comparado.	42
Capítulo IV: Relación de la normativa argentina con los instrumentos internacionales, doctrina y jurisprudencia.	45
IV.1: Instrumentos Internacionales	46

IV.1.1: Organización para la Cooperación y el Desarrollo Económico (OCDE).	46
IV.1.2: Seminarios Internacionales sobre *"Regionalización del Derecho Penal en el Mercosur"*.	47
IV.1.3: Convención contra la Delincuencia Organizada Trasnacional.	48
IV.1.4: Convenio sobre Cibercriminalidad de Budapest.	48
IV.1.5: Conclusiones de las Naciones Unidas sobre el estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionadas con las redes sociales.	49
IV.2: Doctrina y jurisprudencia sobre delitos informáticos.	49
TERCERA PARTE: Repercusión de la ciberdelincuencia en la sociedad y la justicia. Seguridad informática.	53
Capítulo V: Repercusión social y judicial	55
V.1: Repercusión social	55
V.2: Repercusión judicial	56
V.3: Seguridad Informática.	59
V.3.1: Seguridad contra los delitos informáticos	59
Conclusiones.	62
Glosario de terminología informática.	64
Bibliografía.	68

INTRODUCCIÓN

En los últimos treinta años, el desarrollo de la tecnología informática y su masividad en todas las áreas de la vida del hombre ha llevado a que se convirtiera en un valioso medio de comunicación. Pero su gran influencia abrió las puertas a nuevos ilícitos antes impensados y que se vinculan con los medios electrónicos de datos, la doctrina los denomina *"delitos informáticos"*.

De este modo la informática se convierte en un medio idóneo para la comisión de distintas modalidades delictivas, en especial de carácter patrimonial. La idoneidad proviene básicamente de tres características: a) De la gran cantidad de datos que se acumulan, b) De la comodidad de acceso a ellos y c) De la fácil comunicación de esos datos.

Son cuantiosos los perjuicios que estos ilícitos provocan, alejándose así de las características con que se conocen en la delincuencia tradicional, esta nueva y especial delincuencia oculta a especialistas con una gran capacidad para que su actuar no sea detectado y ahuyentar las posibilidades de encontrar culpables, imposibilitando el modo de ser sancionados.

Las publicaciones relacionadas con crímenes informáticos reflejan entre los más relevantes: manipulaciones fraudulentas a sistemas bancarios y accesos indebidos a informaciones públicas o privadas, obteniendo los delincuentes beneficios económicos con los consiguientes daños morales a sus víctimas.

Vale mencionar que el accionar de los ciberdelincuentes se ampara bajo el mal uso de ordenadores portátiles, teléfonos celulares, agendas digitales, y de toda tecnología actual de alta gama que utiliza redes sociales para las comunicaciones.

Planteado el problema de esta investigación: *"Dado el carácter transnacional ¿es suficiente la normativa penal existente para impedir el avance de la ciberdelincuencia?*, se observan dificultades al momento de resolver ciberdelitos.

Para una mejor comprensión del problema planteado, se identifica la configuración de los delitos informáticos, cómo está regulado en Argentina y a nivel internacional. Para ello se formularon los siguientes objetivos:

- Conceptualizar los delitos informáticos.
- Definir el perfil criminológico de quienes incurren en delitos informáticos.

- Caracterizar las particularidades de estas infracciones penales, tipología, bienes protegidos, formas, medios de comisión, características y funciones.
- Identificar la dificultad para encontrar el posible autor.
- Encontrar la eficacia de las normas argentinas y extranjeras vigentes.
- Detectar si existe coherencia entre jurisprudencia, doctrina y escritos profesionales específicos sobre la materia en estudio con normativas actuales.
- Describir y determinar si resulta aplicable por los Estados lo resuelto en instrumentos internacionales, tratados y convenios regionales.
- Conocer los procedimientos penales actuales vinculados con ciberdelitos y describir soluciones propuestas por juristas.
- Brindar posibles remedios jurídicos y practicidades para detener el avance de la ciberdelincuencia.

METODOLOGÍA

Para lograr los objetivos de la investigación, primeramente, se llevó a cabo la elección del tema a desarrollar, buscando que sea novedoso. Para ello se seleccionaron datos, normativas, instrumentos internacionales, doctrina y jurisprudencia, para verificar que su realización fuera viable.

Luego se trazaron los objetivos a que se aspiraba alcanzar, trazando un plan de acción para lograrlos. Teniendo en cuenta cuál es el enfoque que se le brindará al tema, quiénes son los destinatarios de su lectura y cuál es el fin del trabajo.

Se construye un esquema jerárquico que permita obtener las pautas del diseño de trabajo. Por ello el tipo de estudio será *"descriptivo"*, para delinear los contornos de los delitos informáticos, los estudios descriptivos lograron especificar propiedades, características, perfiles, procesos, objetos y otros fenómenos surgidos en la tarea.

La estrategia utilizada es *"cualitativa"*, por llevar adelante la investigación un proceso inductivo y de análisis desde la perspectiva de la realidad subjetiva, para contextualizar el fenómeno delictivo en los sistemas informáticos. Esta estrategia dirigió la exploración, descripción y entendimiento de los fenómenos encontrados.

Como plan de acción con respecto a la organización de la literatura encontrada, se dividió el trabajo en Partes y Capítulos, para facilitar su lectura y localización de temas.

Las conclusiones se realizaron conforme a los objetivos trazados en el inicio de la investigación, teniendo en cuenta la biblioteca encontrada sobre literatura en delitos informáticos.

Para entender la terminología utilizada en diversos documentos propios de los ciberdelitos, se acompaña un Glosario de terminología informático.

Es necesario destacar que como *"delimitación temporal"* se tomará como punto de partida el año 1980, ya que en la década de los años ochenta se conocen las primeras manifestaciones relacionadas con ciberdelitos. Los *"niveles de análisis"* comprenderán toda bibliografía disponible al respecto de normativas, doctrina y jurisprudencia.

Cabe mencionar que este trabajo investigativo fue consultado principalmente de la BIBLIOTECA VIRTUAL eBook21 de la Universidad Siglo 21, de la Biblioteca de la

Universidad Nacional de La Pampa, de la Biblioteca del Superior Tribunal de Justicia de la Provincia de La Pampa y de sitios web disponibles.

PRIMERA PARTE: La informatización y el delito.

Para responder a la problemática planteada y por haber desconocido inicialmente el origen de los ciberdelitos y su incidencia en los usuarios de medios electrónicos de información, considero pertinente desarrollar esta Primera Parte con una introducción al fenómeno informático, su configuración y características de los ciberdelitos.

Porque si revisamos la historia del hombre, éste siempre precisó conservar y a la vez transmitir información relacionada con su vida y sus actividades, pasando así por medios muy primitivos y rudimentarios, hasta llegar a la actual tecnología de medios electrónicos de procesamiento de datos.

Hernández, A. (2006) en su obra *"Delitos Informáticos"* destaca:

> Motivados por la necesidad de encontrar mecanismos de acceso fácil y rápido, el mismo hombre fue creando métodos para procesar información. Con este fin nace la informática, como ciencia encargada del estudio y desarrollo de estas máquinas y métodos, con la idea de apoyo en aquellos trabajos rutinarios y repetitivos.

Con el nacimiento de internet los actores sociales de todo el planeta encaminan sus actividades con el uso de esta innovadora tecnología, enriqueciéndose con sus beneficios la cultura, la ciencia, instituciones públicas y privadas.

Actualmente, las computadoras personales dejaron de usarse como herramienta auxiliar para realizar distintas actividades de la vida humana, convirtiéndose en el medio principal y más eficaz para obtener, procesar, almacenar y transmitir información de diversos tipos.

Las tareas ejecutadas manualmente fueron reemplazadas casi por completo por los sistemas de información. Antes del nacimiento de la informatización automática de datos el esfuerzo humano era fundamental y las máquinas cumplían un rol complementario.

Los sistemas de operación fueron convirtiéndose más sencillos y se requieren menos conocimientos técnicos para operarlos, lo que amplió considerablemente el rango de edad de los usuarios de estos sistemas.

La informática y el proceso de informatización aún no ha llegado a su techo, al contrario, la perspectiva de avances crece imprevisiblemente, los mismos partícipes de este proceso se impresionan de estos avances.

Pero este panorama de avances cibernéticos permitió un cuadro de posibilidades lícitas e ilícitas, que necesitó la regulación jurídica de los variados efectos de esta nueva situación. Y nuestro país no es ajeno a estos cambios que provocó la tecnología, tampoco acompañó en el tiempo oportuno este proceso tan dinámico.

Pero la revolución tecnológica de los medios electrónicos y su contrapartida denominada delitos informáticos, produjo importantes cuestionamientos en el sistema penal mundial, acostumbrado a tipologías tradicionales que por lo general se las relacionaban con la clase baja. Los ciberdelitos se ven potenciados por características especiales y profesionales.

CAPITULO I: Introducción al fenómeno informático.

El Capítulo I realiza una aproximación al fenómeno de los delitos cibernéticos, caracterizando sus lineamientos generales, analizando la existencia de tales delitos y el rol que corresponde al Derecho Informático en cuanto al estudio de normas y principios vinculados con la delincuencia informática.

I.1: Lineamientos generales del delito informático.

No se podría llegar a conclusiones válidas con el presente trabajo si no delimitan a priori características de los ciberdelitos, y a partir de allí relacionarlos con la normativa penal local principalmente y su vinculación con las normas internacionales.

Los modos de delinquir de la delincuencia tradicional se modifican según corren los tiempos, pero sorprende considerablemente que el progreso en la tecnología informática trae aparejado nuevos ilícitos antes no tipificados en los ordenamientos jurídicos.

Ante este panorama delincuencial se debaten los mecanismos para impedir el avance de los cibercrímenes, imprimiendo su discusión en: 1) La necesidad o no de distinguir estos delitos del resto de los delitos, 2) Qué bienes debe tutelar el Estado para ofrecer su protección y 3) La correcta tipificación de los nuevos ilícitos.

Ello conlleva a tener presente si se debe cimentar su estudio en un "numerus clausus" de delitos de manera taxativa o no, teniendo en cuenta la constante evolución y transformaciones permanentes en el mundo de la informática, que trae consigo nuevas ópticas en donde los delincuentes perfeccionan sus procedimientos para delinquir.

La doctrina siempre atenta a los devenires de la sociedad y a la actuación del derecho para impartir justicia, fue elaborando conceptualizaciones acerca de las infracciones cometidas a través de medios electrónicos de datos, impartiendo conceptos según las concepciones de los diversos doctrinarios. Así, se encuentran denominaciones tales como *"delitos electrónicos", "delitos informáticos", "delitos de cuello blanco",* etc.

Como puede observarse enfrentar a los delitos informáticos es un trabajo difícil, donde se necesita considerar varios aspectos, ya que estos ilícitos traspasan las fronteras locales y requieren: 1) Armonizar las legislaciones, 2) Modificar las reglas del Derecho Penal, 3)

Implementar procedimientos penales acordes a las nuevas modalidades de delinquir de los ciberdelincuentes.

Parecería que el modo de trabajo para solucionar todos estos inconvenientes que surgen de la ciberdelincuencia, es llevarlo a cabo mediante la elaboración de un sistema penal que contenga homogeneidad, principios y garantías fundamentales, como así también conceptos y categorías propias de los delitos informáticos.

El Ministerio Público Fiscal de Córdoba[1] caracteriza a los delitos informáticos de la siguiente manera:

> Desde hace unos años se viene observando un fuerte aumento en el uso de las tecnologías de la información y comunicación (TIC) en el mundo y, particularmente en la República Argentina, lo cual tiene como característica principal la afectación en todos los ámbitos de la actuación de los seres humanos y de las infraestructuras críticas (Estado, salud, comunicaciones, transporte, etc.).
>
> En este crecimiento, se suma la fácil accesibilidad en el alcance de la tecnología, y por consiguiente ante la necesidad de que las personas se comuniquen, aumenta la tendencia al uso de herramientas tecnológicas, como correos electrónicos, redes sociales, etc., lo que a su vez refleja un mayor incremento en el manejo de internet en la vida cotidiana.
>
> La utilización de internet, presenta entre otras características, la de ofrecer a una indeterminada cantidad de personas el anonimato para realizar infinidad de tareas.
>
> Es así, que la "gran red de comunicación interconectada", pone al alcance de los usuarios innumerables instrumentos; sólo que algunas personas los utilizan en forma indebida, fraudulenta o con fines no convencionales que perturban la paz social, es decir, en contra del buen uso del resto de los usuarios.
>
> Con el desembarco de la informática en la vida de las personas, el Derecho tuvo que evolucionar para regular y proteger la información y los dispositivos.
>
> En cuanto a la informática como objeto de estudio, es a través del "Derecho Informático", donde se aplican las reglas jurídicas con los problemas vinculados con la tecnología o la informática.
>
> Hoy, existe un área relacionada con el derecho penal, que consiste en el estudio de aquellas conductas donde la informática y la tecnología de la información, desempeñan un papel fundamental como medio para la comisión de un ilícito.

[1] Ministerio Público Fiscal de Córdoba: http//www.mpfcordoba.gob.ar/delitos-informaticos/

En la actualidad, el espectro de las acciones ilícitas se va acrecentando, poniéndose de manifiesto en la comisión de diferentes delitos que son cometidos por medios informáticos: ej. fraudes, obtención no autorizada de datos, pornografía infantil con la producción y su distribución, grooming, etc.

Estos tipos de ilícitos son los denominados: Delitos Informáticos, Delitos Cibernéticos o Cibercrímenes.

I.2: Existencia del delito informático.

En la doctrina se suscitan divergencias respecto de la concepción de ciertos conceptos, principios o la adopción de criterios para identificar institutos legales con sus respectivas normativas jurídicas.

Con los primeros ilícitos cometidos por ciberdelincuentes, los Estados mostraron su preocupación y desorientación al momento de penalizar los mismos, existiendo una desprotección legal para sus víctimas, porque no existían bienes jurídicos informáticos a tutelar, por lo tanto, tampoco tipología que los penalice.

No existía una rama del derecho dedicada al estudio de estos delitos, surgiendo de un modo incipiente lo que los doctrinarios llaman *"Derecho Informático"*. Los más afectados son aquellos estados más poderosos, que sintieron violados sus secretos de estado, tecnológicos o bancarios (EEUU, Alemania, Reino Unido, entre otros).

Costa Hoevel, S. A. (2006) en su artículo publicado en el portal *Justiniano.com* sobre *"Delitos informáticos. Aspectos jurídico-penales a la luz de la Teoría del Delito"* postula lo siguiente:

> Existen varias teorías que niegan la existencia de los delitos informáticos. Aún, luego de su regulación en los códigos penales o leyes especiales, como el caso de España, un gran sector de la doctrina ius-penalista, considera incluso inadecuada hablar de la existencia, como del nomen iuris de "delito informático".
>
> Este sector de la doctrina, sostiene que por imperio del Principio de Legalidad y el de Reserva de la Ley, ambos con raigambre constitucional en la mayoría de los sistemas jurídicos del mundo, no pueden penalizarse conductas que atenten contra supuestos bienes jurídicos que no se encuentran protegidos o que no contengan la categoría de tales, y que no habiendo ley que tipifique una conducta delictiva relacionada con la informática como bien jurídico específico, no existe delito ni pena para dichas conductas. También desechan el Principio de la Analogía de la Teoría General del Delito para aplicarlos a esta clase de delitos.

> Existen otras posturas –que podrían ser de carácter intermedio– que entienden que debe existir algún tipo de protección contra dichas conductas, o más bien, una ampliación en la interpretación sobre ciertas conductas antijurídicas ya tipificadas, en base a las modalidades perpetradas utilizando sistemas tecnológicos avanzados como los sistemas informáticos o telemáticos.
>
> Creemos que, en la actualidad, es innegable la existencia de delitos cometidos mediante el uso de sistemas informáticos. Más aún, mediante el análisis de las normativas existentes en el derecho comparado, de donde surge la necesidad de estructurar un nuevo bien jurídico digno de tutela jurídica-penal, que entendemos y sostenemos que se trata de la "información" en todas sus etapas, la cual conlleva en sí un valor, ya sea económico, ideal o de empresa, que es relevante y digno de tutela jurídico-penal.

Ante el análisis de Costa Hoevel (2006) y la realidad de los ciberdelitos, puedo afirmar que no se pueden negar estos delitos y que es prioritaria la necesidad de regulación penal.

I.3: El Derecho Informático.

No conociendo con precisión acerca de la existencia y el rol del Derecho Informático, urgía conocerlo para vincularlo con los ciberdelitos y si sus estudios científicos son de utilidad para resolver crímenes cibernéticos.

La Universidad Laica de Eloy Alfaro de Manabí (Ecuador, 2014) en su publicación *"Derecho Informático y Delito Informático"* afirma que *"aún no existe un consenso general acerca de la existencia del Derecho Informático, principalmente porque se duda de su Autonomía Científica, ya que para afirmar la misma es importante encuadrarla dentro de un objeto específico, con contenidos y métodos propios".*

Se puede precisar que en la actualidad el Derecho Informático se encuentra en permanente evolución y que no es específico en sí mismo, porque se ve involucrado por todas las ramas del derecho (Derecho Penal, Derecho Civil y Comercial, Derecho Internacional), modificando los procesos sociales, políticos y jurídicos.

El Derecho Informático trata de *"principios y normas que regulan la actividad informática y las vicisitudes que trae aparejada la misma, tutelando bienes que merecen protección estatal y sancionando conductas tipificadas penalmente"*[2].

La caracterización del Derecho Informático contiene las siguientes aristas:

[2] UNIVERSIDAD LAICA DE ELOY ALFARO DE MANABI (2014). *Derecho Informático y Delito Informático.* Publicación del 23 de octubre de 2014 y recuperada el 12/08/2016 de: https://www.jeanvilla.wordpress.com/2014/10/23/derecho-informatico-y-delito-informatico/

– ***Autonomía del Derecho Informático:***

Para hablar de la misma se precisa la existencia de una legislación específica, un estudio particularizado de la materia, investigaciones, doctrinas e instituciones propias para su tratamiento.

Piña Libien (2010) dice que quienes "*defienden su autonomía" afirman que existe legislación específica basada en leyes, tratados y convenios que protegen al campo informático mediante un campo normativo; además se dispone de instituciones propias que no se encuentran en otras ramas del derecho.*

Por otra parte quienes *"niegan su autonomía"*[3] sostienen que en cada rama del derecho la actividad informática se encuentra presente, rechazando la integración de normas en un cuerpo específico, considerando también que no posee un área jurídica de influencia y que el Derecho Informático recurre a los principios jurídicos de otras ramas para la solución de casos concretos.

– ***Objeto del Derecho Informático:***

Salmerón, A. (2015) en su artículo *"Derecho Informático"* publicado en el portal *Informática Forense y Pericial*, nos dice que:

> El objeto está constituido por la tecnología del hardware y del software con sus implicancias económicas, sociales, culturales y políticas frente a las que el derecho ha de reglamentar, pues es el derecho la principal forma de organizar la vida social y la informática incide ya en casi todos los aspectos sociales.

– ***Método científico del Derecho Informático:***

Siguiendo a Salmerón, A. (2015), interpreta respecto de la metodología específica que:

> Para abordar adecuadamente esta disciplina jurídica se ha de tener en cuenta que: a) La reglamentación jurídica de la informática debe adaptarse a la situación de constantes cambios e innovaciones que caracterizan esta tecnología, por ello, es conveniente que su disciplina normativa responda a unos principios generales para disminuir la necesidad de introducir variaciones constantes en las normas y permitir a los órganos encargados de su aplicación adoptar los principios a las situaciones que sucesivamente se presenten. b) La informática y la telecomunicación rebasan los límites de los Estados, baste pensar que para muchos delitos en internet ya no hay fronteras, y por ello el Derecho de la

[3] Piña Libien, H.R. (2010). *El Derecho Informático y su autonomía como nueva rama del derecho".* Publicación recuperada el 08/09/2016 de: http://ordenjuridico.gob.mx/Congreso/pdf/78.pdf

Informática debe concebirse casi como un Derecho internacional. c) El Derecho Informático rebasa los términos de la dicotomía entre el Derecho público y el Derecho privado siendo esta interdisciplinariedad uno de sus rasgos característicos.

– ***Contenidos del Derecho Informático:*** considerando el aporte de quienes aceptan la autonomía del Derecho Informático, se puede afirmar que los contenidos del Derecho Informático permiten obtener soluciones legales propias de los problemas que se generan por el uso en la sociedad de la tecnología informática; para ello los ordenamientos jurídicos de los estados introducen mecanismos técnicos a esas soluciones legales, de modo tal que aseguren las operaciones a través de medios electrónicos, tal es el caso de la "criptología", "firma digital", etc.

En definitiva, el Derecho Informático es de suma utilidad cuando se analizan delitos relacionados con la informática, porque se nutre científicamente de: conceptos, normas, doctrina, jurisprudencia, etc. y busca elaborar soluciones conforme a derecho, ya que como se dijo anteriormente se ven involucradas todas las ramas del derecho y trasvasa al derecho público y privado.

CAPITULO II: Configuración y características de los ciberdelitos.

El Capítulo II versará puntualmente sobre uno de los objetivos de esta Primera Parte y que es la configuración del delito informático, delineando las características que lo componen y diferencian de los delitos tradicionales; para el logro de este objetivo se recurre a las conceptualizaciones doctrinarias, caracteres de estos delitos, sujetos intervinientes y clasificaciones teóricas que nos ubican dentro de los ciberdelitos, ya que en la comisión de estos delitos existen variaciones tanto en el perjuicio que producen como las formas de cometerlos.

II.1: Conceptualización doctrinaria.

Julio Téllez Valdez (1996) conceptualiza al delito informático en forma típica y atípica, entendiendo a la **primera** como *"las conductas típicas, antijurídicas y culpables, en las que se tienen a las computadoras como instrumento o fin"*, y por la **segunda** como *"actitudes ilícitas en que se tienen a las computadoras como instrumento"*.

Gustavo Arocena (2008) brinda un concepto técnico-jurídico diciendo que:

El delito informático o cibernético es el injusto determinado en sus elementos por el tipo de la ley penal, conminado con pena y por que el autor merece un reproche de culpabilidad, que, utilizando a los sistemas informáticos como medio comisivo o teniendo a aquellos, en parte o en todo, como su objeto, se vinculan con el tratamiento automático de datos.

María de la Luz Lima (1984) dice que:

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

Las conceptualizaciones doctrinarias son variadas, pero en general y dejando de lado la redacción de esos conceptos, coinciden en que se trata de un delito, en el que se debe verificar una conducta humana que merece ser penada y que el autor posee las condiciones personales y específicas de los delitos informáticos para imputarle dicha conducta. Se trata de delitos especiales donde al autor no puede ser cualquier sujeto, ya que está limitado a ciertas características específicas de autor especial o cualificado que requiere los siguientes criterios de imputación objetiva: a) posibilidad objetiva del dominio de la propia acción y b) el dominio del hecho.

II.2: Caracteres de los delitos informáticos.

El delito informático presenta caracteres que lo diferencian plenamente de cualquier delito.

Téllez Valdéz, J. (2010) desarrolla en forma específica las siguientes características:

a) ***Especialidad:*** Condiciones personales y especiales del autor.

b) ***Cuantía:*** Cuantía de perjuicios económicos y daños.

c) ***Delito de cuello blanco:*** Cometido por determinadas personas con conocimientos técnicos.

d) ***Ocupacional:*** Son acciones ocupacionales cometidas cuando el actor se encuentra trabajando.

e) ***Oportunidad:*** Los sujetos crean la ocasión propicia para delinquir.

f) ***Amplitud:*** En tiempo y espacio, delinquen en milésimas de segundos y sin necesidad de presencia física.

g) ***Impunidad:*** Pocas denuncias y casos por la falta de regulación.

h) ***Proliferación:*** evolucionan rápidamente los delitos.

i) ***Trasnacionalidad:*** por trasladarse vía internet de un país a otro.

II.3: Caracterización criminológica de los ciberdelincuentes.

Mesegger González, J. de D. (2013), sostiene *"que quienes operan los sistemas informáticos para cometer delitos poseen características especiales y únicas, por lo que es necesario conocerlas para evitar posibles infracciones, ya que ingresan a los ordenadores y redes y provocan daños y perjuicios económicos importantes".*

Algunos autores distinguen en varias conceptualizaciones el perfil de los piratas informáticos, las más conocidas son:

◊ ***Hacker:*** Persona que disfruta husmear los sistemas programables, es un delincuente silencioso y tecnológico, son capaces de crear sus propios softwares para entrar a los sistemas, no pretende producir daños e incluso se apoya en un código ético, aunque el mero hecho de colocarse en un sistema ya es delito.

◊ ***Cracker:*** es aquel que rompe con la seguridad de un sistema con la intención de destruir datos, denegando el servicio a usuarios legítimos, es sinónimo de rotura.

◊ ***Phreacker:*** es el especialista en telefonía, arte y ciencia del sujeto para obtener beneficios personales, necesita conocimientos sobre informática, ya que la telefonía celular o el control de centralitas emplea informática.

El hacker en general utiliza reglas gramaticales y particulares, juega y crea un lenguaje propio con la intención de confundir y diferenciarse para obtener así cierto poder. Detrás de un hacker adolescente hay un autodidacta, se autoconsidera su mejor motivación, aunque a veces es motivado por otro hacker.

Las características de los ciberdelincuentes sobresalen por su alto coeficiente intelectual, su curiosidad y facilidad para las abstracciones intelectuales, son individualistas y anticonformistas. Tienen habilidad mental para retener gran cantidad de detalles, que luego incluirán en un contexto para su fin.

II.4: Sujetos intervinientes.

1) ***Sujeto Activo:*** el apartado anterior (II.3) aproxima a la caracterización del ciberdelincuente, esto conduce a definir al sujeto activo como una *persona física*, diferenciándose de otros delincuentes por la propia naturaleza de los ilícitos que cometen.

Sin embargo esta postura relacionada con el sujeto activo que se trata de una persona física, sienta un importante precedente en EEUU en el año 2001 a raíz del caso "Napster"[4], donde se penaliza a *una persona jurídica*, en este caso la Corte de Apelaciones de San Francisco (EEUU) responsabilizó indirectamente a la empresa Napster por violar derechos de autor, ya que disponía de los medios técnicos para que miles de personas violasen las leyes de copyright (derecho de autor).

2) ***Sujeto pasivo:*** es el ente que sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, mediante el sujeto pasivo se conocen los ilícitos cometidos por los delincuentes informáticos.

Muchos delitos informáticos son desconocidos por sus víctimas, por tal motivo la verdadera dimensión de estos delitos hace difícil su investigación, ya que la mayoría de ese tipo de ilícitos, no son descubiertos o no son denunciados a las autoridades correspondientes.

Por eso, el sujeto pasivo tiene un rol determinante, porque en muchos casos las víctimas son las únicas que pueden brindar datos fundamentales que permiten comenzar con la investigación y hasta descubrir al autor.

Se puede también destacar la tendencia a la victimización masiva, es decir causada por este tipo de delitos, como por ejemplo la propagación de virus, ya que el número de víctimas es demasiado grande.

II.5: Clasificaciones.

Resulta complicado realizar una clasificación clara y ordenada de los delitos informáticos, porque no se conoce un *numerus clausus* de las conductas típicas, antijurídicas y culpables.

Existen diversas clasificaciones de los delitos informáticos, se pueden encontrar desde un punto de vista doctrinario y también legislativo, pero es destacable la clasificación que presenta el Convenio sobre Ciberdelincuencia de Budapest[5], este convenio es el único instrumento internacional que cubre todas las áreas relevantes de la legislación sobre

[4] Corte Federal de Apelaciones del 9º Circuito de los EEUU (12/02/2001). *"RIAA vs. Nasper Inc. s/violación de derechos de autor y asociación ilícita.* San Francisco, EEUU.

[5] Convenio sobre Cibercriminalidad de Budapest. Recuperado el 06/05/2016 de: http://www.coe.int/t/dghl/cooperation/econoccrime/Source/Cybercrime/TCY/ETS_185_spaish.PDF

ciberdelincuencia (Derecho Penal, Procesal y Cooperación Internacional). La Argentina adhiere al Convenio en el año 2010.

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los actos y los sistemas informáticos.

1.1. *Acceso ilícito:* Acceso que infringe medidas de seguridad, con la intención de obtener datos informaticos.

1.2. *Interceptación ilícita:* Interceptación deliberada e ilegítima mediante medios técnicos, de datos informaticos comunicados en transmisiones no públicas efectuadas a un sistema informático.

1.3. *Interferencia en los datos:* Comisión deliberada e ilegítima de actos que dañen, borren, deterioren o supriman datos informáticos.

1.4. *Interferencia en el sistema:* Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático.

1.5. *Abuso de dispositivos:* Comisión deliberada e ilegítima de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo.

2. Delitos informáticos.

2.1. *Falsificación informática:* Comisión deliberada e ilegítima de la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de usarlos como auténticos.

2.2. *Fraude informático:* Actos deliberados e ilegítimos que causen perjuicio patrimonial, mediante introducción, alteración, borrado o supresión de datos informáticos de un sistema informático.

3. Delitos relacionados con el contenido.

3.1. *Delitos relacionados con la pornografía infantil:* Comisión deliberada e ilegítima de producción de pornografía infantil con vistas a su difusión por medio de un sistema informático.

4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

4.1. *Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines:* Infracciones de la propiedad intelectual, de conformidad con las obligaciones asumidas por el Convenio de Berna para la protección de las obras literarias y artísticas, el Tratado de la OMPI sobre propiedad intelectual, y el Convenio de Roma.

Siguiendo la postura de Téllez Valdez (1996), clasifica los delitos informáticos *"Según el uso del sistema informático"* y sigue dos criterios:

> **1. Como instrumento o medio:** Se valen de las computadoras como método y/o medio para la comisión del ilícito.
>
> Este criterio incluye los siguientes delitos: Falsificación de documentos vía computarizada, Variación de los activos y pasivos en la situación contable de las empresas, Planeamiento y simulación de delitos convencionales, lectura, sustracción o copiado de información confidencial, Modificación de datos tanto en la entrada como en la salida, Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas, Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, Uso no autorizado de programas de cómputo, Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas, Alteración en el funcionamiento de los sistemas a través de virus informáticos, Intervención en las líneas de comunicaciones de datos o teleproceso, Obtención de información residual impresa en papel luego de la ejecución de trabajos, Acceso a áreas informatizadas en forma no autorizada.
>
> **2. Como fin u objetivo:** Dirigida en contra de las computadoras, accesorios o programas como entidad física.
>
> Este criterio incluye: Programación de instrucciones que producen un bloqueo total al sistema, Destrucción de programas por cualquier método, Daño a la memoria, Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurológicos computarizados, Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje, Atentado físico contra la máquina o sus accesorios.

Otros doctrinarios clasifican *"Según el uso de la red"*, incluyendo la comisión de los siguientes delitos: Espionaje, Terrorismo y Narcotráfico.

Otras clasificaciones se realizan conforme al *"Bien jurídico o interés tutelado"*: Hurto, Estafa, Falsedades Documentales, como así también aquellos delitos *"Contra el patrimonio"*, en esta última clasificación se puede decir que la mayoría de los delitos informáticos vulneran

el patrimonio, como los que se concretan a través de cajeros automáticos, desviación de dinero a ciertas cuentas bancarias o extorsiones informáticas.

Dentro de los delitos contra el patrimonio se incluyen aquellos contra la propiedad, como la introducción de virus informáticos que afectan cosas muebles o inmuebles, el inconveniente suscita con respecto al software que es un bien intangible, o contra la propiedad intelectual, que abarca la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos.

SEGUNDA PARTE: Regulación de los crímenes en informática.

En esta Segunda Parte se abordarán primeramente los cambios en la regulación penal argentina, analizando leyes vigentes que sancionan delitos informáticos, la adaptación que requiere el derecho procesal penal dentro del marco constitucional. Se tendrá en cuenta en este abordaje los principios y garantías procesales y constitucionales.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa de 2001 surgió a partir de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger la sociedad frente a la ciberdelincuencia, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional.

La Argentina adhiere al Convenio en 2010, y si bien con anterioridad a este Convenio se habían firmado distintos documentos internacionales (estudio para la armonización de leyes penales OCDE de 1983, directrices del Consejo de Europa en 1989, 8° Congreso de Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente realizado en 1990), éste marca un hito en cuanto al esfuerzo por armonizar las distintas regulaciones penales de los estados.

Tratándose el presente trabajo de un análisis local, pero con la mirada de la evolución internacional, se acompañarán a este estudio de regulación de los crímenes en informática las opiniones de doctrinarios y las sentencias dictadas por distintos tribunales de la justicia nacional y mundial.

Se observó en la doctrina opiniones a favor y en contra respecto del modo en que se fueron encausando los delitos informáticos dentro de los ordenamientos jurídicos estatales, y cierto escepticismo en cuanto a la concreción de medidas legales que detengan los cibercrímenes.

Las sentencias judiciales fueron cambiando sus decisiones, ya que ante los primeros casos de procesos relacionados con crímenes informáticos fueron solucionándolos de acuerdo a los medios legales disponibles, con el devenir de los cambios en materia penal y procesal informática, los fallos judiciales adquirieron otra mirada a estas cuestiones penales.

Si bien existe actualmente regulación de los cibercrímenes, se observa la ausencia de consenso acerca de una definición jurídica de la conducta delictiva, la falta de conocimientos técnicos por parte de las autoridades de aplicación de la ley, la inadecuación de las facultades

legales de investigación, la falta de armonización de los procedimientos de investigación y la ausencia de tratados de extradición y asistencia recíproca, entre otros.

CAPITULO III: Regulación de los delitos informáticos en el Derecho Argentino y en el Derecho Comparado.

El Capítulo III comprende la parte esencial de esta investigación, porque conforme a la normativa argentina y al Derecho Comparado, se podrá responder a la pregunta planteada en esta investigación, permitiendo tener una visión actual del tratamiento de los delitos cibernéticos y diseñar un diagnóstico jurídico en materia de cibercriminalidad.

Doctrinarios argentinos, entre ellos Arocena (2008), consideran que la normativa penal relacionada con la ciberdelincuencia, se encuentra bien cimentada por reunir procedimientos legislativos prolijos y de acuerdo a la realidad local e internacional, pero que su actualización debería ser permanente teniendo en cuenta las directivas de instrumentos internacionales.

El tratamiento de normas penales o de cualquier otro tipo de normas implica una metodología que permita subsanar las lagunas normativas existentes, omitir esta perspectiva haría fracasar los intentos de solucionarlas.

Por eso, y recordando los trabajos llevados a cabo por Alchourrón y Bulygin[6], el Derecho y en este caso el Derecho Penal sancionatorio de los delitos informáticos debe ser un sistema normativo de enunciados con consecuencias lógicas.

Alchourrón y Bulygin consideran que el sistema normativo debe ser diseñado para un Universo de Casos y con un Universo de Soluciones. Por lo tanto, dicho sistema normativo es *incompleto* si tiene por lo menos una laguna, es *incoherente* si figuran dos o más soluciones diferentes y es *redundante* si la misma solución figura más de una vez en la misma línea.

En las conclusiones de esta investigación se afirmará cuál es el estado de las normas penales cibernéticas a nivel local principalmente y en el derecho comparado.

III.1: Delitos informáticos en el Derecho Argentino.

El ordenamiento jurídico argentino fue adaptando paulatinamente su normativa ante el devenir de los crímenes cibernéticos, sancionándose entre las leyes más importantes: Ley de Delitos Informáticos Nº 26.388, Ley de Piratería Nº 25.036, Ley de Despenalización de

[6] Alchurrón, Carlos y Bulygin, Eugenio, Introducción a la metodología de las ciencias jurídicas y sociales. Astrea, Buenos Aires 1998 (Introducción y Capítulo 1: Un modelo para los sistemas normativos).

Calumnias e Injurias Nº 26.551, el mismo Código Civil y Comercial (CCC)[7] dentro de la aparición de la informática en el terreno jurídico, ha desarrollado su regulación principalmente en el área contractual. La Constitución Nacional Argentina (CN)[8] enmarca la constitucionalidad en el tratamiento de estos ilícitos mediante principios y garantías constitucionales, acompañados por los principios procesales rectores de todo proceso judicial.

Al sancionarse nuevas normas penales que regulen los delitos informáticos, el legislador consideró el *"Principio de Subsidiaridad"* del Derecho Penal, sobre este principio Luzón Peña (1999) asevera:

> Según el principio de subsidiaridad –también denominado entre nosotros (…) *"principio de intervención mínima* – derivado directamente del de necesidad, el Derecho Penal ha de ser la *"última ratio",* el último recurso al que hay que acudir a falta de otros menos lesivos, pues si la protección de la sociedad y los ciudadanos puede conseguirse en ciertos casos con medios menos lesivos y graves que los penales, no es preciso ni se debe utilizar éstos.

Teniendo en cuenta este principio se justifica la intervención del Derecho Penal, cuando la protección de los bienes jurídicos por parte de las otras ramas del derecho resulte insuficiente para asegurar la defensa de aquellos.

III.1.1: Ley de Delitos Informáticos Nº 26.388 y sus implicancias.

Esta ley es sancionada el 4 de junio de 2008, produciendo cambios profundos en el Código Penal, absorbiendo modalidades delictivas relacionadas con la informática. Para su redacción se utilizó el *"criterio desconcentrado"*, esto implica normativizar figuras delictivas en los diversos títulos del Libro Segundo del Código Penal (CP)[9]. Con la aplicación del criterio desconcentrado no se encuentra un solo *"bien jurídico"* amparado sino varios, en virtud de la necesidad de tutelar variados bienes jurídicos ante los nuevos delitos informáticos.

De este modo Argentina armoniza su legislación basado en el Convenio sobre Cibercriminalidad de Budapest y con la de varios de los miembros regionales del Mercosur.

[7] Código Civil y Comercial Comentado. Tratado Exegético. Alterini, J. H. Director General (2015). Tomos I al XI.
[8] Constitución de la Nación Argentina Comentada y Concordada. Tomo I y II. Gelli, M. A. (2008). (4ª Ed. 2008). 1ª Reimpresión 2008). Buenos Aires: La Ley.
[9] Código Penal Comentado Anotado con Jurisprudencia. Dayenoff, D. A. (2010). (10ª Ed. 2010). Buenos Aires: García Alonso.

Siguiendo la técnica de análisis sobre la Ley Nº 26.388 que brinda Arocena (2008), se destaca lo siguiente:

- ***Modifica el Artículo 77 del CP – Incorporando los siguientes términos:***

– *Documento:* Toda representación de actos o hechos con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

– *Firma y suscripción:* Comprende la firma digital, la creación de una firma digital o firmar digitalmente.

– *Instrumento privado y certificado:* Documento digital firmado digitalmente.

- ***Sustituye el Artículo 128 del CP – Delitos contra la integridad sexual:*** Tipifica *figuras o conductas típicas* orientadas a la *Indemnidad Sexual de los Menores de 18 años*. El artículo es consecuente con el *Protocolo Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía de la ONU de 1989,* como así también lo establecido por el Convenio de Cibercriminalidad de Budapest. Los cambios son:

– *Primer Párrafo, primera hipótesis:* Sanciona las *conductas típicas* de producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir material pornográfico. Con estas acciones se el delito se *consuma.*

En esta primera hipótesis consagra un delito de acción, de resultado instantáneo y de pluralidad de actos, mixto alternativo; habla de la expresión *por cualquier medio,* es decir que basta cualquier conducta que cause el resultado típico.

El objeto *material* del delito son representaciones (dibujos, imágenes, fotografías, etc.) que se apoyan en un soporte físico informático.

El *tipo subjetivo* es doloso, admitiendo el eventual. El *sujeto activo* puede ser cualquier persona, mientras que el *sujeto pasivo* es una persona menor de 18 años. Es admisible la *tentativa.*

– *Primer Párrafo, segunda hipótesis:* Sanciona el *comportamiento típico* de quien facilitare el acceso a espectáculo o suministrare material pornográfico en que participen menores de 18 años.

Es una figura que no fue incorporada por la Ley Nº 26.388, ya que estaba prevista en la Ley Nº 25.087 y no parece incluir algún elemento que vincule con criminalidad informática.

– *Segundo Párrafo:* Sanciona el *comportamiento típico* de tener en su poder representaciones de las descriptas anteriormente, constituye un delito de tenencia de objetos bajo el poder del agente.

El *objeto material* del delito son las representaciones de menores de 18 años utilizando soportes físicos o en uno magnético.

El *tipo subjetivo* solo es compatible con el dolo directo; el *sujeto activo* es cualquier persona, mientras que el *sujeto pasivo* solo puede ser un menor de 18 años; el delito se consuma cuando comienza la tenencia. La figura por su carácter de delito de tenencia, no admite la *tentativa.*

– *Tercer Párrafo:* Relacionado con el análisis realizado con el Primer Párrafo, sólo se diferencia que aquí se trata de menores de 14 años.

➢ ***Sustituye el epígrafe del Capítulo III del Título V del Libro II del CP – Violación de Secretos y de la Privacidad:*** Es importante la modificación ya que incluye a la *privacidad como bien jurídico protegido,* defendiendo en definitiva el *bien jurídico "libertad".*

Ciertos juristas han equiparado las nociones de *"intimidad y privacidad",* sin embargo, es pertinente la separación de estos conceptos, surge como elemental derivación del principio interpretativo de que *donde la distingue, el intérprete debe distinguir.*

Son dos nociones que merecen clara diferenciación, siguiendo a Nino (2010), *"…el bien de la privacidad se relaciona con el derecho que tienen los ciudadanos a que no se los moleste por las acciones voluntarias que no afectan a terceros"*[10].

Gelli (2008) aduce que el derecho a la intimidad se desprende del de privacidad que protege el Artículo 19 de la CN pero no se confunde con éste último, analiza el derecho a la intimidad con el contexto del Artículo 18 de la CN[11].

[10] Nino, C.S. (2000). *Fundamentos de derecho constitucional. Análisis filosófico, jurídico y politólogo de la práctica constitucional.* (1ª Ed., lª Reimpresión). (Tº V p. 304). Buenos Aires: Astrea.
[11] Gelli, M. A. (2008). *Constitución de la Nación Argentina Comentada y Concordada.* (4ª Ed. 2008). (1ª Reimpresión 2008). Tº I p. 276 y ss. Buenos Aires: La Ley.

La Corte Suprema de Justicia de la Nación (CSJN) en el caso "Ponzetti de Balbín de 1984"[12], implícitamente equipara intimidad a privacidad; sin embargo en el caso "Baldivieso" de 2010[13] expresa que deben distinguirse nítidamente los conceptos de intimidad y privacidad.

- ***Sustituye el Artículo 153 del CP:*** Antes de la sanción de la Ley de Delitos Informáticos, el correo electrónico no estaba equiparado al correo postal, por lo que todas las acciones que se planteaban judicialmente eran rechazadas por inexistencia de delitos.

Debe entenderse por *comunicación electrónica* todo mensaje enviado por un remitente a un destinatario, a través de un sistema electrónico incluye correo electrónico, chat, fax, SMS[14].

En el caso "Lanata" (1999)[15] las acciones realizadas sobre correos electrónicos habían sido consideradas atípicas, equiparándose a la correspondencia tradicional en los términos de los Arts. 153 y 154 del CP.

De la interpretación del artículo se materializa un *delito especial impropio*, guarda relación con el tipo penal de los Párrafos 1º, 2º y 3º del Art. 153, el autor puede ser un sujeto no cualificado, las características del autor agravan la punibilidad para el sujeto específico.

- ***Incorporación como Artículo 153 bis del CP – Acceso ilegítimo a un sistema informático:*** Este delito vulnera la confidencialidad de la información en sus dos aspectos: *la exclusividad y la intimidad.*

Este delito constituye una *modalidad propia* de ilicitud informática, donde el *objeto material* recae sobre el sistema o dato informático de acceso restringido y acceder a él es la *conducta típica*; es un delito de *acción*, de *resultado instantáneo.*

El *tipo subjetivo* es doloso, reclamándose el *dolo directo* por conocer el acceso ilegítimo a sabiendas. Los *sujetos activo y pasivo* pueden ser cualquier persona.

[12] CSJN. Fallo 306:1892. "Ponzetti de Balbín, Indalia c/Editorial Atlántida S.A.". Buenos Aires, 11/12/1984.
[13] CSJN. "Baldivieso, César Alejandro s/Causa Nº 4733". Publicado en La Ley el 26/05/2010, p. 7. Buenos Aires, 20/04/2010.
[14] Pallazzi. P.A. (2012). *Los delitos informáticos en el Código Penal.* (Ed. 2ª), Buenos Aires: Abeledo Perrot. Pág. 75.
[15] CNCC. Sala VI, 02/12/1999. "Lanata, Jorge s/Excepción de Falta de Acción". Buenos Aires.

- ***Sustitución del Artículo 155 del CP:*** Este cambio actualiza el delito de *publicación indebida* utilizando ahora *publicación electrónica* dentro de los *objetos materiales* del delito. Atendiendo al ataque que se produciría al bien jurídico el delito es de *peligro hipotético o potencial.*

La *acción típica* lo constituye la acción de *hacer publicar indebidamente*, el artículo incluye un elemento normativo jurídico expresivo de un *eventual tipo de justificación genérica concurrente*, se consagra una *causa de justificación específica.*

En el caso "N.N. Dam., G. S.D." (2010)[16], se trata de un menor de edad que denunció violación de su correo electrónico, al margen de la cuestión de competencia del fallo, interesa la comprobación de la denuncia y que la misma ha quedado comprendida en la conducta de la norma que se está analizando.

Al referirse el artículo al *interés público* en su 3er. Párrafo, designa lo que es de utilidad para todos los habitantes, ya que es de todo el país o de una comunidad regionalmente determinada.

- ***Sustitución del Artículo 157 del CP:*** Lo novedoso en esta sustitución es la introducción del término *dato* y proteger penalmente la información en poder de la administración pública, por ser secreta y por la prohibición de ser revelada a terceros.

Se está ante las *conductas típicas* de *descubrir, manifestar o dar a conocer* representaciones de hechos, manifestaciones o conceptos secretos, contenidos en un formato físico o magnético.

- ***Sustitución del Artículo 157 bis del CP:*** La nueva norma deroga también el Inc. 1º del Artículo 117 bis del mismo texto penal, nuevamente lo que interesó al legislador es la lesión al derecho de intimidad y privacidad ya analizados, porque implica acceso no autorizado a un banco de datos reservado.

El *bien jurídico tutelado* es la privacidad, se trata de una *conducta dolosa*. La *tentativa* es de difícil comprobación. El *sujeto activo* será cualquier persona y el *sujeto pasivo* el dueño o titular de una base de datos y quien tenga la responsabilidad de proteger y resguardar la base de datos. El *agravante* de la pena es si el sujeto es un funcionario público.

[16] C.N.Ap.Crim.Corr. Sala VI. Causa 40.376. "N.N. Dam. G., S.D. s/Competencia". Buenos Aires, 22/10/2010.

Se tipifican varios delitos:

> …que tienen como nota común el que en ellos se protege la voluntad de una persona de que no sean conocidos determinados hechos que sólo deben quedar reservados a ella o a un círculo reducido de personas, es decir, que pueden ser calificados de secretos, y también el derecho de la persona a controlar cualquier información o hecho que afecte a su vida privada y…su intimidad[17].

- ***Incorporación como Inc. 16 del Artículo 173 del CP – Estafa Informática – Fraude Informático:*** Incorpora el Inc. 16 del Artículo 173 del CP.

Lucero, P.G.; Kohen, A. A. (2010) en su obra Delitos Informáticos acotan:

> …nos inclinamos por pensar que el bien jurídico protegido es el patrimonio, ya que la conducta lesiva se afecta holísticamente el patrimonio del damnificado y no un componente de la propiedad de dicho sujeto pasivo, como podría ser el caso de los delitos de hurto o robo…

De este modo se nivela al fraude informático con la estafa, es decir que la estafa podrá servir como punto de contraste y comparación. La nueva figura se materializa con medios determinados, es un *delito de resultado instantáneo*, cometido a través de una *acción u omisión*, cuando el sujeto activo ocupa una posición de garante que lo responsabiliza.

Sin embargo, Faraldo Cabana, P. (2007) aproxima la forma de comisión de esta figura delictiva más al hurto que a la estafa.

Además, es un delito *informático propio* en relación con un sistema informático; la *conducta típica* consiste en *defraudar*, es decir perjudicar patrimonialmente a un tercero mediante fraude.

El *tipo subjetivo* es doloso y requiere dolo directo, la finalidad es lograr el perjuicio patrimonial de un tercero. *Sujeto pasivo o activo* puede ser cualquier persona y el *resultado* se efectiviza con el perjuicio patrimonial.

Es importante mencionar que el *fraude informático* se diferencia de la *estafa tradicional*, ya que en el primero no se exige *el engaño y error*, además no se trata de una *disposición consentida.*

- ***Incorporación como 2º Párrafo del Artículo 183 del CP – Daño Informático:*** Con el 1º Párrafo quedaba un vacío legal en cuanto a la informática y los daños que su uso

[17] De Langhe; M.-Rebequi, J.M. Comentario al Artículo 157 bis. AAA-VV. *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial.* Baigún D.-Zaffaroni, E.R.-Terragni, M.A. Buenos Aires: Hammurabi. 2008. Tº 5 p.811.

podía ocasionar, se conoce ahora el *sabotaje informático o cracking*, cuyas *conductas típicas* son: alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos, a su vez estos son *objetos de acción.*

Presenta dos figuras delictivas: 1) Alteración, destrucción o inutilización de productos informáticos y 2) La venta, destrucción o introducción en un sistema informático de programas destinados a causar daños.

El daño informático se materializa con la utilización de: *virus informático, caballos de troya, gusanos, cáncer routines, bombas lógicas, etc.*

Consagra un delito de *acción, de resultado instantáneo, de pluralidad de actos, mixto alternativo*, tratándose de un *delito informático impropio.*

Dice Pallazzi (2012) que:

> …el nuevo tipo legal no requiere expresamente que los datos o programas estén contenidos en una computadora. (…), la idea del daño informático es amparar los datos y el software de un ordenador, pero no para amparar la propiedad intelectual como tal sino el patrimonio.

De esta manera se amplía el espectro dando lugar a cualquier medio digital actual o por crearse. Ahora se considera cosa a los documentos, programas o datos informáticos.

Del mismo modo que los artículos anteriores, el *bien jurídico protegido* es la *propiedad*, requiriendo del *dolo directo* de querer dañar los programas o documentos o sistemas informáticos.

- ***Incorporación del Inc. 6 al Artículo 184 del CP – Daño Informático Agravado:*** Como *agravante del daño* cuando se presente la siguiente circunstancia: "ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

El *bien jurídico* tutelado es la propiedad de los bienes que trata el inciso; el *sujeto activo* es cualquier persona que realice las *conductas delictivas*, pero el *sujeto pasivo* es el titular del dato y también aquel responsable de esos documentos.

La doctrina ha opinado respecto del agravante, así lo manifiestan Lucero y Kohan (2010):

> …el legislador, al entender que existe un mayor grado de culpabilidad, optó por agravar el daño informático, cuando éste se ejecuta en sistemas informáticos destinados a la prestación de servicios de salud, comunicaciones, provisión o transporte de energía, de medios de transporte u otro servicio público.

Mientras que Pallazzi (2012) agrega:

> …el agravante se refiere a sistemas informáticos, pero no de datos o programas de ordenador contenidos en ellos. Entendemos que la redacción los incluye ya que es muy difícil afectar directamente el hardware de un equipo mediante ataques externos, más bien lo que se estropeará será el software, los datos o los medios de comunicación…

- ***Sustitución del Artículo 197 del CP – Delitos contra la seguridad del tránsito y de los medios de transporte y de comunicación:*** Con este delito se amplían los *objetos materiales del delito,* quedando comprendidas las comunicaciones públicas y privadas. Los *bienes jurídicos* comprendidos son las comunicaciones en general, pudiendo ser el *sujeto activo* cualquier persona que interrumpa o interfiera las comunicaciones y el *sujeto pasivo* el titular de dichas comunicaciones, se trata de un *delito doloso* que no admite la *tentativa* toda vez que el delito se consuma una vez interrumpida la comunicación.

III.1.2: Ley de Piratería de Software Nº 25.036.

Siguiendo al análisis publicado en el Sistema Argentino de Información Jurídica (SAIJ)[18], al cual adhiero, se reproducen en el presente apartado algunos conceptos extractados del mismo.

> … el concepto de software, el cual está en permanente desarrollo, para entender al mismo se puede decir que *"se trata en general de programas que responden a demandas específicas del usuario, controlando el funcionamiento propio del computador y sus periféricos"*.
>
> Respecto de la naturaleza jurídica del software los doctrinarios hablan de distintos conceptos, pero la de mayor aceptación por la tendencia a protegerlo por las instituciones de la propiedad intelectual y que fue escogida por la Ley 25.036 es la que la considera como *un bien inmaterial.*
>
> El *bien jurídico protegido* es el *derecho de autor*, ubicando el *injusto* (reproducir sin autorización con o sin fines de lucro programas o recopilaciones) dentro de la teoría que lo protege mediante el copyright (normas y principios que protegen los derechos morales y patrimoniales de los autores).

[18] SAIJ. *"Piratería de software, nueva Ley 25.036".* Prunotto Laborde, A. COLECCIÓN ZEUS – DOCTRINA. Recuperado el 27/02/2017 de: http://www.saij.gob.ar/adolfo-prunotto-laborde-pirateria-software-nueva-ley-25036-dasf060047/123456789-0abc-defg7400-60fsanirtcod

La tutela del derecho de autor está reconocida como *derecho humano* por la Declaración de Universal de Derechos Humanos de la Naciones Unidas: ARTICULO 27 Inc. 2º DUDHNU: Toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora.

También es reconocido como *derecho humano fundamental* por la Declaración Americana de los Derechos Humanos del Hombre y el Pacto Internacional de Derechos Económicos, Sociales y Culturales, con jerarquía constitucional argentina, auspiciando la protección de los bienes jurídicos en cuestión.

El precedente jurídico a la Ley 25.036 es la promulgación de la Ley 11.723 del año 1933, desde ese entonces se producen distintas incorporaciones de tecnología en los usuarios, con fenómenos antijurídicos que no siempre estaban contemplados en la vieja ley.

Ante presiones de EEUU el Poder Ejecutivo dicta el Decreto 165/94 sobre Propiedad Intelectual modificando el concepto de obra, dicha norma era inconstitucional ya que el Poder Ejecutivo no puede legislar en materia penal. Luego de la reforma constitucional de 1994 en que el Art. 75 Inc. 22 expresa la supremacía de los tratados sobre leyes, se produce un cambio con la sanción de la Ley 24.425 que amplía el concepto de obra literaria, actualizándolo a la realidad de los tiempos políticos.

Un caso relevante atrapado en el medio de los cambios relacionados con los derechos de autor es el Caso "Autodesk" (1997)[19], donde la Cámara Nacional de Casación Penal Sala 1 de la Capital Federal, confirmó el sobreseimiento por inexistencia de delito, en un caso de reproducción de un programa de computación sin autorización del titular del derecho de propiedad intelectual por considerar el Art. 72 de la Ley 11.723 como un tipo penal cerrado. Interpretó el tribunal que el Decreto 165/94 no resultaba complementario de la Ley de Propiedad Intelectual y que sólo reglaba instancias administrativas de registración de software o bien afirmaba la protección civil del mismo, por lo que carecía de la capacidad para definir conductas penalmente reprimidas.

Al sancionarse la Ley 24.425 (anterior a la Ley 25.036) establece que los programas fuente y objeto serán protegidos como obras literarias, al protegerse estas obras ha sido alcanzada por la Ley de Copyright y la reproducción del software sin autorización constituye un *injusto severamente penado y perseguible de oficio.*

La Ley 25.036 modifica especialmente el Art. 1º de la Ley 11.723 y es por demás clara, en cuanto a considerar a los programas fuente y objeto, así como también a la recopilación de datos o de otros materiales, como objeto de la tutela penal.

La nueva ley agrega al Art. 4º de la Ley 11.723 que "la propiedad intelectual de los programas que produzcan los dependientes de una empresa o una persona, contratados para tal fin pertenecerán al contratante salvo estipulación expresa en contrario".

[19] C.N. de Casación Penal de Capital Federal. Sala 1. Sentencia 547 del 19/07/1997. *"Autodesk Inc. s/Recurso de Casación".*

A su vez en el Art. 9º de la Ley 11.723 reformula el mismo diciendo que "la realización de una copia a las personas que tengan una licencia para el uso de un programa, como salvaguarda del mismo, imponiéndole una serie de obligaciones para su obtención y restringiendo el uso de esa copia al reemplazo del original, siempre y cuando el original se perdiera o inutilizara", de esa forma se resuelve el inconveniente por el lucro o no en el autor de una copia.

Con esta última ley sobre piratería de software, se vislumbra que primó en el legislador respecto de su redacción el criterio internacional más difundido en la materia, la protección por el copyright.

Las sanciones penales se igualan a las *"estafas y otras defraudaciones"* del Capítulo IV - Art. 172 del CP, considerándola como caso especial de defraudacion y serán reprimidos con prisión de 1 mes a 6 años. El delito se consuma cuando el *sujeto activo* consigue el beneficio con daño patrimonial de otro, no existiendo consentimiento por parte del *sujeto pasivo.*

Por lo expuesto podría considerarse que las controversias suscitadas alrededor de los derechos de autor quedarían cerradas y este capítulo de la historia estaría terminado.

III.1.3.: Aportes de la Ley de Despenalización de Calumnias e Injurias en Asuntos de Interés Público Nº 26.551 y otras normativas locales relacionadas con delitos informáticos.

La Ley Nº 26.551 es un aporte a la solución de los delitos informáticos, cuando en las conductas relacionadas con calumnias e injurias en asuntos de interés público se utilicen instrumentos informáticos o electrónicos, la ley opta por no reconocer como delito, consagra una *prohibición expresa de criminalización para las conductas objetivamente ofensivas del honor*, cuando éstas se manifiestan con los fines y formas especificadas en los reformulados Artículos 109 y 110 del CP.

Sosa Baccarelli, N. (2011) señala al respecto:

En el año 1994 la Comisión Interamericana de Derechos Humanos (en adelante "la Comisión" o "Comisión IDH") en el caso Verbitsky contra Belluscio tuvo oportunidad de expedirse sobre las leyes de desacato y señaló que resultaban incompatibles con la Convención Americana de Derechos Humanos (en adelante "CADH"). En el marco de una solución amistosa el Estado argentino derogó la figura penal de desacato. Varios proyectos de ley fallidos han postulado la derogación o reforma de los tipos penales que protegen al honor. Especial relevancia tuvo el proyecto elaborado por la Asociación Periodistas y presentado en el Congreso Nacional por los entonces senadores José Genoud y Jorge Yoma. No obstante, los intentos anteriores, la reforma que produjo la sanción de la ley 26.551 tuvo como principal antecedente la condena que la Argentina recibió por parte de la Corte Interamericana de Derechos Humanos (en adelante "Corte IDH") recaída en el caso Eduardo Kimel, el 2 de mayo de 2008, y que será objeto de análisis en la segunda sección de este trabajo. La reforma que aquí estudiamos ha cambiado definitivamente la fisonomía del título 2 del libro segundo del Código Penal argentino.

La resolución de casos judiciales fue cambiando conforme el devenir de las ideas políticas relacionadas con calumnias e injurias, por ejemplo:

- ✓ ***Fallo "Vago" (1992)[20]:*** La Cámara de Apelaciones en lo Civil aplica por primera vez la doctrina de la *Real Malicia*, donde el agraviado público debe demostrar la falsedad de las calumnias e injurias, la entidad y gravedad de las manifestaciones deben poseer una mayor aptitud ofensiva para ser consideradas injurias en el sentido del CP, máxime cuando se está frente a cuestiones de interés público.

Es que "…la investigación periodística sobre asuntos públicos desempeña un rol importante en la transparencia que exige un sistema republicano, y el excesivo rigor y la intolerancia del error llevarían a la autocensura, lo que privaría a la ciudadanía de información imprescindible para tomar decisiones sobre sus representantes…" (Fallo Brugo, 2009)[21].

Fallo "Morales Solá" (1996)[22]: Revela una mayor aplicación de la doctrina de la Real Malicia, donde por primera vez la totalidad de los jueces de la CSJN aceptaron la vigencia de la doctrina mencionada.

- ✓ ***Fallo "Pandolfi"[23]***, donde una de las empresas, según el reportaje, estaba en manos del presidente del partido en el gobierno Dr. Oscar Pandolfi, éste promovió querella por el delito de injurias contra Rajneri, el reportero, el fallo sigue en líneas generales la doctrina sentada por las anteriores.

A modo descriptivo se lista a continuación la normativa más importante que complementa el sistema jurídico argentino de control de los ciberdelitos:

- ➢ ***Ley 26.061 de Protección Integral de los Derechos de Niñas, Niños y Adolescentes:*** Estos derechos están asegurados por su máxima exigibilidad y sustentados en el principio del interés superior del niño.

- ➢ ***Decreto 415/2006:*** Reglamenta la Ley 26.061.

[20] CSJN. Fallo 314: 1517. *"Vago, Jorge Antonio c/Ediciones de la Urraca S.A.* 12/06/1992.
[21] CSJN. Fallo 332: 2559. *"Brugo, Jorge Ángel c/Lanata, Jorge y otros.* 16/11/2009.
[22] CSJN. Fallo 319: 2741. *"Morales Solá, Joaquín c/Giadone, Dante.* 02/11/1996.
[23] CSJN. Fallo 320: 1273. *"Pandolfi, Oscar Raúl c/Rajneri, Julio Raúl.* 01/07/1997.

- ***Ley 26.904 de Grooming:*** Se incorpora al Art. 131 del CP los delitos cometidos contra la integridad sexual por medio de instrumentos informáticos.

- ***Ley 863 de la Legislatura de la CABA:*** Establece que los establecimientos comerciales que brinden acceso a internet deben instalar y activar filtros de contenido sobre páginas pornográficas.

- ***Código Contravencional de la CABA:*** En su Art. 52 pena la intimidación y el hostigamiento amenazante, agravada si se trata de menores; además en su Art. 61 castiga al suministre o permita a un menor el acceso a material pornográfico.

- ***Ley 23.592:*** De actos discriminatorios.

- ***Código Penal:*** Art. 149 bis delito de amenazas; Art. 168 delito de extorsiones; Art. 169 delito de chantaje o amenaza de imputaciones contra el honor o violación de secretos; Art. 213 hacer pública la apología de un delito o de un condenado por delito.

- ***Comunicación "B" 9042 del BCRA:*** Relativa a seguridad en entidades financieras y la Tecnología Informática y Sistemas de Información.

III.1.4.: Principios de aplicación. Las Garantías Constitucionales en el Proceso Penal. Otros recursos.

Cuando estamos en presencia de un caso relacionado con algún delito informático, nos remite a la *acción penal* y a lo que prescribe la ley penal en abstracto ante una conducta punible. Se necesita que el delito deba ser perseguido por el Estado a través de un procedimiento oficial y órganos encargados del proceso, ajustándose a los principios y garantías legales.

Principios de Aplicación.

1) Principio de Legalidad: Exige la existencia de un régimen jurídico que formule la descripción del hecho o conducta criminal y de la pena a imponerse, previamente al hecho que califica a ella como criminal, para imputar a una persona como autora del delito.

Nuestra CN en su Artículo 18 dice "…ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso…" A su vez el Artículo 71 CP prescribe el ejercicio de las acciones.

Ricardo Núñez (1987) enumera las consecuencias que derivan de dicho principio: la indelegabilidad de la facultad legislativa penal, el Principio de Reserva Legal con sus principios y la predeterminación legal de la pena aplicable.

2) Principio de Reserva Legal: Nuestra CN consagra dicho principio en su Artículo 19 que dice: "…ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe…"

Según Núñez (1987), el Principio de Reserva Legal presupone como condiciones de su existencia las siguientes: a) la determinación legal de los hechos punibles, b) la determinación legal de las penas correspondientes, c) la prohibición de la analogía y d) la irretroactividad de la ley penal.

3) Principio de Oportunidad: Significa que ante la posible comisión de un hecho ilícito se pueda o no iniciar la investigación penal de la investigación, iniciada pueda suspenderla provisoria o definitivamente, limitarse la persecución a algunos de los hechos ilícitos o a algunos de los imputados que habrían participado del mismo; esto implica que la investigación se hará objetivamente y subjetivamente.

Dos rasgos característicos de la infracción informática son su extraterritorialidad y su intemporalidad:

– *Extraterritorialidad:* Es una característica de la delincuencia moderna transnacional surgido a partir del uso de internet por un operador situado en cualquier lugar del mundo, valiéndose de una computadora, un teléfono, un modem y un proveedor de servicio, por eso la dificultad para determinar la ley aplicable en el espacio. En esta clase de delitos resulta necesaria una elaboración teórica para determinar cuál o cuáles son los Estados facultados para ejercer su jurisdicción y aplicar su derecho penal sobre el caso[24].

– *Intemporalidad:* La disociación entre acción y resultado típico de los delitos cibernéticos, no se verifica solo espacial, sino temporalmente. Por eso, y siguiendo a Cárdenas (2008) en relación a la *intemporalidad*, existen programas o acciones dañosas que obstaculizan una investigación de hechos ilícitos.

Las Garantías Constitucionales en el Proceso Penal.

[24] Cárdenas, C. (2008). *"El lugar de comisión de los denominados ciberdelitos"*. Política Criminal Nº 6. 2008. A2 – 6. Recuperado el 29/06/2016 de: http//www.politicacriminal.cl/n_06/A_2_6.pdf

Garantías Bilaterales (imputado y víctima).

1) Igualdad ante los Tribunales: Art. 16 CN - 14.1 PIDCP[25] - Garantía Bilateral que se cumple con el Principio del Contradictorio, en donde todas las partes del proceso tienen las mismas facultades.

2) Juez Natural: Art. 18 CN – Art. 14 Inc. 1 PIDCP – Art. 8 CADH[26] – Radica en que el juez debe entender en un conjunto de causas y no para un caso determinado, creado por una ley anterior al hecho, garantizando la imparcialidad, independencia e idoneidad.

3) Imparcialidad del Tribunal: Art. 114 Inc. 6 CN – Art. 8.1. CADH – Art. 10 DUDH[27] - La organización judicial asegurará la independencia de los jueces para la prestación eficaz de justicia.

4) Derecho de Defensa: Art. 18 CN – Art. 8.2. d. e. CADH – Art. 11.1. DUDH – Garantía Bilateral ya que se da tanto para el imputado como para la víctima.

5) *Razonabilidad de la duración del proceso:* Art. 18 CN – Art. 8.1. CADH – Reconocido supranacionalmente y con jerarquía constitucional, la doctrina discute respecto de la definicion del *plazo razonable.*

Garantías Propias del imputado.

1) Reserva de la intimidad: Art. 18 CN – Art. 11.1. CADH – Tiene en cuenta la dignidad personal que le asiste por el sólo hecho de ser individuo, es el derecho de la vida privada que cada persona quiere preservar del conocimiento e intrusión de los demás.

2) Estado de inocencia: Art. 18 CN – Art. 11 DUDH – ART. 1 CPPCba. – Es un estado jurídico que el imputado no debe acreditar.

3) Juicio previo: Art. 18 CN – Art. 14.1. y 3 e. PIDCP – Art. 1 CPPCba. – Requisito indispensable para que el Estado pueda aplicar una pena teniendo en cuenta determinadas características procesales.

4) Non bis in idem: Art. 14.7. PIDCP – Art. 1 CPPCba. – No solo impide ser juzgado dos veces o condenado dos veces, sino que es mucho más amplio, impide inclusive

[25] Pacto Internacional de Derechos Civiles y Políticos. Nueva York. 19/11/1966. Ley 23.313.
[26] Convención Americana de Derechos Humanos. Costa Rica. 22/11/1969. Ley 23.054.
[27] Declaración Universal de Derechos Humanos. Res. 217 A (III) de la Asamblea General de las Naciones Unidas. 10/12/1948.

ser perseguido más de una vez por el mismo hecho. Debe cumplirse la triple identidad: de sujeto, de objeto y de causa.

Otros Recursos.

- ***Derecho del Consumidor:*** Art. 42 CN – Ley de Defensa del Consumidor Nº 22.240 – Los servicios de provisión de internet pueden generar ilícitos relacionados con delitos informáticos, el legislador previó normas para subsanar alguna desigualdad entre consumidor y usuario.

- ***Acción de Amparo (Habeas Data):*** Art. 43 CN – Ley 25.326 – Mediante esta norma se otorga *rango constitucional* a esta garantía.

III.1.5. Los ciberdelitos en la Provincia de Córdoba.

El Área de Coordinación y Seguimiento del Cibercrimen del Ministerio Público Fiscal (MPF), se dispone a brindar un nexo con los distintos órganos encargados de la investigación (Fiscalías de Instrucción, Unidades Judiciales y Direcciones de Policía Judicial), a fin de prestar colaboración y asesoramiento adecuado en la materia[28], y propone:

Los objetivos generales:

- Proporcionar a la estructura del MPF una unidad de trabajo que permita responder a la demanda creciente de la información y tratamiento actual en los delitos relacionados con las TIC.
- Disminuir el tiempo de respuesta a los requerimientos.
- Crear espacios de capacitación y formación.
- Fomentar la inter-disciplina con otras áreas, secciones, dependencias, etc. para la resolución de casos y/o tareas afines.
- Proponer protocolos de trabajo para la materia especifica en Cibercrimen o Delitos Informáticos.
- Establecer canales de comunicación institucional adecuados respecto de la materia.
- Colaborar y asesorar a todos los miembros del Ministerio Público Fiscal.

III.2: Los ciberdelitos en el Derecho Comparado.

Gustavo Arocena (2008) apunta en su análisis sobre *"La regulación de los delitos informáticos en el Código Penal argentino"*:

> Ahora bien, determinada la eventual necesidad de una regulación legal específica del ciberdelito, existen dos opciones a la hora de pergeñar esta normativa particular.

[28] Ob. Cit. en Ref. 1

> Por un lado, puede sancionarse una ley específica complementaria del Código Penal. Es la opción por la que se han inclinado por ejemplo *Venezuela* —que sancionó su Ley Especial contra los Delitos Informáticos el 30 de octubre de 2001—, *Chile* —que hizo lo propio mediante ley núm. 19.223, del 28 de mayo de 1993) y *Alemania* —que el 15 de mayo de 1986 adoptó la Segunda Ley contra la Criminalidad Económica, que se ocupa casi excluyentemente de la ciberdelincuencia, pero atrapa igualmente algunas figuras ajenas a ella, como, por caso, la utilización abusiva de cheques—
>
> Por el otro, puede preferirse una reforma del Código Penal, ya agregando un nuevo título que contemple las nuevas ilicitudes no tipificadas, o ubicando éstas en los distintos títulos del digesto, conforme los diversos bienes jurídicos que pretendan tutelarse. Entre otros países, ha legislado sobre los delitos informáticos en su Código Penal, mediante la creación de un capítulo específicamente dedicados a ellos, Bolivia: en su libro segundo, el título XII —destinado a los delitos contra la propiedad— incorpora el capítulo XI, que tipifica los delitos informáticos. En cambio, ha preferido regular los ciberdelitos en su Código Penal, esparciendo las diversas figuras en distintos pasajes de su articulado, Paraguay, España y Francia, por ejemplo.
>
> En nuestro país, en el desarrollo histórico de la legislación penal más reciente, encontramos ejemplos de cada una de estas dos grandes alternativas, aunque la normativa vigente decide incluir la cibercriminalidad en su Código Penal en forma desconcentrada, esto es, incluyendo los distintos tipos legales en los diversos títulos del libro segundo del digesto, conforme los variados objetos jurídicos que se desea tutelar.

Del Pino, S. A. (2005) en su obra "*Delitos Informáticos"*, informa acerca de los avances regulatorios internacionales en materia de delitos informáticos, sintéticamente destaca:

Estados Unidos: Los delitos informáticos y los nuevos problemas que dichas conductas causan, han sido objeto de diversas investigaciones desde la década de 1960. Siendo los EEUU pioneros en enfrentar las dificultades que encierra esta nueva modalidad delictiva. Sus antecedentes más importantes son:

a) Acta Federal de Dispositivo de Acceso, Falsificación, Fraude y Abuso Computacional de 1984: Contempla delitos informáticos contra la Defensa Nacional; Delitos Informáticos contra Entidades Financieras y Actividad Hacker.

b) Acta Federal de Fraude y Abuso Computacional de 1986: El Congreso de los EEUU se basó para la reforma en los informes de la actividad hacker acaecida entre 1984 y 1986.

c) Acta Federal de Abuso Computacional de 1994: Modificando la de 1986, modificando la regulación de virus.

Alemania: Para hacer frente a la delincuencia relacionada con la informática, se adaptó en 1986 la Segunda Ley contra la Criminalidad Económica en la que se contempla: espionaje de datos, estaba informática, falsificación de datos probatorios, alteración de datos y sabotaje informático. La protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que estos no pueden ser protegidos suficientemente por el derecho vigente, contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

Austria: La ley de reforma del Código Penal Austríaco de 1987 contempla los siguientes delitos: destrucción de datos, estafa informática.

Francia: La Ley Nº 88-19 de 1988 sobre el fraude informático regula: acceso fraudulento a un sistema de elaboración de datos, sabotaje informático, destrucción de datos, falsificación de documentos informatizados y uso de documentos informatizados falsos.

Reino Unido de Gran Bretaña: Reguló el crimen informático y el fraude informático en el Acta de 1990 con tres variantes: a) el acceso no autorizado a materiales de la computadora, b) acceso no autorizado para cometer o facilitar la comisión de ofensas y c) la modificación de materiales de la computadora.

Portugal, España e Italia: Portugal ha contemplado este tipo de delitos en agosto de 1991 mediante la Ley 109/91. El Código Penal español aprobó mediante la Ley Orgánica 10/1995 diferentes tipos de delitos informáticos. Italia a través de la Ley 547 de 1993 llenó el vacío legal que presentaba su legislación penal en materia de los delitos en estudio.

Japón: Cuenta desde 1987 con artículos incluidos en el Código Penal relativos a los delitos informáticos, los mismos tratan acerca de: interferencia en transacción realizada por un sistema computacional, fraude computacional. El Código penal japonés en cuanto a la criminalidad informática es completado por la Ley 128 de acceso no autorizado a computadoras del año 1999.

Chile: Aprobó la Ley 19.223 tipificando las siguientes figuras delictivas: a) daño informático, como agravante la destrucción de datos almacenados en el sistema, b) se tipifica el hacker, c) define el programador de virus.

Brasil: La Ley 12.737 de 2012 dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones en otros artículos. La Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en internet.

México: Mediante reformas en el Código Penal Federal, se buscó tipificar los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación. Se destaca aquellos que atentan contra los sistemas de cómputos que pueden o no ser parte del sector financiero mexicano. Es importante que los estados mexicanos cuentan con sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo.

Uruguay: No posee ley especial, pero sí diferentes normativas parcialmente aplicables a la materia. Cuenta con la Ley 17.815 regula violencia sexual, comercial o no comercial o no comercial cometida contra niños, adolescentes e incapaces que contengan la imagen o cualquier otra forma de representación. La Ley 17.520 penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados.

Los países nombrados son solo algunos ejemplos del Derecho Comparado, hoy en día la mayoría de los estados prevé la sanción de diferentes figuras delictivas relacionadas con el mal uso de la informática cometidos por ciberdelincuentes.

CAPÍTULO IV: Relación de la normativa argentina con los instrumentos internacionales, doctrina y jurisprudencia.

El presente Capítulo es de suma utilidad para la investigación que se lleva a cabo, ya que nos permite conocer aquellas directivas internacionales que sirven de base para la elaboración de normativas locales en materia de cibercrímenes y que la mayoría de los países adhirieron. Por otro parte permite conocer hasta qué punto nuestro país sigue los lineamientos internacionales.

Se completa a la relación de la normativa vigente, las opiniones de doctrinarios y jurisprudencia destacable vinculada con cibercrímenes. La doctrina y principalmente la jurisprudencia marcan el devenir de las decisiones judiciales, que comenzaron a dar un giro importante al tener normativa específica para crímenes informáticos.

Balanta, H. (2009, 4) en la Ponencia presentada en el II Congreso Internacional de Criminología y Derecho Penal, 2009, manifiesta que:

> La evolución incansable de la tecnología, no permite al derecho proveer a tiempo de herramientas legales para combatir este tipo de conductas lesivas, por tal razón en los países a nivel mundial, la manera de estimular la legislación para tipificar los delitos informáticos es que avance la estrategia del crimen y a *posteriori* actuar.
>
> A nivel regional se han elaborado diferentes instrumentos frente a la criminalización de los contenidos ilícitos, sin embargo, guardan sus similitudes entre los países de la misma región, antes que con la legislación a nivel mundial.
>
> Tenemos entonces a la Unión Europea, el Mercado Común para África Oriental y África Austral (COMESA), la Organización de Estados Americanos (OEA), el Consejo de Cooperación del Golfo (GCC), encaminaron a través de instrumentos la difícil tarea de enfrentar estos delitos tan especiales.

Este capítulo analizará los instrumentos más importantes a nivel mundial que fueron perfilando directivas para adaptar las normas penales al devenir de los delitos relacionados con el uso de medios electrónicos de datos.

Y sin duda estos documentos internacionales fueron los precursores para que, en materia de delitos informáticos, los estados fueran armonizando sus normas penales, aunque siempre con movimientos espasmódicos, ya que el delito cibernético evoluciona constantemente ante los nuevos avances tecnológicos, es el caso de los cambios realizados en nuestro país.

IV.1: Instrumentos internacionales.

Los instrumentos influyentes más importantes provienen: de la Organización para la Cooperación y el Desarrollo Económico (OCDE), de los Seminarios sobre Regionalización del Derecho Penal en el Mercosur, de la Convención contra la Delincuencia Organizada Trasnacional y del Convenio sobre Cibercriminalidad de Budapest, Conclusiones de las Naciones Unidas.

IV.1.1: Organización para la Cooperación y el Desarrollo Económico (OCDE).

Sain, G. (2013), analiza el proceso de los diferentes organismos y el rol por definir figuras penales y armonización legislativa en relación a este tipo de conductas:

Uno de los primeros intentos a nivel internacional se dio en 1983, cuando la Organización para la Cooperación y el Desarrollo Económicos (OCDE) inicia un estudio para la armonización de leyes penales en la materia para los países miembros.

Las posibles implicancias económicas de la delincuencia informática, su carácter internacional y el peligro que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución, desembocando en una lista de acciones que pudieran ser consideradas por los estados, por regla general, como merecedoras de pena.

En 1986 publica la OCDE un informe titulado Delitos de Informática, proponiendo propuestas de reformas en los estados miembros y recomendaba una lista de mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales mínimas: fraude, falsificación, alteración de datos y programas, derechos de autor y la interceptación de las comunicaciones, entre otras.

IV.1.2: Seminarios Internacionales sobre "Regionalización del Derecho Penal en el Mercosur".

A este nivel regional el Mercosur ha venido trabajando en la materia a través de los denominados Seminarios Internacionales sobre Regionalización del Derecho Penal, a fines del siglo XX y en estos primeros años del siglo XXI han llegado a importantes avances, pero no alcanza para cubrir este avance de los cibercrímenes, Brasil es uno de los países miembros del Mercosur más afectado con este tipo de ilícitos.

Marcelo A. Riquert (2006) al referirse al estado de la legislación contra la delincuencia informática en el Mercosur, en la Ponencia presentada en el VI Encuentro Argentino de Profesores de Derecho Penal, realizado en Mar del Plata en octubre de 2006 concluye:

a) La protección penal respecto de la delincuencia informática en el ámbito del Mercosur presenta una serie de asimetrías entre los estados miembros con carácter pleno y, además, con aquéllos a los que se hallan unidos por el compromiso democrático.

b) Esto se visualiza desde lo formal, en el distinto modo en que se aproximan a las necesarias actualizaciones legislativas y, desde lo material, en la consideración de algunos de los problemas o la directa ignorancia de lo apuntado, el proceso de armonización se presenta como una necesidad ineludible.

c) Tratándose de una experiencia de integración regional con aún pretensiones y objetivos limitados, estructuralmente se ve favorecida tal falta de armonía, no encontrándose previstas vías institucionales por el aumento para canalizar el proceso de superación del problema, aspecto en el que comparativamente la Unión Europea presenta ventajas notables, sin que ello quite complejidad del asunto.

d) El presentado a discusión Proyecto de Código Penal Argentino en el año en curso, aporta en su articulado la solución a algunas de las lagunas de punibilidad en su oportunidad denunciadas en el derecho interno, significando a la vez un avance hacia la armonización legislativa en la materia con otros países del bloque regional que se han ocupado de esta problemática en un modo más integral.

IV.1.3: Convención contra la Delincuencia Organizada Trasnacional.

Esta Convención fue adoptada en diciembre del año 2.000, se la conoce como la Convención de Palermo (Italia)[29], surgiendo como una convención conforme a los efectos de la globalización y las nuevas tecnologías que implican nuevas oportunidades empresariales, sus determinaciones son muy trascendentes. Pero lo más trascendente se basa en tres dimensiones:

1) El énfasis otorgado a los delitos no tipificados en la mayoría de las legislaciones, en detrimento de conductas delictivas con mayor tradición (homicidio, secuestro, extorsión, etc.) y que constituyen la base del poder de las mafias.

2) El desconocimiento de los delitos informáticos que implícitamente suponen sistemas judiciales y de investigación criminal sofisticados y eficaces, con la participación del sector informal de la economía, la baja penetración del sistema tributario y el exceso de regulación con el blanqueo de dinero o los sobornos a los funcionarios públicos.

3) Limitar la posibilidad de corrupción o amenazas al sistema judicial con una correcta adaptación de la legislación domestica, para estar libre de influencias.

IV.1.4: Convenio sobre Cibercriminalidad de Budapest.

Entre otros instrumentos internacionales se encuentra el Convenio sobre Cibercriminalidad de la Unión Europea, firmado en Budapest en 2.001[30] y que nuestro país adhiere en 2.010. Este Convenio sobresale por la trascendencia que dan los estados firmantes a la conservación inmediata de datos de tráfico e interpretación de datos relativos al contenido, y destaca también el Convenio los rasgos que identifican prioritariamente a los delitos informáticos: *territorialidad, intemporalidad e intangibilidad*.

El acuerdo se constituyó de carácter abierto, para que pueda ser suscripto por otros países fuera de la Unión Europea. Representa en la actualidad el documento de referencia internacional más importante en términos de Derecho Penal, Derecho Procesal y Cooperación

[29] Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional. Recuperado el 06/06/2016 de: http://www.unodc.org/documents/peruandecuador/Publicaciones/tocebook.pdf

[30] Convenio sobre Cibercriminalidad de Budapest. Recuperado el 06/05/2016 de: http://www.coe.int/t/dghl/cooperation/econoccrime/Source/Cybercrime/TCY/ETS_185_spaish.PDF

Internacional en materia de delitos informáticos. Su entrada en vigencia se produjo el 01 de julio de 2004, y a la fecha posee la adhesión de países como Australia, Japón, Canadá y Sudáfrica, entre otros.

IV.1.5: Conclusiones de las Naciones Unidas sobre el estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes sociales.

Surge al mundo en el año 2.001 por medio del Consejo Económico y Social de la Organización, manifestando la preocupación de los estados por las repercusiones de la delincuencia organizada trasnacional, que lesionan la estabilidad y el desarrollo político, social y económico de la sociedad, proponiendo a sus estados miembros contribuir voluntariamente al Fondo de Naciones Unidas para la Prevención del Delito y la Justicia Penal, para asistir a los países en desarrollo y con economías en transición, con la asistencia técnica que requieren para aplicar la Convención y sus protocolos.

IV.2: Doctrina y jurisprudencia sobre delitos informáticos.

Durante el transcurso de la investigación que se llevó adelante, se fue accediendo a opiniones doctrinarias de distintos juristas, las mismas trataban sobre puntos especiales de este trabajo, como ser conceptos de estos ilícitos, clasificaciones, opiniones acerca de decisiones judiciales, entre otras opiniones y en muchos casos no había un consenso general en sus apreciaciones.

Pero en lo que respecta a la situación general del tratamiento de los ilícitos relacionados con la cibernética y a estas instancias de la presente investigación, interesa las versiones vertidas por la doctrina respecto a la implementación de normativas penales y procesales. Y aquí sí se observa en líneas generales que hay mayor consenso respecto al presente y al futuro en que se encuentran las decisiones asumidas por los estados.

Por eso, se transcribirán solo algunas consideraciones doctrinarias, entendiendo que las mismas poseen similares argumentaciones en el contenido de sus comentarios:

Arocena, G.A. (2.008) afirma:

> A la hora de concebir una política criminal seria para la persecución, el juzgamiento y el eventual castigo del delito informático, no es suficiente su tipificación –por más perfecta y acabada que sea– de las distintas hipótesis de ciberdelito que deben ser previstas por el legislador penal. Tampoco la imprescindible adecuación de las estructuras y las herramientas de la Parte General del Derecho Penal.

Antes bien, resulta imprescindible la creación de estructuras procedimentales destinadas a la elaboración y acreditación de la hipótesis fáctica a subsumir en las nuevas figuras delictivas que se instituyen.

Es que, rasgos salientes de los delitos informáticos, como –por ejemplo– su extraterritorialidad, su intemporalidad y la intangibilidad del instrumento y el objeto sobre el cual recae la conducta típica, deben ser tenidos en cuenta por el legislador procesal, para que éste construya métodos de investigación y esclarecimiento del ciberdelito adecuados a tales caracteres.

Si, a la par de la determinación exacta de los ilícitos comprendidos en el ámbito de la delincuencia informática, el derecho Penal realizador no pergeña los instrumentos de comprobación judicial idóneos para la acreditación de tales delitos, se arriba a la inconcusa violación del principio de racionalidad penal legislativa según el cual el legislador sólo debe sancionar leyes que prevean delitos apriorísticamente susceptibles de acreditación fáctica en un debido proceso penal.

Por otra parte, Sain G. (2.013) reflexiona del siguiente modo:

En conclusión, si bien resulta necesaria la tipificación de conductas indebidas, hechos ilícitos e ilegales por parte del Derecho Penal, Civil o Comercial, la cooperación internacional en este sentido y la reforma de los códigos procesales para la admisibilidad de pruebas electrónicas en el marco de una causa judicial, la solución penal resulta insuficiente en términos de diseño de una política pública para la red.

En este sentido, resulta necesaria la creación en el seno de las administraciones centrales de un organismo gubernamental para el diseño de estrategias y políticas integrales en materia de cibercrimen.

Las políticas resultantes deben estar fundadas en la realización de estudios y el acopio de información estadística sobre nuevas modalidades delictivas. A su vez, debe proponer legislación para la regulación del sector y brindar asistencia y asesoramiento a aquellos organismos que así lo requieran, brindando recomendaciones y líneas de acción estratégicas.

Balanta H. (2009) aporta su valiosa opinión diciendo:

Aunque contemos con un instrumento jurídico internacional que nos sirva como modelo a los países para legislar en materia de delitos informáticos y teniendo en cuenta otros países los cuales ya tienen legislado los delitos informaticos, vemos que las leyes no son suficientes para bajar los índices de delincuencia informática.

Como observamos en muchos países, por tratar de regular y describir específicamente un delito informático, hace que rápidamente la norma quede obsoleta, por tal para evitar caer en esta situación se hace necesario que se realicen las respectivas investigaciones para ahondar en la naturaleza del problema y con la característica transnacional que tiene el delito informático.

Sin duda alguna, es necesario una solución global, además de que exista una serie de legislación que sea compatible con los de distintos países, también la cooperación internacional que sería el único

> mecanismo infalible para combatir la delincuencia informática. Es necesario un planteamiento integral, completo, colectivo de los diversos sectores para combatir la delincuencia informática.

Con respecto a la jurisprudencia existente, la misma es abundante y algunos casos se han mencionado y analizado en distintos puntos de este trabajo, observándose que antes de las reformas en la normativa penal respecto de los delitos que se investigan, no se ha podido dar una respuesta favorable a las víctimas por la falta de tipificación legal de los ilícitos, pero ante el avance de los cambios realizados en los ordenamientos jurídicos del mundo se fueron resolviendo situaciones que antes quedaban impunes.

EEUU es pionero en cuanto a regulación de los ciberdelitos y la justicia es estricta en la aplicación y ejecución de severas penas. Así, en el caso "Morris" (1988) sobre bloqueo de las líneas de comunicación y memorias de computadoras de red, Morris fue detenido y condenado a 3 años de prisión, trabajos comunitarios y multa. En el caso "La Macchia" (1994) la justicia americana responsabilizó a La Macchia, estudiante de 20 años de edad por conspiración a fin de cometer fraudes electrónicos.

Otro leading case es el caso "Blue Crest Music" (1979), donde la Corte Suprema de Canadá sostuvo que es irrelevante si el infractor cobra o no por su actividad ilícita en casos de ciberdelitos.

"Ardita" (1995) es un famoso hacker argentino, que en el juicio de Boston lo condenaron puntualmente por posesión fraudulenta de claves de seguridad, nombres de abonados, códigos y otros permisos de acceso, por actividad fraudulenta y destructiva con ordenadores y por interceptación de comunicaciones.

En el caso argentino "Lanata" (1995) se determina que el correo electrónico goza de la misma protección que quiso darle el legislador al incluir los Arts. 153 a 155 del CP cuando aún no existían estos avances tecnológicos, sin embargo, en alzada se revoca el auto de primera instancia.

En "Piamonte" (1993) se inicia una querella por retención indebida de software, mientras que en "Iglesias" (1992) quedó comprobado que el procesado pasaba sumas de dinero a una cuenta personal, mediante distintas modalidades.

Ante el advenimiento de las reformas introducidas en el CP argentino en materia de ciberdelitos, la justicia argentina fue resolviendo casos muy relevantes de grooming, acceso

indebido a cuentas bancarias, uso indebido de tarjetas electrónicas, pornografía infantil, pedofilia con uso de medios informáticos, fraude informático, etc.

Nótese que los cambios en materia penal coadyuvan a la justicia a ir resolviendo casos muy complicados en materia de delitos informáticos, pero en algunas oportunidades la normativa vigente resulta insuficiente, quedando infracciones delictivas sin resolver.

TERCERA PARTE: Repercusión de la ciberdelincuencia en la sociedad y la justicia. Seguridad informática .

Teniendo en cuenta nuestra pregunta inicial: *"Dado el carácter transnacional ¿es suficiente la normativa penal existente para impedir el avance de la ciberdelincuencia?*, considero importante para las conclusiones finales cómo repercute la ciberdelincuencia en la sociedad y en especial cómo la justicia sincroniza sus procedimientos penales.

Pero no se puede dejar de lado la seguridad informática, disciplina que abordaremos más adelante, porque permite tomar recaudos básicos para prevenir o al menos disminuir la comisión de ciberdelitos, además dentro de los objetivos planteados en la investigación se pretende brindar posibles remedios jurídicos y practicidades para detener el avance de la ciberdelincuencia.

La tecnología informática afecta profundamente al mundo laboral, el ocio y el conocimiento a nivel mundial, ya que millones de personas acceden fácil e inmediatamente a una cantidad extensa y diversa de información en línea.

Comparado a las enciclopedias y a las bibliotecas tradicionales, esta misma tecnología informática permite una descentralización repentina y extrema de la información y de los datos que se archivan de un modo virtual.

Esta situación masiva y que involucra a toda la comunidad mundial, trae aparejada la urgente necesidad de lograr una seguridad informática, que permita confiar en este magnífico avance que dispone el hombre.

La seguridad informática es una disciplina que relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

Pareciera que es imposible lograr un sistema informático 100% seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos. Para ello, es necesaria la implementación de barreras de seguridad antivirus, antiespías, encriptación de la información y uso de contraseñas.

Las empresas alertadas por estas nuevas prácticas, se ven obligadas a ser más estrictas en la selección del personal, buscando especialización técnica, pudiendo afectar en forma

negativa a la sociedad laboral, ya que la mayoría de las empresas no brindan esta clase de capacitación y muchos empleados no la poseen.

A medida que se fue masificando internet, fue aumentando el uso indebido de esta red, como así también de los denominados delincuentes cibernéticos que se mueven por el mundo virtual, incurriendo en delitos tales como la piratería informática, el fraude y el sabotaje informático, la trata de niños con fines pornográficos, amenazas, etc.

Los malhechores manipulan los datos o las operaciones, ya sea directamente o mediante los llamados gusanos o virus, que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro.

Coincidiendo con lo afirmado por el juez y jurista cordobés Arocena (2008):

> Lo cierto es que, en el ámbito de la delincuencia dolosa tradicional, el progreso tecnológico da lugar a la adopción de nuevas técnicas como instrumento que le permite producir resultados especialmente lesivos, a la vez que posibilita el surgimiento de modalidades delictivas dolosas de nuevo cuño.
>
> Pero también resultan relevantes, y quizás en mayor grado, los impactos tecnológicos en el ámbito de la delincuencia no intencional (infracciones con dolo eventual o infracciones imprudentes).

El Derecho Penal trata de proporcionar respuestas a la delincuencia transnacional, evitando paraísos jurídico–penales. Pero dar una respuesta uniforme no es fácil, impera la necesidad de una construcción supranacional que permita la armonización de los sistemas penales, conforme a principios y garantías desde un punto de vista político–criminal.

CAPÍTULO V: Repercusión social y judicial. Seguridad informática.

La empresa Symantec–Norton[31] ha realizado un complejo informe vinculado a los crímenes relacionados con la información automática de datos, brindando un análisis exhaustivo de los mismos desde un punto de vista práctico basado en estudios estadísticos. Este trabajo refleja el impacto social y los cuidados que habría que considerarlos.

De sus conclusiones se rescatan las siguientes advertencias:

Las víctimas de todo el mundo necesitan comenzar a hacer frente a los ciberdelitos:

La combinación del sentido común con el software informático apropiado, puede representar una gran diferencia a la hora de combatir el ciberdelito. Es el momento de:

- Dejar de estar paralizado por el miedo y convertir la vergüenza en fortalecimiento;
- Informar de todos los incidentes a las autoridades para ayudarles a obtener una imagen completa del ciberdelito;
- Apoyar a la comunidad global de internet mediante la realización de acciones individuales;
- Cuanto más seguro esté usted, más seguro estarán los demás.
- Todo el mundo puede contribuir.
- El sentido común es gratuito, aunque la seguridad gratuita o tan sólo un software antivirus no resulta suficiente para protegernos.
- Los ciberdelincuentes están siempre buscando formas para burlar el software de seguridad, por lo que cuanto más completo sea su suite de seguridad, más protección tendrá.
- El software correcto le protege de los ataques de los ciberdelincuentes.

V.1: Repercusión social.

Se transcribe textualmente a continuación afirmaciones con las que coincido en su totalidad:

La proliferación de los delitos informáticos ha hecho que la sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en

[31] Informe estadístico realizado por la empresa Symantec–Norton de EEUU. *La epidemia digital silenciosa. Todos podemos ser víctimas de un ciberdelito*. Recuperado el 30/06/2016 de: http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Spanish-Human%20Impact-A4_Aug11.pdf

general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo, el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general.

También se observa el grado de especialización técnica que adquieren los delincuentes para cometer este tipo de delitos, por lo que personas con conductas maliciosas cada vez más, están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global.

Las empresas que poseen activos informáticos importantes, son más celosas y exigentes en la contratación de personal para trabajar en estas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos.

Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito que aquellas que sí los poseen. En vista de lo anterior aquel porcentaje que no conoce nada de informática, por lo general personas de escasos recursos económicos, pueden ser engañados si en un momento dado, poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como internet, correo electrónico, etc.

La falta en la sociedad de cultura informática puede ser un gran impedimento para la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

Existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza por el contrario, el autor o autores de este tipo de delitos son considerados por la sociedad, como personas con habilidades y capacidad intelectual superior a la media normal, por lo que los ven merecedores de "respeto"[32].

V.2: Repercusión judicial.

Es difícil elaborar estadísticas sobre el porcentaje de personas que son víctimas de este tipo de delitos, sin embargo, se estima que la cifra es muy alta.

No es fácil descubrirlo y sancionarlo, en razón de la capacidad que tienen estos delincuentes para borrar pruebas y datos incriminatorios de quienes los cometen, pero los daños económicos son altísimos.

A medida que aumenta la delincuencia electrónica, numerosos países han promulgado leyes declarando ilegales nuevas prácticas como la piratería informática, o han actualizado leyes obsoletas para que delitos tradicionales, incluidos el fraude, el vandalismo o el sabotaje, se considera ilegales en el mundo virtual.

[32] Plus Información. *Delitos informáticos.* Publicación recuperada el 15/07/2016 de: http://plusformacion.com/Recursos/r//Delitos-informaticos#segu

Singapur, por ejemplo, enmendó su ley sobre el uso indebido de las computadoras. Ahora son más severos los castigos impuestos a todo el que interfiera con las *"computadoras protegidas"*, es decir, las que están conectadas con la seguridad nacional, la banca, las finanzas y los servicios públicos y de urgencia, así como a los transgresores por entrada, modificación, uso o intercepción de material computarizado sin autorización.

Hay países que cuentan con grupos especializados en seguir la pista a los delincuentes cibernéticos. Uno de los más antiguos es la Oficina de Investigaciones Especiales de la Fuerza Aérea de los EEUU, creada en 1978. Otro es el de Investigadores de la Internet de Australia, integrado por oficiales de la ley y peritos con avanzados conocimientos de informática. El grupo australiano recoge pruebas y las pasa a las agencias gubernamentales de represión pertinentes en el estado donde se originó el delito[33]

Tobares Catala, G. y Castro Arguello, M. (2010) sostienen que:

Pese a estos y otros esfuerzos, las autoridades aún enfrentan graves problemas en materia de informática. El principal de ellos es la facilidad con que se traspasan las fronteras, por lo que la investigación, enjuiciamiento y condena de los transgresores se convierte en un problema jurisdiccional y jurídico.

Es destacable la siguiente afirmación:

Asumiendo que no existe un estudio estadístico amplio, como sería necesario, relativo a los delitos informáticos, podemos ver que el ámbito de estos delitos está aumentando al crecer el número de posibles delincuentes y víctimas conectadas, situación más que previsible al momento de entender el perfil de aquellas personas que incursionan en el uso de estas nuevas herramientas tecnológicas, como también los lugares desde los cuales los usuarios se conectan a la red informática para acceder a las diferentes opciones que allí se presentan.

La gama de actividades delictivas parece ir aumentando a medida que las tecnologías crean nuevas oportunidades delictivas y que los delincuentes encuentran nuevas formas de aprovecharlas. Entre algunos ejemplos históricos podemos mencionar al virus "Melissa", creado y propagado en marzo de 1.999, que causo un daño de más de 10 millones de dólares solamente en los EEUU. Y el virus "Iloveyou" que en el año 2.000 infectó a 45 millones de computadoras en todo el mundo[34]

Desde hace cinco años el Instituto de Seguridad de Computadoras (CSI) en los EEUU realiza un estudio anual sobre seguridad informática y los crímenes cometidos a través de las computadoras, anunció recientemente los resultados del "5º Estudio Anual de Seguridad y

[33] Trabajo realizado por Landaverde Contreras, M. L.; Soto Campos, J. G.: Torres Lipe. J. M. (2000). *Delitos Informáticos.* Universidad de El Salvador. Recuperado el 30/06/2016 de: https.//criminalisticaencolombia.files.wordpress.com/2010/11/delito-informatico-melvin-leonardo-landaverde

[34] Ob. Cit. en Ref. 29

Delitos Informaticos" realizado a un total de 273 instituciones, principalmente grandes corporaciones y agencias de gobierno[35].

Este estudio de seguridad y delitos informáticos es dirigido por CSI con la participación de la Agencia Federal de Investigaciones (FBI) de San Francisco. Entre lo más destacable del estudio se incluye:

- **Violaciones a la seguridad informática:** El 90% de los encuestados descubrieron violaciones a la seguridad de sus computadoras en los últimos 12 meses. El 70% reportó una variedad de serias violaciones de seguridad, entre las más comunes los virus de computadoras y abusos por parte de empleados.

- **Pérdidas financieras:** El 74% reconoció pérdidas financieras debido a las violaciones de las computadoras, las pérdidas financieras ascendieron a U$S 265.589.949, cuando el promedio total anual en los últimos 3 años era de U$S 120.240.180.

Los resultados del estudio ilustran que esa amenaza del crimen por computadora a las grandes corporaciones y agencias de gobierno viene de ambos lados, tanto dentro como fuera de sus perímetros electrónicos.

Las violaciones de seguridad detectadas por los que respondieron a las encuestas incluyen ataques como: acceso no autorizado por parte del personal de la misma entidad, negativa de servicio, penetración de sistemas por parte de elementos ajenos a la entidad, robo de información protegida por derechos de propiedad intelectual, fraude financiero y sabotaje de datos y redes.

> A pesar de los diversos esfuerzos, las pérdidas reales son de difícil cuantificación, pero incluyen los costos directos de reparar sistemas y programas, la pérdida de acceso o servicio para los usuarios de datos valiosos y de ingresos procedentes de la explotación de sitios. Estos delitos necesitan también de la preparación y del mantenimiento de medidas de seguridad y de otras medidas preventivas, como factor de costo añadido. Otro costo oculto de estos incidentes es el miedo al delito cibernético, que puede perjudicar la utilización de las tecnologías o disuadir a los gobiernos y poblaciones de los países en desarrollo de hacer un uso más eficaz de ellas[36].

[35]CSI. EEUU (2013). *Delitos Informáticos.* Publicación del 05/06/2013. Recuperada el 30/07/2016 de: http://infodelito.blogspot.com.ar/2013_06_01_archive.html

[36] Naciones Unidas. Consejo Económico y Social. Comisión de Prevención del Delito y Justicia Penal. *Conclusiones del estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes sociales.* Viena, 8 al 17 de mayo de 200l.

V.3: Seguridad Informática.

Tobares Catala, G.; Castro Arguello, M. (2010) analiza lo siguiente:

> La Seguridad Informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.
>
> La seguridad significa guardar algo seguro. *Algo,* puede ser un objeto, tal como un secreto, mensaje, aplicación, archivo, sistema o una comunicación interactiva. Y respecto a *seguro*, se refiere a los medios que protegen desde el acceso, el uso o alteración no autorizada.
>
> Para guardar algo u objetos seguros, es necesario lo siguiente:
>
> - ***La autenticación:*** Promesa de identidad, es decir la prevención de suplantaciones, que se garantice que quien firma un mensaje es realmente quien dice ser.
> - ***La autorización:*** Se da permiso a una persona o grupo de personas de poder realizar ciertas funciones, al resto se le niega el permiso y se les sanciona si lo realizan.
> - ***La privacidad o confidencialidad:*** Es el más obvio de los aspectos y se refiere a que la información solo pueda ser conocida por individuos autorizados.

Posiblemente otros doctrinarios aporten otros elementos a tener en cuenta cuando se refieren a la seguridad informática, pero los conceptos vertidos por Tobares Catala y Castro Arguello (2010) sirven a la investigación que se está concluyendo.

V.3.1: Seguridad contra los delitos informáticos .

Actualmente muchos usuarios del servicio de internet no confían en la seguridad del mismo.

En 1.996 IDC Research, el principal proveedor mundial de inteligencia para los mercados de tecnología de la información, telecomunicaciones y tecnología de consumo, realizó una encuesta en donde el 91% de los usuarios expresaron gran interés sobre la seguridad de internet, pues temen que alguien pueda conseguir el número de su tarjeta de crédito mediante el uso de la red, y otros datos importantes que afecten su economía, vida privada o laboral.

La Seguridad Informática busca disminuir la infinidad de ataques contra la privacidad, especialmente en la comunicación de los datos, por ejemplo:

- ✓ **La integridad de los datos:** Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte o lo borre.

- ✓ **La disponibilidad de la información:** Comprende a la seguridad que la información pueda ser recuperada en el momento que se necesite, es decir, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

- ✓ **Medidas de seguridad:** Existen numerosas técnicas para proteger la integridad de los sistemas y lo primero que se debe hacer es diseñar una política de seguridad. Autores especializados en Seguridad Informática recomiendan medidas a tener en cuenta, que se pueden sintetizar de la siguiente manera: *1) Medidas relacionadas con el equipo:* actualizar regularmente el sistema, instalar antivirus, instalar un firewall; *2) Medidas relacionadas con la navegación en internet y la utilización del correo electrónico:* utilizar contraseñas seguras, navegar por páginas web seguras y confiables, tener cuidado con programas de acceso remoto, atención especial de correos electrónicos.

- ✓ **Firma digital:**

> Es la solución a muchos problemas respecto a la seguridad en la red, ya que se adapta a los soportes tecnológicos, por los que se contrata y además otorga mayor seguridad, teniendo en cuenta la particularidad de estar equiparada a la firma manuscrita[37].

Su particularidad es que es una clave asimétrica, de doble encriptación, tiene una clave pública y otra privada, es la más segura para contratar electrónicamente. Por eso las empresas deberían comenzar a incorporar mecanismos para que la firma digital sea posible de ser usada en sus transacciones.

> Expertos en seguridad nos indican cómo cuidar nuestras casas y hasta animan a alentarnos sobre salideras bancarias, pero pocos nos indican sobre la inseguridad a la que nos exponemos cuando compartimos información en las redes sociales.
>
> Son diversas las dificultades con los que se enfrenta el derecho a la hora de juzgar un caso de delincuencia relacionado con lo informático. Aníbal Pardini, profesor de Derecho Informático de la Facultad de Derecho y Ciencias Sociales de nuestra universidad, sostiene que la poca posibilidad de

[37] González Unsueta, C. (2009). Gocourse. Informática Jurídica. Universidad Empresarial Siglo 21

vincular a una persona determinada con el hecho, la volatilidad de la prueba y la falta de herramientas jurídico–procesales (al no estar regulada la llamada "cadena de custodia") hacen que la tarea de la justicia sea realmente faraónica y exija una preparación específica, la cual no siempre está.

Con respecto a la prevención efectiva ante la criminalidad informática, lamentablemente no existen recetas, pero Pardini subraya:

- ✓ La importancia de acciones de capacitación y difusión.
- ✓ Capacitación sobre el uso de los medios electrónicos y las falencias que representan, y difusión de los modus operandi de los delincuentes para poner sobre aviso a las posibles víctimas.
- ✓ Pero también agrega un tercer punto: conocer las posibilidades de denuncia y saber cómo actuar ante un posible delito. En este caso aconseja no borrar la información de la computadora ni reenviar los mensajes, denunciar inmediatamente y guardar toda la evidencia posible[38].

[38] Universidad Católica de Córdoba (2015). *Delitos Informáticos.* Publicado el 24/08/2015 en Actualidad. Recuperado el 24/05/2016 de: http://www2.ucc.edu.ar/noticiasucc/delitos-informaticos/

CONCLUSIONES

Con relación a la conceptualización de los delitos informáticos, no existían a nivel mundial estos delitos, por no encuadrarse en tipología alguna y por no encontrarse bienes jurídicos a tutelar por el derecho, esto determinó en los inicios de los ciberdelitos la imposibilidad de ser sancionados y a medida que la tecnología informática avanzaba, aparecieron nuevas formas delictivas.

Para dar marco regulatorio a los delitos cibernéticos cometidos por sujetos especializados en informática, los distintos países mediante las medidas implementadas a través de convenios, tratados u otros instrumentos internacionales, actualizaron su normativa penal encuadrando estas conductas delictivas ya no en figuras típicas tradicionales sino en delitos especiales propios derivados de la actividad informática.

Es conveniente que esta nueva disciplina normativa responda a principios generales del derecho, para disminuir la necesidad de introducir variaciones constantes en las mismas y que los órganos encargados de aplicar esas normas no encuentren inconvenientes en su aplicación.

Aparecieron diversos bienes jurídicos protegidos denominados: privacidad, derecho de autor, publicidad electrónica, tránsito, medios de transporte y de comunicación informática, etc. Respecto de los tipos penales legislados existe cierta coincidencia entre los países en sus denominaciones: delitos contra la integridad sexual, violación de secretos y privacidad, sabotaje, acceso ilegítimo a un sistema informático, estafa y fraude informático, daño informático, piratería, etc.

En nuestro país se tipificaron diversos ilícitos relacionados con la cibernética, posibilitando el llenado de lagunas de punición que existían en nuestro derecho, mientras que a nivel internacional y regional (Mercosur), existen instrumentos jurídicos que sugieren a los países el tratamiento legislativo en la materia de estudio, sin embargo, las leyes vigentes no son suficientes para bajar los índices de delincuencia informática.

La normativa actual en nuestro país respecto de los ciberdelitos responde a la *completitud*, ya que ha posibilitado la eliminación de lagunas antes existentes. Responde también a una *coherencia* porque no existen soluciones diferentes. Hasta la actualidad no se observa *redundancia* entre las figuras normativas respondiendo todas a una misma línea lógica deóntica. El inconveniente suscitaría ante el devenir de nuevos delitos vinculados con

esta actividad, trayendo como consecuencia que las normas quedaran obsoletas, perdiendo de este modo la *eficacia* que dichas normas actualmente lo poseen.

Además de que la realidad actual requiere de una legislación que sea compatible con los distintos países, es necesaria una solución global con cooperación internacional por ser ésta el mecanismo adecuado para combatir la delincuencia informática, por tanto, urge un planteamiento integral, completo y colectivo de los diversos sectores para combatir la delincuencia informática.

Debería surgir también la coordinada implementación de investigaciones, es decir en forma cooperativa, porque para lograr el objetivo principal de disminución de los ilícitos cibernéticos, no coadyuvan los trabajos asilados de las fuerzas de seguridad o fuerzas armadas de los estados afectados. Es prioritario que la misma se lleve a cabo mediante un proceso de armonización internacional, que se presenta como una necesidad ineludible y no con movimientos normativos aislados, como se llevó a cabo en nuestro país.

El Derecho Procesal Penal tiene un rol fundamental y necesita avanzar de manera adecuada en el procedimiento de la investigación de la cibercriminalidad. La buena técnica de haber incorporado los delitos informáticos al Código Penal, debería estar acompañado de técnicas procesales para la investigación de estos casos, muchas veces muy complejos, esto implica fiscales y jueces especializados conforme a la normativa penal especial que cada estado debería tener correctamente delimitado, y no en normas dispersas en los Códigos Penales locales.

Las repercusiones sociales y judiciales que traen aparejadas los delitos informáticos, impone considerar una seguridad informática basada en medidas preventivas que contengan: autenticación y privacidad adecuada, para dar seguridad a la integridad de los datos y a la disponibilidad de la información.

En definitiva, actualmente las regulaciones penales de los estados prevén su tipicidad y régimen sancionatorio, pero estas normativas precisan actualización constante, además que se potencie la seguridad informática y que los controles sobre el uso de tecnologías informáticas sean estrictos, por su masividad y los perjuicios que causan a usuarios y empresas.

GLOSARIO DE TERMINOLOGÍA INFORMÁTICA

- ***Adware:*** Programa que difunde publicidad a través de banners, ventanas emergentes, etc. mientras está funcionando. Genera polémica porque en algunos casos se cede a terceros información de los usuarios sin su consentimiento.

- ***Antivirus:*** Programas que se utilizan con el fin de prevenir y detectar posibles infecciones producidas por virus y todo tipo de programas maliciosos, y reparar los daños que éstas hayan podido causar.

- ***Backdoor:*** Puerta trasera que tiene una especial secuencia dentro del código de programación mediante la cual el programador puede acceder o escapar de un programa en caso de emergencia o contingencia en algún problema. A su vez, estas puertas también pueden ser perjudiciales debido a que los crackers al descubrirlas pueden acceder a un sistema sin conocimiento por parte del usuario.

- ***Bomba atómica:*** Programa que se instala en un equipo y se mantiene inactivo, en espera de que se cumplan una serie de requisitos o condiciones. Cuando se ejecutan las condiciones de activación pueden ordenar que: se realice una transferencia bancaria, dañar un sistema, borrar datos del disco duro, etc.

- ***Cibercrimen:*** Delitos cometidos a través de medios electrónicos de información de datos.

- ***Cibernética:*** Ciencia que estudia los sistemas de comunicación y de regulación automática de los seres vivos y los aplica a sistemas electrónicos y mecánicos que se parecen a ellos.

- ***Computadora u ordenador:*** Máquina electrónica que recibe y procesa datos para convertirlos en información útil.

- ***Cracker:*** Es aquel que rompe con la seguridad de un sistema con la intención de destruir datos, denegando el servicio a usuarios legítimos, es sinónimo de rotura.

- ***Crimeware:*** Programas diseñados para obtener beneficios económicos, mediante la comisión de todo tipo de delitos online, estos son: plishing, spam, adware, etc.

- ***Daño informático:*** Se denomina así a todo ataque, borrado, destrucción o alteración intencional de bienes intangibles. La incriminación tiende a proteger a los usuarios.

- ***Delito informático:*** No existe una definicion formal y universal, en algunos países como el nuestro existe tipificación de los mismos, en otros no, el mismo se lleva a cabo a través de un medio electrónico de datos, para cometer fraudes, estafas y otras manifestaciones dañinas de los equipos computarizados.

- ***Dialer:*** Programa que modifica datos de acceso a internet para que al conectarse utilice un número de tarificación adicional, cuyos costos son superiores.

- ***Dispositivo:*** Aparato, artificio, mecanismo, órgano o elemento de un sistema.

- ***Exploit:*** Programa que aprovecha los fallos de seguridad, defectos o vulnerabilidades de otros programas o sistemas, con el fin de obtener algún tipo de beneficio, por ejemplo, acceder a recursos protegidos, controlar sistemas sin autorización, etc.

- ***Firewall:*** Contrafuegos es un mecanismo de seguridad que regula el acceso entre dos o más redes, teniendo en cuenta la política de seguridad establecida por la organización responsable de la red.

- ***Firma digital:*** Conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. La huella digital del firmante se encripta y el firmante posee una marca única.

- ***Flood o flooder:*** Programa que se utiliza para enviar mensajes repetidamente en forma masiva mediante correo electrónico, sistemas de mensajería instantánea, chats, foros, etc., su objetivo es producir el colapso de los sistemas.

- ***Gusano:*** Similares a los virus, capaces de realizar copias de sí mismos y programarse a través de la red para infectar equipos, sin la autorización de los usuarios.

- ***Hacker:*** Persona que disfruta husmear los sistemas programables, es un delincuente silencioso y tecnológico, son capaces de crear sus propios softwares para entrar a los sistemas, no pretende producir daños e incluso se apoya en un código ético, aunque el mero hecho de colocarse en un sistema ya es delito.

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

- ***Hijacking:*** Técnicas utilizadas para adueñarse o secuestrar páginas web, conexiones de internet, dominios, Ips, etc.

- ***Hoax:*** Mensaje de correo electrónico con información engañosa, se caracterizan por solicitar al destinatario que reenvíe el mensaje a todos sus contactos, para captar correos de usuarios y enviar spam, virus, etc.

- ***Informática:*** Ciencia que estudia el tratamiento de la información en un ordenador, dispositivo o sistemas electrónicos.

- ***IP:*** Protocolo para la comunicación en red a través de paquetes conmutados principalmente usado en computadoras por internet.

- ***Keylogger:*** Programa o dispositivo que registra las combinaciones de teclas pulsadas por los usuarios y las almacena para obtener datos confidenciales como contraseñas, contenido de mensajes electrónicos, etc.

- ***Malware:*** Programas maliciosos que buscan obtener un determinado beneficio, produciendo perjuicios al sistema o al usuario.

- ***Pharming:*** Modalidad de estafa online manipulando DNS (Nombre de Dominio del Servidor) para redireccionar el nombre de un dominio, visitado habitualmente por el usuario, para obtener datos confidenciales, datos bancarios, etc.

- ***Phreacker:*** Es el especialista en telefonía, arte y ciencia del sujeto para obtener beneficios personales, necesita conocimientos sobre informática, ya que la telefonía celular o el control de centralitas emplea informática.

- ***Plishing:*** Fraude informático que pretende conseguir datos como contraseñas o acceso a cuentas bancarias. Crean páginas similares a las originales para que, ingresando el usuario al mismo, sea defraudado para conseguir beneficios económicos.

- ***Scam o plishing laboral:*** Similar al plishing creado para datos confidenciales, también se engaña enviando mensajes masivos, donde al ingresar el usuario se produce el daño.

- ***Seguridad informática:*** Disciplina relacionada con técnicas, aplicaciones y dispositivos para asegurar la integridad y privacidad de los usuarios.

- ***SMiShing:*** Variante del plishing utilizando mensajes a teléfonos móviles para realizar el ataque, el objetivo es el mismo.

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

- ***Spam:*** Correos masivos no solicitados con contenido publicitario que se realiza a través de foros, blogs, etc.

- ***Spear plishing:*** Tipo de plishing que no utiliza mensajes sino concretos, consiguiendo que los mensajes resulten más creíbles que los plishing tradicional.

- ***Spyware o programa espía:*** Programa cuyo objetivo es recopilar información del usuario del sistema en el que se instala, puede realizarse con consentimiento del usuario.

- ***Troyano:*** Programa ejecutable que aparenta realizar una tarea determinada para engañar al usuario con el fin de controlar el equipo, robar información confidencial, borrar datos, etc., no se replican a sí mismos.

BIBLIOGRAFÍA

⇒ *Doctrina*

Arocena, G. (2008). *Sobre la regulación de los delitos informáticos en el Código Penal Argentino – Introducción a la Ley Nacional Nº 26.388.* Recuperado el 17/06/2016 de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002#nota

Balanta, H. (2009). Ponencia presentada en el II Congreso Internacional de Criminología y Derecho Penal. Colombia. *Aproximación Legal a los delitos informáticos. Una visión de derecho comparado.* Recuperado el 30/06/2016 de: http://es.slideshare.net/Derechotics/34849363-aproximacionlegalaltratamientodelosdelitosinformaticosencolombia.

Benderelli, J. (2016). *Informática Forense.* Publicación recuperada el 08/05/2016 de: http://www.benderelli.com.ar/

Borghello, C.F. (2001). *Seguridad Informática: sus implicancias e implementación.* Tesis en Licenciatura en Sistemas. Universidad Tecnológica Nacional. Recuperado el 27/05/2016 de: http://www.segu-info.com.ar/tesis/

Cárdenas, C. (2008). *"El lugar de comisión de los denominados ciberdelitos"*. Política Criminal Nº 6. 2008. A2 – 6. Recuperado el 29/06/2016 de: http//www.politicacriminal.cl/n_06/A_2_6.pdf

Centro de Estudios y Datos (CEDATOS) (2011). *Seguridad en la ciudad.* Estudio de opinión, abril 2011. Colombia. Publicación Recuperada el 16/07/2016 de: http://www.cedatos.com.ec/quienes_somos.php

CSI. EEUU (2013). *Delitos Informáticos.* Publicación del 05/06/2013. Recuperada el 30/07/2016 de: http://infodelito.blogspot.com.ar/2013_06_01_archive.html

Cysi. *Estudio de Informática Forense.* Publicación recuperada de: http://cysi.com.ar/

De Langhe, M., Rebequi J.M. (2008). Comentario al Artículo 157 bis. AAA-VV. *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial.* Baigún D.-Zaffaroni, E.R.-Terragni, M.A. Buenos Aires: Hammurabi. Tº 5 p.811.

Del Pino. S.A. (2005). *Delitos Informáticos.* Publicación recuperada *el* 11/17/2016 de: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Delitos Informáticos. Publicación recuperada el 08/05/2016 de: http://www.delitosinformaticos.com.ar

Diario Infobae. http://www.infobaeprofesional.com

Diario la Gaceta. http://www.lagaceta.com.ar

Diario La Nación. http://www.lanacion.com.ar

Faraldo Cabana, P. (2007). *Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática.* Recuperado el 15/07/2016 de: http://www.ehu.eus/documents/1736829/2176629/02+Faraldo.indd.pdf

Fernández Delpech, H. (2016). *Derecho Informático Internet.* Recuperado el 12/07/2016 de: http://www.hfernandezdelpech.com.ar

García de la Cruz, J.M. (2009). *Delitos Informaticos.* México DF: El Cid Editor/Apuntes.

Gelli, M. A. (2008). *Constitución de la Nación Argentina Comentada y Concordada.* (4ª Ed. 2008). (1ª Reimpresión 2008). Tº I p. 276 y ss. Buenos Aires: La Ley.

González Unsueta, C. (2009). Gocourse. Informática Jurídica. Universidad Empresarial Siglo 21.

Hernández, A. (2006). *Delitos Informáticos*. Publicación digital de octubre de 2006. Recuperado el 23/06/2016 de: http://www.delitosinformaticos.com

Información Legislativa y Gubernamental (Infoleg). http://infoleg.gov.ar.

Informática Forense y Pericial. Salmerón, A. (2015) en su artículo *"Derecho Informático".* Recuperado el 26/02/17 de: http://forense.info/articulos/informaticayderechopenal.html

Informe estadístico realizado por la empresa Symantec–Norton de EEUU. *La epidemia digital silenciosa. Todos podemos ser víctimas de un ciberdelito*. Recuperado el 30/06/2016 de: http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Spanish-Human%20Impact-A4_Aug11.pdf

Justiniano.com. Costa Hoevel, S. A. (2006). Artículo publicado sobre *"Delitos informáticos. Aspectos jurídico-penales a la luz de la Teoría del Delito"*. Recuperado el 15/10/16 en: https://www.justiniano.com/revista_doctrina/delitoinformatico.htm

Landaverde Contreras. M.L.; Soto Campos, J.C.; Torres Lipe; J.M. (2000). *Delitos Informáticos.* Universidad de El Salvador. Recuperado el 30/06/2016 de: https://criminalisticaencolombia.files.wordpress.com/2010/11/delito-informatico-melvin-leonardo-landaverde-contreras3.pdf

Levene, R; Chiaravalotti, A. (1998). *Delitos Informáticos.* Publicación digital recuperada el 14/07/2016 de: http://abogadoszulia.org.ve/eavillalobos/wp-content/uploads/2015/06/Unidad-uno.pdf

Librería Virtual. Red Iberoamericana. *El Derecho Informático.* Recuperado el 08/05/2016 de: http://elderechoinformatico.com/wordpress/

Lima, M. (1984). Criminalia Nº 1-6 Año L. *Delitos Electrónicos.* Academia Mexicana de Ciencias Penales. Enero-Julio 1984. México: Ed. Porrua.

Lorenzetti, R.L. (2001). *Responsabilidad por daños en Internet, en Derecho Privado. Homenaje al Dr. Alberto Bueres.* Oscar Ameal (Director). Buenos Aires: Hammurabi.

Lucero, P.G., Kohen. A.A. (2010). *"Delitos Informáticos"* (269). Buenos Aires: Ediciones D&D.

Luzón Peña, D. M. (1999). *Curso de Derecho Penal. Parte General.* (Ed. 1ª, 1ª Reimpresión). (Tº I, pág. 82). Madrid: Ed. Universitas).

Mariani & Asociados (1999). *Delitos Informáticos. Nociones de Derecho Informático.* Paper del año 1998/1999. Recuperado el 08/05/2016 de: http://www.mariani-abogados.com.ar/detalle.php?a=delitos-informaticos&t=9&d=256

Mesegger González, J. de D. (2013). *La comprensión psicojurídica de los ciberdelincuentes y cibercriminales.* LexNews. Publicación del 13/05/2013 recuperada el 01/05/2016 de: http://www.lexnews.es/la-comprension-psicojuridica-de-los-ciberdelincuentes-y-cibercriminales/

Ministerio Público Fiscal de Córdoba: http://www.mpfcordoba.gob.ar/delitos-informaticos/

Nino, C.S. (2000). *Fundamentos de derecho constitucional. Análisis filosófico, jurídico y politólogo de la práctica constitucional.* (1ª Ed., lª Reimpresión). (Tº V p. 304). Buenos Aires: Astrea.

Núñez, R. (1987). *Manual de Derecho Penal. Parte General.* (Ed. 3ª p.79). Córdoba: Lerner Editora S.R.L.

Pallazzi, P. A. (2012). *Los delitos informáticos en el Código Penal.* (Ed. 2ª), Buenos Aires: Abeledo Perrot. Pág. 75.

Piña Libien, H. R. *El Derecho Informático y su autonomía como nueva rama del derecho".* Publicación recuperada el 08/09/2016 de: http://ordenjuridico.gob.mx/Congreso/pdf/78.pdf

Plus Información. *Delitos informáticos.* Publicación recuperada el 15/07/2016 de: http://plusformacion.com/Recursos/r//Delitos-informaticos#segu

Real Academia Española: http://www.rae.es/rae

Riquert, M.A. (2006). Ponencia VI Encuentro Argentino de Profesores de Derecho Penal. "*Estado de la legislación contra la delincuencia informática en el Mercosur"*. Recuperado el 30/06/2016 de: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_88.pdf

SAIJ. *"Piratería de software, nueva Ley 25.036".* Prunotto Laborde, A. COLECCIÓN ZEUS – DOCTRINA. Recuperado el 27/02/2017 de: http://www.saij.gob.ar/adolfo-prunotto-laborde-pirateria-software-nueva-ley-25036-dasf060047/123456789-0abc-defg7400-60fsanirtcod

Sain, G. (2013). *"El Derecho aplicado a los delitos informáticos: ¿Una política eficiente para el cibercrimen?* SAIJ. Publicado el 18/06/2013. Recuperado el 06/05/2016 de: http://www.saij.gob.ar/

Sosa Baccarelli, N. (2010). *Delitos contra el honor. Aportes para un análisis de la reforma de la Ley 26.551 al Código Penal Argentino* (27). Buenos Aires. Recuperado el 08/05/2016 de: http://www.pensamientopenal.com.ar/system/files/2011/05/doctrina28925.pdf

Téllez Valdez, J. (1996). *Derecho Informático (171).* (Ed. 2ª). México: Mc Graw Hill.

Tobares Catala, G.; Castro Arguello, M. (2010). *Delitos Informáticos.* (281). Prólogo de Sayago, M. Córdoba: Advocatus Ediciones.

Universidad Católica de Córdoba (2015). *Delitos Informáticos.* Publicado el 24/08/2015 en Actualidad. Recuperado el 24/05/2016 de: http://www2.ucc.edu.ar/noticiasucc/delitos-informaticos/

UNIVERSIDAD LAICA DE ELOY ALFARO DE MANABI (2014). *Derecho Informático y Delito Informático.* Publicación del 23 de octubre de 2014 y recuperada el 12/08/2016 de: https://www.jeanvilla.wordpress.com/2014/10/23/derecho-informatico-y-delito-informatico/

Zaffaroni, R.E. (2010). *Manual de Derecho Penal. Parte General.* (Ed. 2010) (800 páginas). Buenos Aires: Ediar.

⇒ *Legislación*

Código Civil y Comercial Comentado. Tratado Exegético. Alterini, J. H. Director General (2015). Tomos I al XI.

Código Contravencional de la Ciudad de Buenos Aires. Acceso a Material Pornográfico. Informática Legal. Publicación recuperada el 17/06/2016 de: http://www.informaticalegal.com.ar./legislacion-informatica/

Código Penal Comentado Anotado con Jurisprudencia. Dayenoff, D. A. (2010). (10ª Ed. 2010). Buenos Aires: García Alonso.

Código Procesal Penal de la Nación. (5ª Ed.). Códigos de Estudio. Buenos Aires: Editorial Estudio.

Código Procesal Penal de la Provincia de Córdoba Comentado. Tomo I y II. Ley 8.123 y sus modificaciones. Cafferata Nores J.I., Tarditti, A. (2003). Córdoba: Ed. Mediterránea.

Constitución de la Nación Argentina Comentada y Concordada. Tomo I y II. Gelli, M. A. (2008). (4ª Ed. 2008). 1ª Reimpresión 2008). Buenos Aires: La Ley.

Decreto 415/2006. Reglamentario de la Ley 26.061 de Protección Integral de los Derechos de Niñas, Niños y Adolescentes. Información Legal. Recuperado el 17/06/2016 de: http://www.informaticalegal.com.ar/legislacion-informatica/

Ley Nº 25.036 de Piratería de Software. Recuperado el 09/05/2016 de: http://www.infoleg.gov.ar/infolegInternet/anexos/50000-54999/54178/norma.htm

Ley Nº 26.061 de Protección Integral de los Derechos de Niñas, Niños y Adolescentes. Informática Legal. Recuperado el 17/06/2016 de: http://www.informaticalegal.com.ar/legislacion-informatica/

Ley Nº 26.388 de Delitos Informáticos. Recuperado el 06/05/2016 de: http//infoleg.mecon.gov.ar/infolegInternet/anexos/135000-139999/135314/norma.htm

Ley Nº 26.551 de Despenalización de Calumnias e Injurias en Asuntos de Interés Público. Recuperado el 06/05/2016 de: http://www.infoleg.mecon.gov.ar/infolegInternet/verNorma.do?id=160774

Ley Nº 26.904 de Grooming. Incorpora el Art. 131 del Código Penal. Informática Legal. Recuperado el 17/06/2016 de: http://www.informaticalegal.com.ar/legislacion-informatica/

Ley Nº 863 de la Legislatura de la CABA. Internet con páginas pornográficas. Informática Legal. Recuperado el 17/06/2016 de: http://www.informaticalegal.com.ar/legislacion-informatica/

⇒ *Instrumentos Internacionales*

Convención Americana de Derechos Humanos. Costa Rica. 22/11/1969. Ley 23.054.

Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional. Recuperado el 06/06/2016 de: http://www.unodc.org/documents/peruandecuador/Publicaciones/tocebook.pdf

Convenio sobre Cibercriminalidad de Budapest. Recuperado el 06/05/2016 de: http://www.coe.int/t/dghl/cooperation/econoccrime/Source/Cybercrime/TCY/ETS_185_spaish.PDF

Declaración Universal de Derechos Humanos. Res. 217 A (III) de la Asamblea General de las Naciones Unidas. 10/12/1948.

Naciones Unidas. Consejo Económico y Social. Comisión de Prevención del Delito y Justicia Penal. *Conclusiones del estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes sociales.* Viena, 8 al 17 de mayo de 200l.

Pacto Internacional de Derechos Civiles y Políticos. Nueva York. 19/11/1966. Ley 23.313.

⇒ *Jurisprudencia*

Corte Federal de Apelaciones del 9º Circuito de los EEUU. (12/02/2001). *"RIAA vs. Nasper Inc. s/violación de derechos de autor y asociación ilícita.* San Francisco, EEUU.

CSJN. Fallo 306:1892. *"Ponzetti de Balbín, Indalia c/Editorial Atlántida S.A.".* Buenos Aires, 11/12/1984.

CSJN. *"Baldivieso, César Alejandro s/Causa Nº 4733".* Publicado en La Ley el 26/05/2010, p. 7. Buenos Aires, 20/04/2010.

CNCC. Sala VI, 02/12/1999. *"Lanata, Jorge s/Excepción de Falta de Acción".* Buenos Aires.

CNACC. Sala VI. Causa 40.376. *"N.N. Dam. G., S. D. s/Competencia".* Buenos Aires, 22/10/2010.

CNCP de Capital Federal. Sala 1. Sentencia 547 del 19/07/1997. *"Autodesk Inc. s/Recurso de Casación".*

CSJN. Fallo 314: 1517. *"Vago, Jorge Antonio c/Ediciones de la Urraca S.A.* 12/06/1992.

CSJN. Fallo 332: 2559. *"Brugo, Jorge Ángel c/Lanata, Jorge y otros.* 16/11/2009.

CSJN. Fallo 319: 2741. *"Morales Solá, Joaquín c/Giadone, Dante.* 02/11/1996.

CSJN. Fallo 320: 1273. *"Pandolfi, Oscar Raúl c/Rajneri, Julio Raúl.* 01/07/1997.

CNCC. Sala 6ª, 30/04/1993. *"Pinamonti, Orlando M."*. JA 1995-III-236. Buenos Aires.

CNCC. Sala I, 13/03/2002. Juzgado 10, Secretaría 20. *"Vita, Leonardo G. y González Eggers, Matías"*. Buenos Aires.

CNCC. Sala III, 04/06/1992. Sent. "S", Sec. 23, 30.725. *"Iglesias, Carlos M. s/defraudación"*. Buenos Aires.

CNCC. Sala I. *"Grimberg, Alfredo H. s/sobreseimiento"*. Buenos Aires, 11/02/2003.

CLabCABA. Sala VII. *"Pereyra, Leonardo R. c/Servicios de Almacén Fiscal Zona Franca y Mandatos SA s/despido.* CABA, 27/03/2003.

CNApLab. Sala X. *"GDM del R c/YPF s/despido.* Expte. Nº 9337/02 (17095). Buenos Aires, 12/08/2002.

Corte Suprema de Canadá (1979). *Caso "Compo Co. Ltd. Vs. Blue Crest Music et al.".* S.C.R. 357-

Juzgado Comercial Nº 18. Secretaría 36. *"GDE c/C SA s/diligencia preliminar".* Expte. 39749. Buenos Aires, 23/10/2001.

Juzgado Nacional de 1ª Instancia Nº 75. *"Da Cunha, Virginia c/Yahoo de Argentina SRL y otro"*. Buenos Aires, 29/07/2009.

Juzgado Nacional en lo Criminal de Instrucción Nº 38. *"Ardita, Julio C. s/defraudación.* Buenos Aires. JC 1996-V-391.

USCA. Second Circuit, *"United States v. Morris".* F.2d 504. 1991.

USDC. District of Massachusetts. *"United States vs. La Macchia". 871.* F. Supp. 535. 1994.

⇒ ***Biblioteca Consultada***

Biblioteca de la UNIVERSIDAD NACIONAL DE LA PAMPA.

Biblioteca del SUPERIOR TRIBUNAL DE JUSTCIA (STJ) DE LA PAMPA.

eBook21. Librería Virtual. Universidad Empresarial Siglo 21. http://ecampus.uesiglo21.edu.ar/menu/