TRABAJO FINAL DE GRADUACIÓN

Delitos informáticos

Agustina Haarscher
VABG1766
Mayo, 2012
ABOGACIA

Índice general

Introducción:

En los últimos 10 años, el desarrollo de la tecnología informática, su masividad en distintos sectores sociales, su fácil y rápido acceso, ha llevado a que internet se convirtiera en uno de los principales medios de comunicación, logrando achicar distancias, mantener abiertos los mercados 24hs, e infinidades de beneficios que brinda este avance tecnológico.

Pero su gran influencia en casi todas las áreas de la vida del hombre, ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables, los llamados delitos informáticos.

La informática reúne las características necesarias que la convierten en un medio idóneo para la comisión de distintas modalidades delictivas, en especial de carácter patrimonial. La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente comodidad de acceso a ellos y la fácil manipulación de esos datos.

La cuantía de los perjuicios ocasionados vía red, son en algunos casos muy superiores a la causada en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrir o castigar al verdadero delincuente.

Manipular fraudulentamente sistemas bancarios o acceder indebidamente a información privada, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos, mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños morales.

En la mayoría de los casos se trata de una delincuencia de especialistas, que tienen la capacidad de borrar toda huella de los hechos y lograr que éstos delitos no tengan culpables visibles.

En la actualidad, las computadoras portátiles, los teléfonos celulares de alta gama, agendas digitales, entre otros, han logrado que los resultados de los delitos sean más “eficientes”.

Con la ley 26.388, sancionada en el 2008, la Argentina se encuentra en América latina a la vanguardia de la legislación de delitos informáticos, pero todavía quedan varias “lagunas” pendientes por legislar.

En este trabajo, vamos a poder conocer algunas de las formas en que se puede comer un delito informático, cómo está regulado en Argentina ese aspecto y cuáles son esos vacíos que todavía no están legislados.

¿Con la llegada de los delitos informáticos, estaremos ante la presencia del crimen perfecto…?

.

Objetivos

- Realizar una investigación profunda acerca de esta nueva modalidad de delinquir, los llamados delitos informáticos, analizando doctrina especifica.

- Conceptualizar a que se llama delito informático, demostrar porqué se los denomina delitos de cuello blanco.

- Estudiar las características de estos delitos, sus particularidades, formas y medios de comisión,

- Analizar en profundidad cada tipo de delito informático, respetando la trilogía presentada por la ONU para reconocer a esta clase de delitos.

- Presentar los medios por los cuales cometen estos delitos, y analizar sus características y funciones. Ya que estos son medios novedosos que presentan particularidades que los convierten en velos para cubrir al delincuente, y dificultar la investigación.

- Investigar cómo impacta en la sociedad la incertidumbre que generan estos delitos, cuales son los medios para denunciar esta modalidad delictiva.

- Estudiar detenidamente la modificación del código penal, mediante la ley 26.388, y ahondar en las lagunas jurídicas respecto al tema.

- Averiguar porque es tan difícil identificar a los autores de estos delitos. En este trabajo nos responderemos la siguiente pregunta: ¿Es imposible encontrar al autor?

- Mostrar indicadores estadísticos referentes a estos actos delictivos.

Metodología

Para el desarrollo de este proyecto, primero se llevó a cabo la elección del tema a desarrollar, buscando que sea novedoso y entretenido. Para ello se seleccionaron datos, doctrina, jurisprudencia y estadísticas, para verificar que su realización fuera viable.

Después se trazaron los objetivos que aspiramos alcanzar con este trabajo, trazando un plan de acción, para lograrlos. Teniendo en cuenta cual es el enfoque que le queremos dar al tema, a quien estaba destinada su lectura, y cuál es el fin del proyecto.

Con toda la información necesaria para poder trabajar en el tema, se construye un esquema jerárquico, que nos permite obtener la pauta del diseño del trabajo, y de esta manera evitar acciones y conceptos similares que se repitan, para que no se dupliquen recursos ni esfuerzos, ni tampoco caer en una sobreabundancia de información que torne tediosa su lectura.

La estrategia utilizada en éste trabajo es analizar toda la información nacional, teniendo un particular interés en ver cómo repercute en la sociedad este tipo de delitos, como así también cuales son las expectativas de que se los controle, y cuáles son los mayores miedos sobre su posible expansión.

El plan de acción será llevado a cabo mediante la exposición del tema en cuestión, usando como forma de organización de la información la división del trabajo en capítulos y sub capítulos, para poder hacer más fácil y práctica su lectura como así también localizar de manera rápida la información.

La conclusión será realizada de acuerdo a los objetivos trazados. Plasmando en ella cual fue el desenlace al que arribamos, teniendo en cuenta cuales fueron los alcances y limitaciones que tuvo la investigación.

Capítulo 1:

La informatización y el delito

A lo largo de la historia, el hombre ha necesitado transmitir y manejar la información de forma continua. Quedan en el recuerdo las señales de humo y los destellos con espejos.

Movidos por la necesidad de encontrar mecanismos de fácil y rápido acceso, la humanidad no ha cesado en la creación de métodos para procesar información. Con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de estas máquinas y métodos, y con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos[1].

Luego, en los años sesenta, nace Internet como una tecnología que pondría años después a la cultura, la ciencia y la información al alcance de millones de personas de todo el mundo.

En la actualidad, las computadoras dejaron de usarse como una herramienta auxiliar para realizar distintas actividades de la vida humana; hoy se han convertido en el medio principal y más eficaz para obtener, procesar, almacenar y transmitir información de distintos tipos.

Las tareas ejecutadas manualmente fueron reemplazadas casi por completo, por los sistemas de información.

Hasta hace unos años, el esfuerzo humano jugaba un papel determinante en el procesamiento de datos y las máquinas únicamente cumplían el rol de equipos complementarios para imprimir esos datos.

Los sistemas de operación cada vez son 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 todavía no ha llegado a su techo, la perspectiva de su ampliación no tiene límites previsibles, aún los partícipes de este proceso se impresionan de su avance.

Actualmente todos los aspectos de la vida social, laboral, gubernamental y privada se encuentran empapados de este nuevo fenómeno de la informatización, lo que permitió un cuadro de posibilidades licitas e ilícitas. Por ello es fundamental la regulación jurídica de los múltiples efectos de una situación nueva y con tantas potencialidades en el medio social.

[1] http://www.delitosinformaticos.com autor: Andrés Hernández , octubre, 2006

Hasta hace unos años se consideraba al periodismo como el más importante “poder social”, ahora llegó a pensarse en la informática y sus acciones como el reemplazante del primer puesto.

El proceso de informatización de casi todos los campos de la vida moderna, ha llevado a que el caudal de conocimiento, que antes se operaba manualmente, ahora pueda obtenerse en segundos o minutos, transmitirse enormes documentos y llegar al receptor mediante sistemas sencillos de operar, confiables en algunos casos y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Estamos viviendo en una verdadera era de la informatización, su progreso, la miniaturización de los chips y las nuevas formas de comunicación nos permiten ver, que los recaudos, las protecciones e incluso las leyes no estaban a la altura de las circunstancias.

La Argentina no es ajena a estos nuevos cambios que provocó la tecnología, pero la legislación, no acompañó a tiempo con el proceso.

Esto genera en la sociedad sensación de incertidumbre y desamparo, como así también desconfianza en las transacciones que uno constantemente debe realizar.

Las computadoras se ha convertido en la herramienta, más accesible, rápida y económica para conseguir información, para comunicarse con personas de distintos lugares del mundo, de la misma manera que lo hacen con el compañero de trabajo que está en la oficina de al lado. Esta tecnología nos permite crear, procesar, almacenar y transmitir datos, con la rapidez y eficacia que ningún otro medio nos permite aún.

La tecnología de la computarización se ha vuelto indispensable por las ventajas que ella proporciona sobre otros métodos obsoletos. Tanto los sistemas bancarios, los órganos del gobierno, como los particulares, hacen uso de ella.

La mayoría de las personas cuando hacen uso de la informática, lo hacen con fines lícitos, de esparcimiento, educativos, entre otros, sin embargo hay quienes sacan provecho de estas nuevas tecnologías para cometer delitos, los llamados, delitos informáticos.

Los delitos informáticos, cometidos por los denominados delincuentes de cuello blanco, amenazan contra la economía mundial y contra la sociedad en su conjunto. Su sofisticada forma de comisión lleva a presentar grandes dificultades para su comprobación, y sobre todo para identificar al verdadero autor del delito, esto se debe principalmente a su propio carácter técnico.

Hoy, el crecimiento de la tecnología, ha llevado a que los límites que antes se creían controlados, ya no tengan fronteras.

Esta nueva modalidad delictiva, de fácil acceso y economicidad, tiene como particularidad que es muy eficaz para cometer graves perjuicios, como incalculables beneficios para el autor o para un tercero, todo esto ha llevado a que su proliferación sea cada vez mayor, por lo que se había convertido en una necesidad urgente su regulación. Esta necesidad fue en parte satisfecha por la ley 26.388, sancionada en julio de 2008.

Se entienden por delitos de cuello blanco, a aquellos ilícitos penales cometidos por sujetos de elevada condición social, utilizando como herramientas sus conocimientos profesionales, o sus contactos en el mundo de los negocios, la política, etc. Este concepto, fue ideado en el año 1939 por Edwin Sutherland, en una reunión anual organizada por la American Sociological Society en Filadelfia[2].

El resultado de los estudios realizados, causó un impacto revolucionario, ya que permitió vislumbrar con evidente claridad, falencias y contradicciones en el sistema penal**,** rompiendo con la ficción que consideraba al delito como patrimonio exclusivo de la clase baja**.**

Éste tipo de ilícitos se distinguen del resto, por determinadas características[3]:

- la lesión de la confianza en el ámbito mercantil.
- el uso de la credulidad o ignorancia de la víctima.
- especial astucia y conocimientos por quienes preparan el ardid.
- la circunstancia de que la sociedad tenga conciencia de la ilicitud del hecho, pero no de su trascendencia criminal.
- imagen de honorabilidad del autor, normalmente debido a su posición social, estudios, profesión o situación económica y/o política.
- La escasa visibilidad del delito.
- La volatilización de la cantidad de víctimas.
- Falta de estadísticas criminales.
- Alto costo patrimonial en los perjuicios hacia los damnificados.

Las personas que cometen los delitos informáticos, son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, que los sujetos activos tienen particulares habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral, se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de

[2] Edwin H. Sutherland Traductora Laura Belloqui, edición 2009, Editorial B de F.

[3] www.alfonsozambrano.com/doctrina_pena Autor: El Dr. Alfonso Zambrano Pasquel, ex magistrado de la Corte suprema del Ecuador, es además profesor de Criminología y Derecho Penal y Derecho Procesal Penal de la universidad Laica Vicente Rocafuerte de Guayaquil.

los sistemas informatizados, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Investigaciones[4] al respecto, lograron demostrar que entre los sujetos activos de estos tipos de delitos, existían similitudes en sus características psíquicas:

- **Materialismo**: solo da valor a los bienes materiales, es un auténtico maníaco, su tensión patológica se libera con la ganancia, tiene una psicología similar a la del jugador compulsivo.

- **Egocentrismo**: no alcanzan a lograr afectividad, esta soledad la compensan mostrándose generosos económicamente.

- **Narcisismo**: son soberbios, inestables, y esto se traduce a su situación social, suelen ser muy audaces.

- **Peligrosidad**: no valoran los límites éticos.

- **Hipocresía**: son fríos y se muestran generosos y complacientes.

- **Neuróticos**: falta de conciencia de culpabilidad, debido a que estos actos no provocan reacción social, ya que hay personas que no lo consideran delitos.

Este tipo de delincuentes, no es considerado como un enfermo, por lo cual su punición es perfectamente aplicable.

En la argentina, los delitos de cuello blanco, carecen de necesarios organismos de control que posibiliten la obtención de resultados eficientes. En sede administrativa no hay suficiente personal especializado en la prevención, ni en sede judicial para su investigación y represión, lo que posibilita que sea más fácil su comisión y más difícil su descubrimiento.

El sistema judicial en nuestro país, no cuenta con suficientes oficinas especializadas en este complejo tipo penal, encontrándose totalmente desarticulado frente a la comisión del delito específico.

En esta clase de delitos, el sujeto activo es generalmente un delincuente habitual respecto a este tipo de maniobras, muchos son cometidos por múltiples actos y en algunos casos encuadran en diferentes

[4] Revista Internauta de Práctica Jurídica. Agosto-Diciembre 2006, PRINCIPIOS DE CRIMINOLOGÍA Dr. MARIO EDUARDO CORIGLIANO

figuras, por ejemplo, primero violan una casilla de correo y desde allí amenazan a otro, o al descubrir la cuenta bancaria, hacen vaciamiento de ella, y para demorar la investigación infectan de virus el ordenador.

El delito de "cuello blanco" es un flagelo que con el avance de la tecnología, de las comunicaciones, y el aumento significativo de transacciones comerciales, ha ido creciendo exponencialmente, motivo por el cual debe ser combatido por mecanismos eficientes y modernos que posibiliten una eficaz prevención, y una rápida investigación que finalice en la condena del delincuente, en caso de su real comisión.[5]

5 MsC. Antonio Rodríguez Pérez, Asesor Jurídico; Dra. Belkis Frenis Mederos, 07-10-2010, Artículo publicado en la página web http://www.gestiopolis.com, sección economía, titulado: Los delitos de cuello blanco. Evitarlos para proteger la economía nacional Cubana

Sub-capitulo1

Delitos informáticos

El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas y medios de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos.

Esta realidad ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos del resto, muchos doctrinarios lo creen fundamental, como hay algunos que le restan importancia.

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que, según éstos se trata de los mismos delitos, cometidos a través de otros medios.

El "Convenio de Ciberdelincuencia del Consejo de Europa", define a los delitos informáticos como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos".

1-**CARACTERÍSTICAS PRINCIPALES:**

- Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
- Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.
- Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.[6]

Mas bajo haré una breve reseña de las definiciones de algunos autores, para que podamos ver distintas posturas doctrinarias.

[6] http://www.delitosinformaticos.info/delitos_informaticos/definicion.html

Argibay Molina señala al respecto de definir los delitos informáticos, ”Si hacemos una analogía entre “ delitos informáticos **"** y “ delitos económicos" concluiríamos que, solo son delitos los tipificados en nuestro ordenamiento jurídico; y como ninguno de ellos lo está, tanto la informática como lo económico son solo "factores criminógenos"

Una **investigación de la Universidad de México**, sintetiza que “ delitos informático" son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

Carlos Sarzana , en su obra Criminalitá e tecnología, comenta que los crímenes por computadora comprenden "Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo"

Nidia Callegari define al "delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas"

Rafael Fernández Calvo por su parte comenta que "delito Informático" es la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando en elemento informático o telemático contra los derechos y libertades de los ciudadanos”.

María de la Luz Lima 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"[7]

Julio Tellez Valdés conceptualiza al "delito Informático" en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento ".[8]

El delito Informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

[7] LIMA de la LUZ, María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrua. México. Enero-Julio 1984 (Gabriel h, Tobares Catala, Maximiliano Castro Arguello, Delitos Iinformáticos, advocatus)

[8] TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996

Hasta ahora, no hay definición de carácter universal propia de delito Informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema.

Es importante, hacer referencia a las distintas denominaciones que se les ha dado a las conductas ilícitas, que usan como medio de comisión dispositivos de alta tecnología, estas son " delitos informáticos", " delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", "delincuencia relacionada con el ordenador", "delitos de alta tecnología".[9]

Para hablar de delitos, primero debemos verificar que una conducta humana (acción u omisión) se adecue a la descripción realizada por el tipo (tipicidad), luego que la misma no esté autorizada ni que goce de un permiso por el ordenamiento jurídico (antijuricidad). Y por último, comprobar que el autor posee las condiciones personales para imputarle dicha conducta (culpabilidad).

Esta es una construcción doctrinal, surgida a fines del siglo XIX. Comienza en Alemania, con los planteamientos de Von Lizt, quien adopta este sistema para poder enseñar derecho penal a sus alumnos, y se difunde por toda Europa en países tales como Italia, España, Portugal, Grecia. Luego es acogida en América Latina por la influencia española.

Elementos:

1. Acción (acciones y omisiones)
2. Tipicidad
3. Antijuricidad
4. Culpabilidad

Esta teoría no se ocupa de los elementos o requisitos específicos de un delito en particular (homicidio, robo, violación, etc.), sino de los elementos o condiciones básicas y comunes a todos los delitos. [10]

Acción

La acción es conducta omisiva o activa voluntaria, que consiste en un movimiento de su organismo destinado a producir cierto cambio, o la posibilidad de cambio, en el exterior del mundo.

Von Liszt "la acción es la producción, reconducible a una voluntad humana, de una modificación de mundo exterior"[11]

[9] Trabajo de investigación realizado por Ricardo Levene (nieto) y Alicia Chiaravalloti,. Publicado en el Vl Congreso Latinoamericano en 1998, en Colonia, Uruguay.

[10] http://es.wikipedia.org/wiki/Derecho_penal ZAFFARONI, Eugenio Raúl, Manual de Derecho Penal, Parte General, Ediar, 2005

Tipicidad

Es la descripción abstracta de la conducta prohibida por la norma, esta descripción es efectuada por el legislador[12].

La tipicidad es la adecuación, es el encaje del acto humano voluntario ejecutado por el sujeto, a la figura descrita por la ley como delito. Si la adecuación no es completa no hay delito.

Es el resultado de un juicio u operación mental llevada a cabo por el intérprete o el juez, que permite determinar que la conducta objeto de examen coincide con la descripción abstracta contenida en la ley penal[13].

Antijuridicidad

La antijuridicidad es la oposición del acto voluntario típico al ordenamiento jurídico. La condición de la antijuridicidad es el tipo penal. El tipo penal es el elemento descriptivo del delito, la antijuridicidad es el elemento valorativo.

Culpabilidad

La culpabilidad es la reprochabilidad de la conducta de una persona imputable y responsable, que pudiendo haberse conducido de una manera no lo hizo, por lo cual el juez le declara merecedor de una pena. Es la situación en que se encuentra una persona imputable y responsable.

Para que haya culpabilidad tiene que haber: Imputabilidad, dolo o culpa y la exigibilidad de una conducta adecuada a la prohibición o imperatividad de la norma.

Según Núñez la imputabilidad es la capacidad de ser penalmente culpable. Esa capacidad presupone madurez, salud mental y conciencia, en una medida que habiliten al autor para comprender la criminalidad del acto y dirigir sus acciones[14].

La pena:

Este elemento es el resultado del acto jurídico no cambia la naturaleza del delito, pero influye en la punibilidad.

La doctrina no es pacífica en cuanto a la ubicación de la pena, algunos autores consideran que debe situarse antes de la teoría de las consecuencias del delito. Incluyen a la punibilidad como una categoría de la teoría del delito.

[11] Maximiliano Octavio Davies, Lorena Elbaum, Derecho Penal 1.
[12] Maximiliano Octavio Davies, Lorena Elbaum, Derecho Penal 1.
[13] Maximiliano Octavio Davies, Lorena Elbaum, Derecho Penal 1.
[14] Núñez Ricardo, Manual de Derecho Penal- parte general, 4ta edición actualizada.

Otros, consideran que el tratamiento de las circunstancias que componen la punibilidad corresponden a la teoría de las consecuencias del delito.[15]

2- **Medio de comisión**

El medio de comisión de estos delitos, es la informática, vocablo que fue acuñado, por primera vez por el francés Philippe Dreyfus, en 1962, siendo un acrónimo de las palabras información y automática.

Pronto adaptaciones locales del término aparecieron en italiano, español, rumano, portugués y holandés, entre otras lenguas, refiriéndose a la aplicación de las computadoras para almacenar y procesar la información

La real academia define a la informática, como un conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automático de la información por medio de ordenadores. [16]

Respecto a lo que hoy conocemos, en la informática confluyen muchas técnicas y procesos, como así también distintos tipos de máquinas que el hombre ha desarrollado a lo largo de la historia para potenciar su capacidad de memoria, de comunicación, y así agilizar las tareas cotidianas.

Conceptualmente, se puede entender como aquella disciplina encargada del estudio de métodos, procesos, técnicas, desarrollos y su utilización en ordenadores (computadoras), con el fin de almacenar, procesar y transmitir información y datos en formato digital.

Los sistemas informáticos deben realizar las siguientes tareas básicas:

- Entrada: Captación de la información digital.
- Proceso: Tratamiento de la información.
- Salida: Transmisión de resultados binarios.

3-**Tipos de delitos informáticos**:

La Organización de las Naciones Unidas, reconoce 3 tipos de delitos informáticos a nivel mundial:

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

[15] Maximiliano Octavio Davies, Lorena Elbaum, Derecho Penal 1.

[16] http://www.rae.es/rae.html; Real academia española, Diccionario Panhispánico de dudas, octubre 2005

Los fraudes cometidos mediante manipulación de computadoras pueden clasificarse en:

* Manipulación de los datos de entrada o sustracción de datos.
* La manipulación de programas: modificación de programas existentes en un sistema o la inserción de nuevos programas.
* Manipulación de los datos de salida.
* Fraude efectuado por manipulación informática, aprovecha las iteraciones automáticas de los procesos de cómputo.

Los fraudes cometidos mediante la manipulación de los datos de entrada:

* Como objeto: alteración de los documentos digitales
* Como instrumento: uso de las computadoras para falsificar documentos de uso comercial.

Los daños o modificaciones de programas o datos computarizados:

* Sabotaje informático: acción de eliminar o modificar funciones o datos en una computadora sin autorización, para obstaculizar su correcto funcionamiento.
* Acceso no autorizado a servicios y sistemas informáticos.
* Reproducción no autorizada de programas informáticos de protección legal.

4-**Sujeto activo**

Las personas que cometen delitos creados en virtud de las nuevas tecnologías constituyen una esfera de estudios en cierta medida muy nueva.

Las motivaciones de delincuentes tradicionales son perfectamente conocidas, como las de los asesinos, ladrones, traficantes de drogas, etc., pero en estos casos es necesario un examen desde la perspectiva de la delincuencia relacionada con las redes informáticas.[17]

En principio, a los delitos pueden cometerlos cualquier persona, como ocurre por ejemplo, en el homicidio (art 79), la privación ilegal de la libertad (art 141), la violación de secretos (art 153), etc. En estos ilícitos, como en la mayoría de los tipificados en el código penal, no hay limitaciones de naturaleza alguna en cuento a sus posibles autores[18]. Por el

[17] 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 informáticas, Viena, 8 a 17 de mayo, 2001. (Gabriel h, Tobares Catala, Maximiliano Castro Arguello, Delitos Iinformáticos, advocatus)

[18] Terán lomas, Roberto a. m., derecho penal. Parte general, t, 1.,pag 318, (Gabriel h, Tobares Catala, Maximiliano Castro Arguello, Delitos Iinformáticos, advocatus)

contrario , Terán Lomas enumera los delitos llamados propios, que solo pueden ser cometidos por determinadas personas, como el oficial público art 136, medico, art 83 y 139, descendiente o cónyuge art 80 inc. 1. Como así también encontramos los delitos de propia mano, que son aquellos que solo pueden ser ejecutados en forma directa por los sujetos activos previstos en el tipo. No puede haber en estos actos criminales autoría mediata[19].

Citando a Lilly y Massa[20], podemos observar que éstas conductas son cometidas generalmente por personas de un determinado nivel de inteligencia y educación que supera al común, es el llamado hacker.

Pertenecen a sectores instruidos con accesos a determinadas oportunidades y conocimientos imprescindibles que les permiten incrementar su riqueza mediante el uso de modernas técnicas a las que tienen acceso por su ocupación o disponibilidad de medios, como así también otros fines diferentes a los meramente económicos. Siendo potenciales autores los : operadores, programadores, analistas, supervisores, personal técnico y de servicio, funcionarios superiores y de control, auditores, bibliotecarios, personal temporarios, ex empleados, impostores, intrusos, y violadores externos [21].

El crecimiento del número de adolescentes, que se ven involucrados en hechos de ésta naturaleza, es sumamente notable.

El sujeto activo de los delitos informáticos son aquellas personas que poseen ciertas características, que no presentan el denominador común de los delincuentes, o sea, tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos, que por el medio de comisión de los delitos.

Tenemos que dejar en claro, que el nivel de aptitud no es un indicador para diferenciar al delincuente informático, del delincuente tradicional, ya que generalmente se lo ha relacionado con personas listas, decididas, con niveles intelectuales superiores, y no en todos los casos es así, sino que está aumentando y de manera sorprendente, las amenazas desde computadoras domésticas, y sin programas especiales, sino a través de páginas de uso cotidiano.

---

[19] Terán lomas, Roberto a. m., derecho penal. Parte general, t, 1.,pag 318 y 319 (Gabriel h, Tobares Catala, Maximiliano Castro Arguello, Delitos Iinformáticos, advocatus)

[20] Lilli Alicia Raquel, Massa María Amalia, Delitos Informáticos, bs as, 1999, pág. 52

[21] Riquert Marcelo Alfredo, pág. 53, 54 y 55.

El sujeto activo del delito, generalmente, es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Socialmente este tipo de delincuentes, no son considerados como tales, no sufren la condena social, como si lo sufre el delincuente tradicional.

Un axioma de la teoría de la seguridad indica que cualquier ataque necesita para llevarse a cabo, 3 elementos: motivación, capacidad y oportunidad,[22]

El hecho que marca la mayor diferencia en los cambios criminológicos surge de la globalización, como también el surgimiento de las nuevas tecnologías donde se mezclan diferentes culturas, historias, creencias, rituales, ideologías, dando paso a relaciones sociales más conflictivas y complicadas, creando una criminalidad más compleja obligando al cambio de estrategias para su resolución.

En la actualidad se diferencia con 3 cambios fundamentales, perfil del delincuente, exposición en la comisión del delito y la disminución al mínimo en la amenaza física dirigida al delincuente.

El antiguo delincuente estaba catalogado con una tipología determinada en la personalidad, que combinaba rasgos de psicotismo, con una activación baja, lo que se denomina comúnmente sangre fría.

El delincuente de sangre fría, es aquel que encontramos en los delitos que en su mayoría están tipificados en la legislación penal, estos requieren una importante exposición física, lo que les limita la posibilidad de realizar nuevos intentos o pruebas limitando las oportunidades para la comisión del suceso criminoso, donde la amenaza de supervivencia existe en mayor grado.

En cambio, el delincuente informático, tiene la posibilidad de realizar mejoras, ensayos, probando en diversas oportunidades, todo ello sin exponerse a la amenaza física, dado que el medio comisivo que utiliza, le permite la ausencia de su persona en el lugar del hecho. Procurando de esta manera, el “anonimato del delincuente”.

Las motivaciones que pueden llevar al sujeto activo a la consecución del delito, pueden ser comunes a aquellos ilícitos tradicionales, como son: la obtención de ganancia personal, resentimiento, venganza, perturbación mental o estados emocionales, encargo, o aprovechando la oportunidad, que da la facilidad de la vulnerabilidad de los controles y la despersonalización que tiene la computadora.

[22] Olivart David, “ perfiles psicológicos de amenazas de entornos virtuales”

Pero debemos agregar que con las nuevas tecnologías, también surgieron nuevas motivaciones, como es la actitud, o la superación personal.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse, o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en "paraísos informáticos", que son aquellos países que carecen de leyes o experiencia para seguirles la pista.

5-**Sujeto pasivo**

El hecho de que gran parte de la doctrina emplea el término de víctima, responde en cierta medida al tratamiento que a través de la historia y desde sus comienzos con el derecho romano hasta el medieval, se le dió.

La víctima del delito ocupaba un papel preponderante, quedando a su cargo o de sus herederos la reacción frente al hecho delictivo que dió origen[23].

Con posterioridad, con la aparición del Estado de derecho moderno, el derecho penal, se transforma en una herramienta fundamental de estado, para perseguir, juzgar y aplicar una pena al autor de un delito, evitando la justicia por mano propia y progresando de esta manera en consecuencias favorables de índole social, ya que se logró proporcionalidad, imparcialidad y objetividad. Pero, quizás quitándole intervención a la víctima. Y desde ese momento el derecho penal de manera tradicional centró su atención principalmente en el sujeto activo del accionar delictivo.

Así mismo, con el transcurso del tiempo, y con los avances de la ciencia penal, podemos ver la importancia que se le da al sujeto pasivo, logrando un protagonismo más participativo, dentro del derecho[24].

---

[23] **www.stj-sin.gov.mx/delitosinformaticos2.htm.** UNIVERSIDAD VALLE DEL BRAVO, Maestría en Administración con Especialidad en Informática, Aspectos Legales de la Tecnología, Catedrático Lic. Fernando Pérez Holguín, Articulo de Publicación: *"Delitos Informáticos"*, AUTOR:Juan Manuel García De la Cruz, 13 de Abril de 2005

[24] **www.stj-sin.gov.mx/delitosinformaticos2.htm.** UNIVERSIDAD VALLE DEL BRAVO, Maestría en Administración con Especialidad en Informática, Aspectos Legales de la Tecnología, Catedrático Lic. Fernando Pérez Holguín, Articulo de Publicación: *"Delitos Informáticos"*, AUTOR:Juan Manuel García De la Cruz, 13 de Abril de 2005

Debemos tener presente que sujeto pasivo es tanto la persona física, como la jurídica en su calidad de ofendido por el accionar delictivo.[25]

Se puede definir al sujeto pasivo como la víctima del delito, como la persona que ha sido perjudicada directamente por su comisión, en su art 25 la Convención Americana sobre Derechos Humanos, incorporada a la Constitución Nacional, art 75 inc 22, establece en términos generales la obligación del estado de proveer a los ciudadanos sometidos a su jurisdicción, una debida protección judicial cuando algunos de sus derechos hayan sido violados, siempre que éste derecho les sea reconocido por la convención, la constitución , o las leyes internas del estado. Esta protección corresponderá "cualquiera sea el agente" al cual pueda eventualmente atribuírsele la vulneración.[26]

El sujeto pasivo, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

Contra lo que usualmente se cree, la víctima, pasado el primer momento de indignación y especialmente en delitos contra la propiedad y los cometidos en ámbito familiar, dista mucho de responder al estereotipo degradado de un ser sediento de venganza, e insaciable en su exigencia de reparación[27].

El estudio del sujeto pasivo, en las conductas que estamos analizando es clave, ya que mediante él, podemos conocer los diferentes hechos ilícitos, que cometen los delincuentes informáticos.

Muchos delitos son desconocidos por sus víctimas, es por ello, que es imposible conocer la verdadera dimensión de los delitos informáticos, ya que la mayoría de este tipo de ilícitos, no son descubiertos o no son denunciados a las autoridades responsables.

El sujeto pasivo de ese tipo de delitos, juega un papel determinante, ya que en muchos casos las víctimas son las únicas que pueden brindar ciertos datos fundamentales que permiten comenzar con la investigación, y hasta descubrir al autor.

En materia de números y estadísticas se podría afirmar que no existen datos certeros que permitan conocer la real magnitud de la propagación de los delitos informáticos, ya que muchas víctimas de este tipo de delitos, no saben que lo son y en otros casos muchos no son

[25] De ello se deduce que tenemos que considerar como sujeto pasivo a la persona física que sufre o soporta materialmente la acción que como dijimos no siempre es el ofendido por el delito.

[26] Cafferata Nores, José y otros, manual de derecho procesal penal, 2da edición, educación ciencia y sociedad, Córdoba, 2004.

[27] Zaffaroni Eugenio Raúl, manual de Derecho Penal, parte general, Ediar bs as, 2005 pag 771

denunciados, por la creencia falsa, en parte, de que no hay nada que se pueda hacer en estos casos.

Muchas empresas sienten temor de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa, respecto a su seguridad y confiabilidad y las consecuentes pérdidas económicas, eso trae como consecuencia que las estadísticas sobre este tipo de conductas se mantengan bajo la llamada "cifra negra".

Para lograr una prevención efectiva de esta nueva modalidad delictiva, como medida, se debería analizar las necesidades de protección y divulgar las fuentes principales de peligro, alertar a las potenciales víctimas, para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática ,crear una adecuada legislación que proteja los intereses de las víctimas, una eficiente preparación por parte del personal encargado de la procuración y administración de justicia para atender e investigar estas conductas ilícitas.

Los organismos internacionales, están convencidos que educando a la comunidad y estimulando la denuncia de los delitos, capacitando a los encargados de hacer cumplir la ley y a las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos, se reduciría en gran medida este tipo de delitos, como así también, se promovería la confianza pública, ya que esta nueva modalidad provoca gran incertidumbre en la sociedad.

También podemos marcar una tendencia a la victimización masiva, causada por este tipo de delitos, como por ejemplo la propagación de virus, ya que el número de víctimas es demasiado grande.

6- **Legislación argentina**

A pesar de que argentina ya cuenta con legislación referida al tema, todavía quedan varias “lagunas” pendientes por legislar, como por ejemplo los procedimientos legales para capturar y resguardar las pruebas digitales de estas actividades ilícitas.

El fiscal de la Nación Ricardo Sáenz[28] precisó que la reciente reforma al Código Penal sólo reprime la comisión de delitos dolosos, es decir, aquellos producidos con la intención y voluntad de producir el daño [29].

[28] Ricardo Saenz, Abogado graduado en 1983 en la Universidad de Buenos Aires, es desde 1993 Fiscal General ante la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal

[29] http://www.iprofesional.com/notas/69532-Delitos-informaticos-cuales-son-los-alcances-y-penalidades-que-preve-la-nueva-ley.html Autores: César Dergarabedian y Matías Debarbieri, Delitos informáticos: cuáles son los alcances y penalidades que prevé la nueva ley; 26 de Julio, 2008.

En lo referente a la efectividad de la flamante ley, Sáenz puntualizó que los jueces y fiscales deberán capacitarse en lo relativo a los desafíos que implican las nuevas tecnologías, para que el magistrado no resulte cautivo de las opiniones de los peritos al momento de resolver los juicios.

Esto es muy importante, ya que para que el magistrado pueda cumplir eficientemente su función, debe tener conocimientos básicos para poder desempeñar sus tareas y tomar sus propias decisiones y no quedar sujeto únicamente a la opinión de los especialistas en el tema.

"En este temática, y ante la falta de capacitación adecuada, se puede correr el peligro de que el técnico se convierta en el juez de la causa si éste no se capacita"[30], puntualizó

Debemos entender que por una cuestión lógica, la tecnología, va más rápido que las leyes, y por lo tanto el delito informático, va mucho más rápido que las regulaciones.

En la actualidad, precisamente como señala Mauricio De Núñez[31], todos los delitos prácticamente pueden ser cometidos por medios informáticos, No hay delito que no esté vinculado a la informática, ya que tampoco hay actividad que no tenga relación alguna con la informática. Como consecuencia es muy común que en los procedimientos policiales, por cualquier delito que sea, se secuestran los equipos informáticos que se encuentren en el lugar del operativo[32].

Obviamente las empresas o particulares en el caso que deban intervenir los sistemas o acceder a comunicaciones, por ejemplo, para reparar sus sistemas o servidores, no deben preocuparse. Ya que en este último caso hay una causa justificada que legítima el acceso, no produciéndose la comisión de un delito.

Respecto a las prácticas informáticas en las empresas, es importante señalar que en principio, las empresas no tienen responsabilidad penal por los delitos informáticos y que esa responsabilidad, en todo caso, recaerá sobre aquellos empleados, encargados , o gerentes, que cometan alguno de los ilícitos establecidos en la ley, aunque no hay que dejar de lado que en varias situaciones se pueden dar casos de "complicidades" de las compañías, sobre todo, en cuestiones relacionadas con la falta de adopción de medidas de seguridad, en este último supuesto, las empresas podrán quedar expuestas a acciones por daños y perjuicios si se llegara a demostrar la falta de recaudos que hubieran posibilitado que un empleado cometa algún delito informático.

[30] http://www.iprofesional.com/notas/69532-Delitos-informaticos-cuales-son-los-alcances-y-penalidades que-preve-la-nueva-ley.html; Autores: César Dergarabedian y Matías Debarbieri**,** Delitos informáticos: cuáles son los alcances y penalidades que prevé la nueva ley**;** 26 de Julio, 2008**.**

[31] Mauricio De Nuñez, Delitos Informaticos sin castigo, domingo 2 de enero, 2005, diario Clarin,

[32] www.clarin.com, Mauricio De Nuñez, Delitos Informaticos sin castigo, domingo 2 de enero, 2005.

El botín más atractivo, para estos delincuentes, es el dinero o algún objeto de gran valor, por lo tanto, los sistemas que pueden estar más expuestos a fraude son los que tratan pagos, como los de ventas, compras y depósitos. Entonces, financieras, bancos y empresas de seguros son las que se sienten en mayor riesgo respecto de otras. Aunque no podemos dejar de lado, que en varias ocasiones los documentos privados y datos confidenciales, son muy atractivos para este tipo de delincuente.

Los sistemas mecanizados, muy utilizados en la actualidad, y con perspectiva de aumento, son susceptibles de pérdidas o fraudes debido a que, tratan grandes volúmenes de datos e interviene poco personal, lo que impide verificar todos los movimientos y partidas.

Los sistemas son impersonales, aparecen en un formato ilegible y están controlados parcialmente por personas cuya principal preocupación son los aspectos técnicos del equipo y del sistema y que no comprenden, el significado de los datos que manipulan. En el diseño de un sistema importante es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir. Los sistemas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos.

7-**Los delitos pueden ser examinado desde dos puntos de vista diferentes:**

- Los delitos que causan mayor impacto a las organizaciones.
- Los delitos más difíciles de detectar.

Aunque depende en gran medida del tipo de organización, se puede mencionar que los Fraudes y sabotajes son los delitos de mayor incidencia en las organizaciones.

Pero si se examina la otra perspectiva, referente a los delitos de difícil detección, se deben situar a aquellos producidos por las personas que trabajan internamente en una organización y que conocen perfectamente la configuración interna de las plataformas; especialmente cuando existe una cooperación entre empleados, cooperación entre empleados y terceros, o incluso cuando está involucrada la administración misma.

Otro grave obstáculo al enjuiciamiento por delitos cibernéticos es el hecho de que los delincuentes pueden destruir fácilmente las pruebas cambiándolas, borrándolas o trasladándolas.

Si los encargados de la investigación operan con más lentitud que los delincuentes, se pierde gran parte de las pruebas; o puede ser que los

datos estén cifrados, una forma cada vez más popular de proteger tanto a los particulares como a las empresas en las redes de computadoras.

Tenemos que tener en cuenta que tal vez la criptografía estorbe en las investigaciones penales, pero el derecho a la intimidad podría ser vulnerado si los encargados de hacer cumplir la ley adquieren demasiado poder técnico, e intromisión en nuestros datos personales y privados, como ser correos, sesiones de chat, mensajes de texto, entre otras.

Las empresas electrónicas sostienen que el derecho a la intimidad es esencial para fomentar la confianza del consumidor en el mercado de la Internet, y los grupos defensores de los derechos humanos desean que se proteja el cúmulo de datos personales archivados actualmente en ficheros electrónicos.

Podemos concluir finalmente que dado la contemporaneidad del fenómeno tecnológico que avanza exponencialmente, existe en materia de delitos informáticos un vacío legal que provoca un deseo -imposible de concretar, de salvar dicha ausencia normativa con injertos o interpretaciones extensivas que contrarían el sentido axiológico que inviste al Derecho Penal, ya que la proscripción de la analogía es un principio penal insoslayable.

Vemos así, que en el Derecho comparado existe una tendencia a formular leyes especiales con figuras específicas, o a incorporarlas al Código Penal en el capítulo más afín con el bien jurídico protegido.

Consideramos que dada la importancia que el tema reviste en la actualidad y que se proyecta como irreversible, es menester además que las fuerzas de prevención administrativas y/o judiciales posean conocimientos teórico-prácticos acordes a la realidad compleja que implica la investigación de ésta clase de delitos.

8-**Criminalidad tecnológica**

En el plano jurídico penal la criminalidad informática puede suponer una nueva versión de delitos tradicionales o la aparición de nuevos delitos. Tanto los delitos contra la propiedad, los delitos contra el honor, los delitos contra el orden público, entre otros, se manifiestan hoy potenciados en razón del aumento constante a las nuevas tecnologías. Y por otra parte, nuevas situaciones de hecho que afectan bienes no tutelados tradicionalmente por el Derecho Penal, abarcando grandes redes de información mundial como puede ser la web y las comunicaciones electrónicas, en combinación de diversos medios informatizados.

La criminalidad informática se caracteriza por las dificultades que entraña descubrir, probar y perseguir los delitos. Tanto las empresas como así también los estados de diferentes países, se han procurado organizar y establecer mecanismos tendientes a fortalecer los sistemas de seguridad

informática, realizando investigaciones proactivas en la búsqueda de vulnerabilidades antes de que fuesen descubiertos por otros.

La aplicación universal de medidas eficaces de lucha contra el delito, será necesaria.

Mientras que los delincuentes tradicionales se ven limitados por factores como la distancia geográfica, los controles aduaneros y la necesidad de tener acceso físico a las víctimas, los delincuentes electrónicos pueden operar remotamente y con una impunidad real desde cualquier jurisdicción que carezca de legislación suficiente, o de la voluntad o la capacidad de aplicarla, o a través de varias jurisdicciones.

El hecho de que las tecnologías y los delitos que dependen de ellas sigan evolucionando, requerirá un esfuerzo mundial para seguir los nuevos acontecimientos, elaborar respuestas eficaces y difundirlas con suficiente rapidez para que los organismos encargados de aplicar la ley puedan perseguirlos eficientemente con resultados acordes a los reclamos de la sociedad.

La precariedad del sistema jurídico penal, que cuenta con una novedosa reforma de la materia, refuerza la tendencia social ya instalada a no denunciar estos delitos, para evitar la alarma social o el desprestigio que podría derivarse de su conocimiento. Esto es sumamente comprensible debido a la gran penetración de las nuevas tecnologías en toda sociedad y de las constantes inversiones que las empresas llevan a cabo en cada uno de sus procesos económicos, incluidas las de seguridad informática.

Hoy en día los virus suponen el problema más común, junto con el robo de información confidencial, situaciones que conforman la llamada “cifra negra” de la delincuencia informática.

Además de lo expuesto, la mayoría de los expertos creen que formas comunes de delitos relacionadas con las redes informáticas no son suficientemente denunciadas, porque las que las víctimas no comprenden que lo han sido, o quizás no comprenden que el comportamiento de que se trata, es un delito.

La insuficiencia de los instrumentos penales, en el contexto anterior a la sanción de la ley 26.388, para evitar y castigar las distintas formas de criminalidad informática, suponía un reto para la política criminal de los próximos años.

La existencia de redes internacionales como internet abre la posibilidad de transgresiones a nivel mundial y con un gran potencial de impunidad. Las conductas no se realizan en un solo acto, sino en una serie continuada de ellos.

Los daños pueden ser experimentados en un país distinto a aquel donde se encuentra el delincuente físicamente. Fenómeno que representa un gran problema referido a su perseguibilidad.

El reto probatorio es en estos aspectos fundamental, pero lo más importante son las trabas que plantean los límites de la jurisdicción, nacionalidad del autor del hecho y el bien jurídico ofendido. Siendo relevante el origen y destino.

Una vez cometidos, estos delitos es posible eliminar toda evidencia de su comisión, lo que produce dificultades en el descubrimiento y prueba.

Con frecuencia su ilegalidad no es clara (depende el país donde el delito se verifica) resultando las leyes penales tradicionales insatisfactorias para la prevención del nuevo fenómeno, tornando casi imposible su persecución y castigo.

Una característica general de este tipo de conductas disvaliosas, es que, en la mayoría de los casos detectados, el accionar del sujeto activo es repetido varias veces en el tiempo. Lo que sucede, que una vez que el autor descubre o genera falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera la comisión del hecho. Incluso, en los casos de "manipulación del programa", la reiteración puede ser automática, realizada por el mismos sistema sin ninguna participación del autor y cada vez que el programa se active.

Por lo que podemos observar, para combatir a esas nuevas tendencias criminales con las características anteriormente descriptas, es necesario contar con una política criminal adecuada, y acorde con los cambios tecnológicos y científicos.

Pero no debemos dejar de tener presente que es imprescindible contar, como punto de partida, con una legislación adecuada que contemple las actualizaciones mencionadas por ser ésta una realidad en constante evolución. Siendo para ello indispensable que nuestros legisladores estén preparados para esta labor.

Finalmente se torna ineludible la preparación de los tribunales, tanto sus empelados como los magistrados y funcionarios y la policía, con una constante capacitación en éstos temas, a los fines de armonizar y sincronizar multidisciplinariamente, la lucha contra éste nuevo flagelo que se ha dado en llamar "Delito Informáticos".

Sub-capitulo2

La sociedad y el delito informático

Internet tiene un impacto profundo en el mundo laboral, el ocio y el conocimiento a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea.

Comparado a las enciclopedias y a las bibliotecas tradicionales, la web ha permitido una descentralización repentina y extrema de la información y de los datos.

Algunas organizaciones comerciales animan a su personal para incorporar sus áreas de especialización en sus sitios, con la expectativa de que impresionen a los visitantes con conocimiento experto.

Esta red de redes, en sus primeros tiempos, había llegado a gran parte de los hogares y de las empresas de los países ricos. En este aspecto se había abierto una brecha digital con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías era muy limitada para las personas[33].

No obstante, con el transcurso del tiempo se ha venido extendiendo el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar computadoras conectadas, en regiones remotas.

Desde una perspectiva cultural del conocimiento, Internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes proporciona una cantidad significativa de información y de una interactividad que sería inaccesible de otra manera.

Internet entró como una herramienta de globalización, poniendo fin al aislamiento de culturas. Debido a su rápida masificación e incorporación en la vida del ser humano, el espacio virtual es actualizado constantemente de información, fidedigna, útil o irrelevante, o en algunos casos errónea.

No ponemos en duda que el progreso de la tecnología, ha traído aparejado un sinfín de beneficios, avances económicos, de comunicación, culturales y ha facilitado el acceso y la distribución de la información. Pero al mismo tiempo puso en peligro los derechos a la intimidad, y a la libertad de los individuos, como así también la seguridad de los sistemas informáticos, entre algunas de sus desventajas. Es aquí cuando la sociedad moderna, tiene que poner un freno a las consecuencias de estos avances y controlarlos.

La posibilidad de gran almacenamiento que poseen estos sistemas, como así también su fácil distribución, ha llevado a que mucha información privada, haya sido violada, o utilizada con un fin distinto al que

[33] www.alambre.info; esta anotación fue publicada, el lunes 6 de octubre, 2008, a las 5.55 pm

propuso su autor. Muchos han utilizado estos ordenadores para ocultarse y así cometer amenazas o calumnias e injurias, con total impunidad.

Todo esto causó un gran impacto en la sociedad, hubo una urgente necesidad de lograr una seguridad informática, que nos permitiese confiar en este magnífico avance que nos proporcionó el estudio del hombre.

En estos años, las redes de computadoras han crecido de manera asombrosa. Hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos online superan los 200 millones, comparado con 26 millones en 1995.

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.

Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos. Para ello, es necesario la Implementación de barreras de seguridad antivirus, anti-espías, encriptación de la información y uso de contraseñas.

El escepticismo que genera el uso de éstas tecnologías, puede llegar a obstaculizar nuevas formas de hacer negocios, como el comercio electrónico, que permite conectar países de todo el mundo, homogeneizar horarios, y ofrecer productos diversos de una manera sencilla y práctica.

También podemos observar como 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 de nuestros tiempos, ya que la mayoría de las empresas no brindan esta clase de capacitación y muchos empleados no la poseen.

Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, según señala el manual de la ONU[34].

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

[34] www.segu-info.com.ar; publicado por el Departamento de Información Pública de las Naciones Unidas DPI/2088/H

tales como piratería informática, el fraude y el sabotaje informático, la trata de niños con fines pornográficos , amenazas, etc[35].

Otra clase de delincuentes de la informática, pueden sabotear las computadoras para ganar ventaja económica a sus competidores o amenazar con daños a los sistemas, con el fin de cometer extorsión.

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[36].

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson , Acecho cibernético: delito, represión y responsabilidad personal en el mundo online, publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.[37]

1-**Impacto a Nivel Social[38]**

La proliferación de los delitos informáticos ha hecho que nuestra 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 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 éste 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 éstas 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 aquellos que si los poseen. En vista de lo anterior aquel porcentaje que no conoce nada de informática, por lo general personas de escasos recursos económicos,

[35] Gabriel h, Tobares Catala, Maximiliano Castro Arguello, delitos informaticos, advocatus

[36] "Delitos Informáticos", trabajo realizado por Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Universidad de El Salvador, Octubre de 2000

[37] "Delitos Informáticos", trabajo realizado por Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Universidad de El Salvador, Octubre de 2000

[38] "Delitos Informáticos", trabajo realizado por Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Universidad de El Salvador, Octubre de 2000

pueden ser engañadas si en un momento dado, poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la 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".

2-**Impacto en la Esfera Judicial**[39]

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 consideren ilegales en el mundo virtual.

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 Estados Unidos, 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

[39] "Delitos Informáticos", trabajo realizado por Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Universidad de El Salvador, Octubre de 2000

gubernamentales de represión pertinentes en el estado donde se originó el delito.

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[40].

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 conectados, 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[41] se conectan a la red informática para acceder a las diferentes opciones que allí se presentan[42].

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 a el virus “Melissa”, creado y propagado en marzo de 1999, que causo un daño de más de de 10 millones de dólares, solamente en los Estados unidos. Y al virus “I love you” que en el año 2000 infectó a 45 millones de computadoras en todo el mundo.

El instituto de seguridad de computadoras (CSI), en los Estados Unidos realiza un estudio anual sobre la seguridad informática y los crímenes cometidos a través de las computadoras, anunció recientemente los resultados de su quinto estudio anual denominado “estudio de seguridad y delitos informáticos” realizado a un total de 273 instituciones, principalmente grandes corporaciones y agencias de gobierno.

Este estudio de seguridad y delitos informáticos es dirigido por CSI con la participación de la Agencia Federal de Investigaciones (FBI) de San Francisco.

[40] Gabriel h, Tobares Catala, Maximiliano Castro Arguello, delitos informaticos, advocatus

[41] Cambio de perfil de usuario de internet de argentina. El 60% pertenece a sectores medios y bajos y el nivel educativo de la mayoría es el secundario, que se conecta desde lugares públicos. Se trata de un perfil muy diferente al de los navegantes de fines de los ’90, mucho más elitista. Ahora dio paso a un usuario que se conecta mas desde lugares públicos, donde pesa más la información secundaria, que ya que redujo la edad de quienes se incorporar. Disponible en www.infobae.com/contenidos/186952-0-0-cambio-el-.perfil-del-usuario-internet-la-Argentina.

[42] “Delitos Informáticos”, trabajo realizado por Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Universidad de El Salvador, Octubre de 2000

Entre lo más destacable del estudio se pueden incluir:

Violaciones a la seguridad informática[43]

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

Pérdidas financieras[44]

- El 74% reconoció pérdidas financieras debido a las violaciones de las computadoras, las pérdidas financieras ascendieron a 265.589.940 dólares, cuando el promedio total anual en los últimos 3 años era de 120.240.180 dólares.

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 una gama diversa de ataques tales 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 difíciles de cuantificar 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 esos 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 uso un uso más eficaz de ellas.[45]

[43] "Delitos Informáticos", trabajo realizado por Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Universidad de El Salvador, Octubre de 2000

[44] "Delitos Informáticos", trabajo realizado por Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Universidad de El Salvador, Octubre de 2000

[45] 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 informáticas, Viena, 8 a 17 de mayo, 2001.

Capítulo 2:

Calumnias, injurias y amenazas por internet

Si por algo se ha destacado Internet es por la posibilidad que ofrece a todo el mundo de expresarse con gran libertad, de manera fácil, barata y cómoda, ya sea mediante la publicación de contenidos en páginas personales, fotografías o mediante foros, entre otros[46].

Sin embargo, esta libertad y el anonimato que aporta muchas veces la Red, han contribuido a que se lleven a cabo conductas tan poco lícitas y molestas como la emisión de mensajes injuriosos, calumniosos y en algunos casos amenazantes, contra otras personas.

Nuestro Código Penal, luego de los "delitos contra las personas", contempla a través de 9 artículos, los "Delitos contra el honor". Esto nos demuestra que para nuestro Código existe una jerarquía de valores: primero la persona y luego el honor. Además considera a los "delitos contra el honor" como una categoría especial de delitos, independiente de los delitos contra las personas.

El honor, como bien jurídico tiene características muy especiales: es un bien de estimación relativa, es decir que no todas las personas estiman de igual modo. Reviste dos formas diferentes, esto es, que se da a conocer a través de dos maneras distintas y bien definidas, a saber: el honor subjetivo, y el honor objetivo.

El honor, es un bien jurídico inmaterial, protegido por el código penal, estos delitos admiten reparación posterior, mediante la retractación, es por ello que hablamos de una categoría especial de delitos, y no se los incluye dentro de delitos contra las personas, ya que estos últimos nunca pueden ser reparados mediante una retractación. Los doctrinarios creen que ésta es una correcta división, aunque en otras legislaciones, son tomados como delitos contra las personas, justificando que las personas tienen dos aspectos, el moral y el físico.

Toda persona física puede ser sujeto activo de este tipo de delitos contra el honor, en el caso de personas jurídicas, no, pero si pueden serlos sus directores y administradores. Ya que en nuestro derecho las personas jurídica no pueden delinquir. En cambio, víctimas contra el honor, pueden ser tanto las personas jurídicas, como las físicas.

[46]Noelia García Noguera, Abogados, Portaley.com ,Abogada Especialista Nuevas Tecnología, *Calumnias e injurias en Internet.*

Dada las características de estos delitos contra el honor, cometidos por internet, podemos ver que en muchos casos las víctimas son menores. A primera vista se podría sostener, que el menor no puede ser sujeto pasivo, alegando que en su corta edad no ha podido formarse una reputación, (honor objetivo), ni tampoco tener la suficiente madurez como para adquirir conciencia del sentimiento del honor (honor subjetivo). Sin embargo, la doctrina nacional, sostiene que el menor pude ser víctima de estos delitos. Fundándose en las consecuencias futuras que puede acarrearle al menor tal hecho.

Aunque ésta sería la solución más acertada, no es la adoptada por nuestro código penal, que impide la posibilidad de perseguir los delitos contra el honor cuando son cometidos contra menores, al establecer el art 75 ”la acción de calumnias e injurias, solo podrá ser ejercida por el ofendido”, lo mismo pasa con los dementes y con los muertos, aunque hay que aclarar que en este último caso la acción podrá ser ejercida por el cónyuge, hijos, nietos o padres sobrevivientes, si el ataque fue a una persona viva, la cual al morir, le transmite el derecho de ejercitar la acción a sus parientes o cónyuge.

Este tipo de delitos pueden ser cometidos por cualquier medio, en este caso los medios de comisión deben ser informáticos, como ser los correos electrónicos, mensajes de textos, o cualquier otra modalidad que tenga como soporte un medio electrónico.

Amparadas en el anonimato del ciberespacio, muchas personas intimidan a otras mediante correo electrónico o mensajes de texto. Los avances tecnológicos pueden brindar confort y mejorar la calidad de vida, pero también pueden convertirse en una herramienta para cometer delitos.

Por mes se denuncian entre tres y cinco ilícitos, solamente en San Miguel de Tucumán, llevados a cabo mediante mensajes de textos enviados a celulares o por correo electrónico, confirmaron fuentes policiales y judiciales, de esa capital.

Los Fiscales del foro tucumano consultados en una entrevista publicada en el diario “La Gaceta” afirmaron que el delito más común es la amenaza de muerte. Lo siguen la extorsión y la divulgación de hechos que afectan el honor de las víctimas. Los casos van en aumento y no son fáciles de investigar[47].

[47] http://www.lagaceta.com.ar/vernotae.asp?id_nota=241271, Nota publicada en el diario “La gaceta”, sección tecnología, titulada “Aumentan las amenazas por internet o por celular”, el día Lunes 22 de Octubre de 2007

El principal obstáculo es el anonimato que brinda el ciberespacio. En el caso de los mensajes de texto de telefonía celular, las personas que cometen el ilícito suelen utilizar líneas telefónicas que no puedan ser identificadas o enviarlos desde las páginas web de las compañías de telefonía móvil. En internet, lo corriente es habilitar una casilla de correo con datos falsos. De esa manera, las amenazas o intentos de extorsión no pueden ser rastreados, ya que los datos ingresados para abrir la casilla no corresponden a una persona de existencia real.

De acuerdo con la información brindada por los fiscales la mayoría de los protagonistas de estos delitos tienen menos de 40 años.

Las cuestiones pasionales encabezan la lista de móviles de estos hechos, pero también ocurren por conflictos de intereses laborales.

En el diario la nación, el viernes 11 de septiembre, 2009 fue publicado un artículo titulado ¿Quién me mandó ese mail anónimo?, escrito por Ariel torres[48], que intenta plasmar cuán frecuentes son las consultas al estilo de "alguien me está mandando amenazas por mail, o me dice que yo le mandé y me va a denunciar, porque tiene mi IP". Pero... ¿es posible saber quién me mando ese mail?

La respuesta es sí, sí se puede, pero tenemos que saber, que el IP, es solo una identificación, que posee cada dispositivo conectado con internet, como ser la máquina, la impresora, el celular. Es como la patente del auto, el DNI o la dirección postal,[49] no da más que esa información, pero puede ser que esos aparatos hayan sido utilizados por otros y no por los dueños.

Tenemos que tener en cuenta que se están usando prácticas nuevas, para fraguar el IP. Esta técnica se llama spoofing, y aunque hoy se ha vuelto mucho más difícil, sigue siendo posible. No obstante, es poco probable que un sujeto que envía mails intimidatorios se tome tanto trabajo. Es posible, pero no ocurre con frecuencia.

No olvidemos que la dificultad no radica, en identificar el IP de la computadora que se mandó el mensaje. Sino que el problema es probar qué persona mandó el mail desde ese IP.

Pensemos en una situación que perfectamente puede ocurrir, el que desea mandar un mail intimidatorio, sin querer que lo descubran, se va a un locutorio a 10 kilómetros de su casa, crea en ese momento una cuenta de correo gratuita, pone allí datos totalmente falsos y luego envía el correo

[48] http://www.lanacion.com.ar/1172989-quien-me-mando-ese-mail-anonimo, Ariel Torres, , ¿Quién me mando ese mail anónimo?, publicado en la edición impresa, Viernes 11 de septiembre de 2009

[49] Ariel torres, La Nación, ¿Quién me mando ese mail anónimo?, 11 de septiembre, 2009, EDICION IMPRESA.

malintencionado, en ese caso de nada serviría conseguir el IP de esa computadora. Además de que en los locutorios casi siempre hay un NAT (Network Address Translation) para todas las PC.

La víctima buscará en el encabezado de ese mail un número IP, pero con solo ese dato no es suficiente, ya que lo complicado será probar que persona de todas las que usaron la computadora, fue la que lo envió.

Pablo Palazzi, abogado experto en alta tecnología, manifiesta que "Sólo se conocen un par de casos donde se pudo probar el delito. Uno fue el de un empleado de un banco que infectó la red con un virus, y lo descubrieron porque había una cámara filmando lo que hacía. El otro fue por amenazas enviadas por mail. Rastrearon los IP y pudieron procesar a uno de los dos culpables"[50].

Algunas personas, sobre todo quienes fueron víctimas de estos delitos, reprochan por qué, el gobierno no tiene una base de datos con los ISP registrados, o cuándo se usa una computadora pública no se les solicita a los usuarios que entreguen una identificación.

Los especialistas responden que una idea así, sería inútil, como medida a largo plazo, ya que los DNI, pasaportes y las cédulas también se pueden fraguar, y es altamente improbable que el empleado del locutorio conozca las técnicas para detectar documentos falsos.

Sabemos que estas prácticas ya están instaladas, por lo tanto se debe hacer algo al respecto.

Por último tenemos que tener en claro que el IP no es un dato personal, con el que se pueda relacionar directamente a una persona, la dirección IP sólo identifica una conexión. Para llegar a la persona detrás de toda esa cadena de números se requiere información adicional que sólo siguiendo los cursos de investigación normales se podría obtener.

[50] Ariel Torres, La Nación, ¿Quién me mando ese mail anónimo?, 11 de Septiembre, edición impresa.

Subcapitulo1:

Calumnias e injurias informáticas

Nuevos medios para cometer calumnias e injurias, se fueron propiciando a partir de las nuevas tecnologías, donde las imágenes, las relaciones sociales, vinculaciones profesionales, entre otros, se ponen a la vista de un sin número de usuarios, tornándose muy difícil la forma de evitar estas conductas, para lograr de alguna manera proteger a las personas de estas injurias y calumnias cibernéticas.

La calumnia según el art 109 del C.P. es la falsa imputación de un delito que dé lugar a acción pública, en cambio injuria es según el art.110 la deshonra o desacreditación a otro, la voz injuria hace referencia a toda expresión proferida en descrédito o menosprecio a otra persona

1-El honor como bien jurídico tutelado.

El Código Penal argentino no da el concepto de injuria, solo se limita a decir, que quien deshonrare o desacreditare a otro será reprimido con multa (conforme a la nueva reforma del código).

El bien jurídico protegido con sanción penal es el honor, independientemente si se lo hace en forma pública o privada[51].

El honor, como bien jurídico protegido en esta clase de tipos penales, puede ser considerado desde dos puntos de vista, desde un punto de vista subjetivo el honor significa la "autovaloración", la "propia estimación"; es decir, el juicio que cada uno de nosotros se forma de sí mismo.

Soler, expresa que “el honor subjetivo puede ser considerado "como una autovaloración, es decir, como el aprecio de la propia dignidad, como el juicio que cada cual tiene de sí mismo en cuanto sujeto de relaciones ético sociales[52]".

Ahora bien, el honor desde un punto de vista objetivo es lo que comúnmente se llama "reputación"; es decir, la valoración que los demás hacen de nosotros a través de nuestra conducta real o aparente.

[51] Núñez, Ricardo, manual de derecho penal parte especial

[52] Conf. Sebastián Soler; Tratado de Derecho Penal Argentino, T. III, Pág. 202. Ed. TEA, año 1992 (Gabriel h, Tobares Catala, Maximiliano Castro Arguello, Delitos Iinformáticos, advocatus)

El hombre, al actuar dentro de la sociedad, provoca en los demás, con sus actos, un juicio de valor. Esto es la reputación (lo que los demás piensan de nuestra integridad moral) y en ella reside el honor desde el punto de vista objetivo.

La reputación puede ser producto de una conducta real o aparente, según que el sujeto actúe como en realidad es, o que actúe disimulando sus vicios de modo tal que los demás lo vean de forma diferente a lo que es en realidad.

Núñez también distingue el honor entre las dos clases ya citadas y así expresa que "El honor (…) es la propia personalidad entendida como la suma de cualidades físicas, morales, jurídicas, sociales y profesionales, valiosas para la comunidad, atribuibles a las personas. Cuando el que atribuye esas cualidades es el propio interesado se habla de honor subjetivo u honra de la persona. Cuando los que le atribuyen esas cualidades al interesado son los terceros, se habla de honor objetivo o crédito de la persona"[53].

El honor subjetivo y el objetivo pueden no coincidir. Así por ejemplo, un hombre puede tener un bajo concepto de su dignidad y disimularlo con su conducta de modo tal que su reputación es la de un caballero.

Todas las personas poseen una autoestima determinada, la que sea. Algunos la tendrán más elevada que otros, pero ello no obsta a que cada cual tenga la suya propia y que ello sea de suma importancia para los hombres. Es la valoración como persona que cada uno tiene de sí mismo.

Corresponde aclarar ahora si la ley argentina protege el honor subjetivo o el objetivo. Sin dudas nuestra ley protege ambos, tanto el honor subjetivo como el objetivo.

La protección al primer aspecto está más marcada en los delitos de injurias, en tanto que en el segundo aspecto, lo está más en los delitos de calumnias.

El honor, como valor, ha sido reconocido en la Convención Americana sobre Derechos Humanos, 'Pacto de San José de Costa Rica, la cual en su art. 11 del Capítulo I de la Parte Primera, bajo el título "Protección de la honra y de la dignidad", reza: " 1- Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad".

Asimismo, dispone el inc. 2-: "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, o

[53] Conf. Nuñez Ricardo C., Manual de Derecho Penal, parte especial, 2da. Edición actualizada por Victor F. Reinaldo, Ed. Marcos Lerner, año 1999. (Gabriel h, Tobares Catala, Maximiliano Castro Arguello, Delitos Iinformáticos, advocatus)

en su domicilio o en su correspondencia, ni de ataque ilegales a su honra o reputación".

2-**Sujeto pasivo. Problemática**

Toda persona física, ser humano, es titular de un honor, honra o crédito, por lo que cualquier persona podría ser el sujeto pasivo, es decir la víctima de esta clase de delitos.

Nuestra Constitución Nacional en su artículo 15 prohíbe la esclavitud, concepto tomado de la Revolución Francesa de 1789, y de la Asamblea del año XIII que abolió la esclavitud, proclamando igualdad entre todos los hombres y la libertad de vientres.

Asimismo tampoco la incapacidad, ya sea esta por falta de edad legal, demencia, sordomudez, etc., no es impedimento para que aquella persona incapaz posea también un honor, el cual es tutelado.

Pero el problema se plantea cuando la pregunta es si las personas muertas pueden ser titulares de un honor.

Sólo sería admisible la acción cuando la calumnia o injuria indirectamente afectara a una persona viva, o cuando habiéndose dirigido contra una persona viva, fallecida ésta, la acción fuera continuada por sus sucesores.

El Código Penal no protege el honor como un derecho del cual sea titular un muerto, ni protege su memoria.

El art. 75 del C.P, una vez muerto el ofendido, les concede a sus familiares el ejercicio de la acción penal emergente de la calumnia o injuria inferida a aquél mientras vivía, no se refiere a la ofensa al honor de un muerto, sino a la ofensa al honor de una persona viva que luego fallece[54].

3-**Delito de Injuria.**

Según el diccionario de la Real Academia Española[55], la injuria es un “agravio o ultraje de obra o de palabra”; se vincula a la cuestión del honor, noción que en su dimensión subjetiva nos refiere a la autovaloración, al aprecio de la propia dignidad.

También tenemos que tener en cuenta que forma parte de aquella noción, la valoración que otros hacen de la personalidad ético-social de cada sujeto.

[54] Conf. Nuñez Ricardo C., Manual de Derecho Penal, parte especial, 2da. Edición actualizada por Víctor F. Reinaldo, Ed. Marcos Lerner, año 1999.

[55] http://www.rae.es/rae.html, Real academia española, Diccionario Panhispánico de dudas, octubre 2005

Nuestro código penal, sancionado a principios de la década del ´20, ubica esta figura en el Título II dentro de los denominados “delitos contra el honor”, a continuación del Título I, que enumera los delitos contra la vida.

Se encuentra regulada en el artículo 110 del Código penal, siendo la figura básica; la injuria viene así a ser el género y la calumnia la especie.

El honor es la valoración como persona que cada uno tiene de sí mismo muy dentro suyo, ya en la psiquis, ya en el espíritu, por el solo hecho de ser tal. Este aspecto se encuentra debidamente custodiado por la figura de la injuria, prevista y reprimida en el artículo 110 del Código Penal dentro de la esfera del verbo "deshonrar", por lo que la afección consiste en ofender moralmente, esto es, menospreciar a una persona, desestimarla.

La injuria es la ofensa genérica al honor ajeno; que puede ser a la honra de la persona (honor subjetivo), y en este caso es una lesión al derecho que tienen las personas a que los terceros respeten las cualidades que ellos le asignan a su personalidad.

O bien, puede ser una ofensa al crédito de la persona (honor objetivo), y en este caso es una lesión al derecho de las personas a que no se perjudique la opinión que sobre su personalidad tengan o puedan tener los terceros. Es la fama o reputación.

Es la acción de deshonrar o desacreditar a una persona, utilizando la red de redes como medio idóneo para expresar la injuria.

La deshonra está dada por el ataque a la propia valoración del honor o dignidad, y el descrédito por la ofensa a la estima que las demás personas tengan respecto de un sujeto, vale decir, su reputación.

3.1**Elemento objetivo**

La conducta del autor debe ser objetivamente injuriosa, es decir, que tiene o puede asumir un significado ofensivo.

Requiere imputaciones de calidades, costumbres o conductas que pueden ser apreciadas como peyorativas

3.2 **Elemento Subjetivo**.

“La injuria es una figura dolosa, por lo tanto debe existir en el sujeto activo, es decir la persona que profirió la ofensa, el conocimiento y la voluntad de cometer aquel hecho injurioso. Esto es lo que se ha denominado animus injuriandi”[56].

[56] Dayenoff David Elbio, Código Penal comentado, pág. 264, Ed. a-Z, año 2000.

Así lo ha expresado la jurisprudencia, al establecer que: “la injuria está constituida esencialmente por un elemento subjetivo, el designio, la intención, el ánimo de deshonrar o desacreditar a la persona. Ausente este ánimo de injuriar, no hay delito”.

3.3 **Consumación**.

La injuria se consuma en el momento en que la palabra o el hecho deshonrante llegan a conocimiento de su destinatario o de un tercero. Es un delito formal, que no requiere que el hecho dañe efectivamente la honra o el crédito ajeno.

Dependiendo de las modalidades utilizadas cabría la posibilidad de tentativa, como por ejemplo en el envío de un correo electrónico donde se ofende a una persona, pero cuya recepción no se produce por causas ajenas al autor.

Para llevar a cabo su cometido, el agente se puede valer de cualquier medio relacionado con Internet y las nuevas tecnologías de la información y comunicaciones que le sea útil para atribuir tal ofensa objetivamente injuriosa.

Por ejemplo, la colocación de frases ofensivas en portales de Internet, donde los individuos tienen la libertad, aunque limitada bajo ciertos parámetros por moderadores, de expresar sus ideas o intereses, es una forma de injuriar.

El delito es formal y se consuma con la realización de la conducta que deshonra o desacredita, aunque el ofendido no se haya sentido deshonrado o no haya alcanzado el descrédito ante los demás.

Lo que si es necesario, es que, por lo menos la ofensa llegue a conocimiento de terceros que puedan comprender su carácter ofensivo, no siendo obligatorio que la víctima lo conozca efectivamente.

Tampoco se requiere la publicidad de la injuria, la que puede llevarse a cabo mediante un correo electrónico, un chat, o un mensaje privado.

Pero no olvidemos que actualmente la publicidad se ve favorecida por la difusión generalizada del acceso que presenta la red de redes, en cualquier sujeto que tenga la oportunidad de acceder a una computadora con conexión a Internet, siempre teniendo en cuenta las restricciones que cada sitio tenga. Pero cualquiera que tenga acceso se puede enterar de esas injurias proferidas por estos medios.

3.4 **La llamada "prueba de la verdad".**

Respecto de la prueba de la verdad en el delito de injuria, la regla general es que el acusado no puede probar la verdad de su imputación, salvo en los casos establecidos por el artículo 111 del Código Penal.

El artículo 111 del Código Penal expresa que: "El acusado de injuria sólo podrá probar la verdad de la imputación (…) Si la imputación hubiere tenido por objeto defender o garantizar un interés público actual; Si el hecho atribuido a la persona ofendida, hubiere dado lugar a un proceso penal; Si el querellante pidiere la prueba de la imputación dirigida contra él (…)".

Sólo en estos tres casos que enumera la norma citada se admite la exceptio veritatis, la cual significa el derecho del querellado de probar la verdad de la imputación y quedar exento de pena.

El derecho de exigir la prueba de la verdad de la imputación, tiene como límite la incolumidad de los derechos o secretos de terceras personas. La prueba de la verdad debe ser hecha en la querella, pues contribuye a determinar los extremos de la acción ejercida y así respetar la defensa del querellado. La prueba de la verdad de la imputación por el querellado no justifica la injuria, pero se excusa al autor de la pena, porque ha obrado con arreglo a la verdad.

4. **Delito de Calumnia.**

La calumnia se encuentra regulada en el artículo 109 del Código penal, siendo la figura agravada de los delitos contra el honor. Dicha figura penal es definida por aquel cuerpo normativo como "la falsa imputación de un delito que dé lugar a la acción penal pública".

4.1. **Elemento Objetivo.**

La acción típica de la figura analizada es la atribución a otra persona de un delito que dé lugar a la acción pública. Esta atribución a persona o grupos de personas determinadas, tiene que ser falsa. Y debe utilizarse como medio de comisión, vías informáticas.

Acción pública, significa que la naturaleza de la imputación, implica el peligro para el ofendido de la posibilidad de un proceso penal en su contra. Esto no exige que la acción pública pueda ser ejercida en el caso concreto, sino que sólo requiere que se trate de un delito que, con arreglo a la ley, es perseguible por acción pública de oficio, con prescindencia de lo que suceda en el caso particular[57].

[57] Núñez Ricardo C., Manual de Derecho Penal, parte especial, 2da. Edición actualizada por Víctor F. Reinaldo, Ed. Marcos Lerner, año 1999.

La calumnia o falsa imputación en su elemento objetivo se refiere a la falsedad objetiva y se configurará cuando aquel no se haya cometido, o cuando no lo ha cometido la persona a quien se lo imputa.

La falsedad debe ser analizada objetivamente, por lo tanto verifica que falta un elemento de la relación imputativa; o que el hecho atribuido no ha existido; o que no ocurrió del modo como lo señala el agente y que lo convierten en un delito de acción pública.

El delito que el agente atribuya debe ser una conducta que esté penalmente contemplada y debe atribuirse como tentado o consumado, además de que tiene que ser un delito que dé lugar a la acción pública, puesto que si es de acción privada, claramente no será calumnia, pero podría constituir una injuria[58].

4.2 **Elemento Subjetivo**.

Dicha imputación o atribución del delito a otra persona debe ser intencionada, es decir a sabiendas de la falsedad de dicha atribución. Es el conocimiento de quien imputa, que aquella atribución de un delito es falsa.

Es necesario que el sujeto activo actúe con conocimiento de la falsedad de la imputación y con voluntad de efectuarla, pero no es necesaria la intención de causar perjuicio.

5. **Calumnias o injurias encubiertas.**

Son aquellas calumnias o injurias que no son manifiestas, es decir proferidas expresa o directamente, por ello son dudosas en su existencia. Es decir que se refiere a aquella ofensa que no se infiere abierta o directamente, sino valiéndose de detalles o circunstancias de los cuales puede deducirse a quien va dirigida, o utilizando palabras que pueden interpretarse con doble sentido.

Algunos autores ha criticado la disposición del artículo 112 del Código Penal, entre otras razones, por su falta de claridad y porque lo que es equívoco o encubierto, mal se concilia con el concepto de calumnia o con el ánimo de la injuria.

El carácter equívoco de la calumnia e injuria puede estar contenido en la dirección, es decir cuando no está claramente individualizado a quién va dirigida la ofensa, o puede estar en el contenido mismo de la injuria, lo cual se dará cuando pueda tener dos sentidos, esto es: ofensivo o inocente.

[58] DÁlessio, Andres Jose, ob. Cit.ps. 107/110 (Gabriel h, Tobares Catala, Maximiliano Castro Arguello, Delitos Iinformáticos, advocatus)

El carácter dudoso de la conducta desaparece si antes de la sentencia definitiva, en cualquier momento de juicio, el reo responsable da una explicación satisfactoria para el ofendido, o en su defecto, para el juez, sobre el sentido de su expresión o de su acto.

Este delito sólo puede tipificarse si el acusado se rehúsa a dar explicaciones acerca de su expresión.

6. **El honor y su vinculación con la libertad de prensa**

Prensa, en el sentido de la Constitución Nacional es la obra impresa destinada a la publicación de las ideas. Para Joaquín V. González, la palabra prensa comprende todas las formas de exteriorizar y poner en conocimiento del público ideas, opiniones, consejos, hechos, ya se presenten en libros, periódicos, hojas sueltas, circulares con o sin dibujo, ya de palabra o por escrito en sitios destinados o no a la publicidad.

Con los nuevos medios informáticos, el común de la gente, tiene un mayor acceso a publicar sus ideas, ya que se han abierto los novedosos diarios digitales, con actualizaciones inmediatas, y la con posibilidad de comentarios on-line de sus lectores.

Cuando la injuria o calumnia se hubiere propagado por medio de la prensa, tengamos en cuenta que también comprenden los medios de prensa informáticos, en la Capital y territorios nacionales, sus autores quedarán sometidos a las sanciones del presente Código y el juez o tribunal ordenará, si lo pidiere el ofendido, que los editores inserten en el mismo medio por el cual se propagó, a costa del culpable, la sentencia o satisfacción.

El código prevé un modo especial de reparación para este delito, que consiste en la publicación de la sentencia o satisfacción en los respectivos medios informáticos, a pedido del querellante.

El honor y la libertad de prensa son dos derechos a veces encontrados. Por un lado el honor es un derecho personalísimo de la persona humana, forma parte de sus derechos humanos, pero por el otro también existe el derecho a la libertad de prensa, fundamental en todo estado democrático y republicano.

7. **Problemática**

Podemos decir que por Internet se puede injuriar, o calumniar, cualquier medio expresivo es idóneo para ofender, basta que pueda ser vehículo de una voluntad ofensiva y que por alguien pueda ser entendido. Más problemático resulta definir entre otros temas, si el servidor puede ser incluido en la figura autónoma del art 113 del C.P que reprime como autor

de las calumnias e injurias al que publicare o reprodujere por cualquier medio, injurias o calumnias inferidas por otro.

Las acciones típicas son reproducir y publicar. Reproducir la calumnia vertida por otro, quien repite la ofensa. Llevándola a personas que no la habían captado cuando el autor original la produjo, divulgándola así a un mayor número de personas.

Obviamente tenemos que tener en cuenta que se exige que se trate de personas efectivamente dotada de la facultad de examinar el original y de impedir la publicación, es fácil de determinar si se trata de un editor de prensa, pero es difícilmente predicable de un servidor de internet, salvo en los casos en donde hace de moderador de grupos de discusión y que tiene la posibilidad concreta de examinar lo que quiere difundirse, y precisamente de eliminar lo lesivo[59].

El superior tribunal de justica de Brasil, se ha convertido en el primer órgano judicial en tomar en cuenta una denuncia por injurias en internet, los miembros del tribunal dijeron que utilizar la red para divulgar acusaciones personales no exime al responsable de ser juzgado por injuria, calumnia, o difamación[60].

Por ultimo traemos a colación la cámara web y el micrófono, la doctrina ha dejado en claro, que por estos medios también se pueden producir gestos o manifestaciones ofensivas.

Imágenes y palabras ofensivas pueden propagarse y circular por este mundo virtual, donde la facilidad y el anonimato son características de las que se vale el agente para llevar a cabo sus intenciones.

8. **Tentativa**

En cuanto a la posibilidad de tentativa de estos delitos, pueden darse casos donde el sujeto activo lleve a cabo el comienzo de la ejecución por hechos exteriores, no logrando la consumación del delito por causas ajenas a su voluntad, como por ejemplo el envío de un correo con contenido ofensivo, que no llegue a su destinatario por error del servidor.

Pero no podemos dejar de mencionar que respecto a estos casos hay un fallo de la cámara criminal y correccional de la capital federal, 2/12/1935, que habla que las injurias a distancia se consuman cuando por lo menos toma conocimiento un tercero del contenido.

[59] Freeland, Alejandro, internet y derecho penal, numero 3
[60] www.delitosinformaticos.com Fuente: Noticias.com

9. **Reforma**[61]

La ley 26.551 que modifica la parte del código penal referente a calumnias e injuria, fue sancionada por unanimidad de los 52 senadores presentes y pasó sin debate en la Cámara alta.

La norma sancionada ajusta los delitos de calumnias e injurias a la figura de la real malicia, doctrina fijada por la Corte Suprema de los Estados Unidos en el caso Sullivan / The New York Times , en la década del 60.

En ese sentido, elimina la pena de prisión por la comisión de esos delitos, reemplazándola por una multa pecuniaria que la ley fija entre los 3000 y los 30.000 pesos.

En ningún caso configurarán delito de calumnia las expresiones referidas a asuntos de interés público o a las que no sean asertivas, se establece en la norma.

En el caso de las injurias, se aclara además que no configurarán ese delito "los calificativos lesivos del honor cuando guardasen relación con un asunto de interés público".

Una de las fuentes en las que se basa esta reforma es en un fallo de la Corte Interamericana de Derechos Humanos a la Argentina, advirtiéndole que estos delitos tal como estaban configurados atentaban contra la libertad de expresión.

Expresiones no asertivas[62]

En lo que respecta al segundo requisito, la reforma ha incorporado, también, una rica elaboración jurisprudencial de la Corte Suprema. En efecto, en el fallo "Campillay c. la Razón", que dio origen al estándar de responsabilidad por el dicho de otro, la Corte Suprema habló de la necesidad de utilizar el tiempo de verbo potencial para ser eximido de responsabilidad. Más tarde, en el fallo "Granada", el Tribunal habló de "noticias asertivamente expuestas", al igual que en "Espinosa, Pedro Francisco c. Herrera de Noble, Ernestina". Años más tarde, en el fallo "Bruno", la Corte Suprema volvió a utilizar el término "asertivo"[63].

[61] Gabriel H. Tobares Catala, Maximiliano J. Castro Arguello, Delitos informaticos, editorial Advocatus, diciembre 2009. Publicado por Derecho de la COMUNICACIÓN- LA PLATA- Bs AS., Lunes 7 de Junio de 2010

[62] Publicado por Derecho de la COMUNICACIÓN- LA PLATA- Bs AS., Lunes 7 de Junio de 2010

[63] Delitos contra el honor. Reforma al Código Penal de la Nación por la ley 26.551, Rufino, Marco A, 11 Nov. 2011, http://legislacion.elderecho.com.ar

Pena de multa

Por último, se ha modificado la pena de todos los delitos del capítulo, reemplazándolas por la de multa exclusivamente. Esto trae como consecuencia, la posibilidad para el querellado de extinguir la acción con el pago de la multa. Al respecto, el art. 64 del Código Penal establece que la acción penal por delito reprimido con multa se extinguirá en cualquier estado de la instrucción y mientras no se hubiera iniciado el juicio, por el pago voluntario del mínimo de la multa correspondiente y la reparación de los daños causados por el delito. Si se hubiese iniciado el juicio, deberá pagarse el máximo de la multa correspondiente, además de repararse los daños causados por el delito.

La eliminación de la pena privativa de libertad, es una clara señal del legislador acerca del menor contenido de injusto que se le asigna a las acciones incriminadas, y una disminución del grado de protección del bien jurídico honor.

Conclusiones

En primer lugar, se reconoció expresamente que las personas jurídicas no tienen honor.

Por otra parte, se le otorgó mayor precisión al tipo penal, al establecer que el delito imputado falsamente a otro debe ser concreto y circunstanciado. Se incorporó así, de modo expreso, la elaboración jurisprudencial sobre el tema. En efecto, la imputación, para ser considerada calumnia, debe ser expresa, determinada, concreta y circunstanciada, esto es, constitutiva de todas las circunstancias (de modo, tiempo y lugar) que sirvan para determinar el delito en el caso concreto.

Se suprimió la pena de prisión por la de multa así como también se despenalizaron totalmente las expresiones sobre asuntos de interés público o las que no sean asertivas.

La reforma legal le ha otorgado mayor precisión al sujeto pasivo del delito, que debe tratarse de una persona física determinada.

Al igual que en las calumnias, también se han despenalizado en forma absoluta las expresiones sobre asuntos de interés público o las que no sean asertivas.

Quedan comprendidos dentro del concepto de interés público los calificativos lesivos del honor. De este modo, cabe colegir que la protección alcanza a los simples insultos y expresiones lacerantes, siempre que guarden relación con un tema de interés público.

La reforma suprimió, la parte que se refería al supuesto de si la imputación hubiere tenido por objeto defender o garantizar el interés público, pues esto ha quedado ya excluido de responsabilidad penal.

El legislador ha tenido en mente un proceso penal que no revista interés público, pues de lo contrario ya estaría comprendido en la excepción general. De todos modos, bien puede sostenerse que siempre que exista un proceso penal el interés público está comprometido.

Se eliminaron las injurias encubiertas o equívocas. Pese a que pocas veces se utilizaron estas figuras en la práctica de nuestros tribunales, debe considerarse un acierto su supresión por tratarse de tipos penales sumamente vagos e imprecisos.

Esta norma regula la responsabilidad penal por la reproducción del dicho de otro. En esta oportunidad, una vez más, el legislador tomó la elaboración de la jurisprudencia de la Corte Suprema en la materia.

Teniendo en cuenta el caso "Campillay", el Alto Tribunal sentó las bases que permitirían excusar la responsabilidad del periodista: a) atribución del contenido a la fuente; b) utilización de un verbo potencial; c) mantener en reserva la identidad del involucrado.

La ausencia de culpabilidad del hecho que dio origen a la retractación traerá aparejada consecuencias prácticas beneficiosas. Por un lado, incentivará la retractación en los casos de calumnias e injurias (esto ha sido poco común hasta ahora, precisamente, porque implicaba la aceptación de culpabilidad del querellado) y por el otro, trasladará al ámbito del derecho civil la discusión sobre la existencia o no del hecho lesivo y la responsabilidad del autor[64].

[64] http://derechodelacomunicacion.blogspot.com/2010/06/calumnias-e-injurias-su-modificacion-en.html, PUBLICADO EL LUNES 7 DE JULIO, 2010.

Sub-capitulo2:

Amenazas vía internet

Los delitos de amenaza y coacción se encuentran ubicados en el capítulo 1 del título V del CP argentino, más específicamente en el artículo 149 bis.

En el esquema de la ley, la amenaza representa el género y la coacción la especie. Algunos doctrinarios prefieren decir que la coacción representa un grado más en el ataque contra la voluntad puesto que quien coacciona se vale también de amenazas y de violencia.[65]

El medio utilizado para la comisión de estas figuras delictivas es internet a través de las nuevas tecnologías de la información posibilitando el anonimato principalmente y la impunidad[66] en algunos casos.

Se considera que este accionar delictivo se ha incrementado de manera considerable en los últimos años.

Los medios más utilizados son el correo electrónico, los mensajes de textos, las llamadas por teléfonos celulares, las publicaciones en páginas web y en portadas de redes sociales, entre otros.

Principalmente el delito de amenaza atenta contra el derecho de las personas a no ser víctimas de actos que alteren nuestra tranquilidad infundiéndonos temor , mientras que la coacción es una amenaza realizada con el propósito de obligarlo a que actúe , o no actúe, a que soporte o sufra algo .[67]

Siempre teniendo en cuenta que ambas conductas utilizan como medio soportes tecnológicos como herramienta para lograr su cometido.

Vale aclarar que tanto la amenaza como la coacción son dos conductas diferentes pero vinculadas entre sí, como ya dijimos, en una relación de género y especie.

Las amenazas, deben tener la finalidad de “alarmar o amedrentar” a una o más personas. Esto implica que la acción del sujeto activo debe estar dirigida a infundir miedo o atemorizar al sujeto pasivo. En cambio, en el caso de las coacciones (art. 149 bis, segundo párrafo, del Código Penal) la amenaza se anuncia con el objeto de lograr que la víctima se comporte de una determinada manera.

[65] D´Alessio , Andres Jose , Ob. Cit , p. 31 (Gabriel h, Tobares Catala, Maximiliano Castro Arguello, Delitos Iinformáticos, advocatus)

[66] www.elmundo.es/elmundo/2006.

[67] Núñez, Ricardo C. , Manual de derecho penal cit, ps. 187/189

La amenaza, entonces, contiene el anuncio de un daño, toda vez que se trata de una lesión o detrimento de un bien o interés de una persona, dependiente de la voluntad de quien lo expresa; debe ser futuro, ya que sólo de ese modo puede constituir un peligro potencial para la víctima, capaz de perturbar su normalidad vital (cónf. Creus, Carlos, "Derecho Penal, Parte Especial", t. I, ed. Astrea, Buenos Aires, 1983, pág. 331.

Es necesario que la amenaza sea grave, que se anuncie con seriedad, ya que de lo contrario no es posible amedrentar o motivar una decisión. De no ser así, jamás podría lesionarse la libertad psíquica del sujeto pasivo.

La amenaza debe ser idónea para atemorizar o amedrentar. Ello significa que, independientemente del medio utilizado el anuncio debe ser formulado de manera tal que resulte inteligible como advertencia de un mal futuro para el sujeto pasivo.

1-**Bien jurídico protegido:**

Lo que se tutela es la libertad, vista la libertad como un conjunto de derechos que el individuo puede ejercitar y cuyo límite está fijado por el ejercicio de los demás y las restricciones indispensables para el desenvolvimiento de la vida en comunidad, todo lo cual resulta de las imposiciones del ordenamiento jurídico, tendientes a mantener el orden social y a evitar la lesión de los derechos ajenos [68].

Para Ricardo Núñez la libertad del hombre es la facultad de poder obrar de una manera o de otra y el derecho a no sufrir injerencias en el ámbito material o espiritual de sus derechos y en la defensa de sus intereses.

Para Creus, sin embargo, hay dos aspectos en la protección de la libertad alrededor de los cuales se nuclean los distintos tipos penales.

Para D´Alessio por un lado está la manifestación de la libre actividad de la persona para decidir que quiere hacer, y para hacer lo que ha decidido y por otro lado se refiere a la manifestación de la reserva de una zona de intimidad de la que el individuo tiene derecho a excluir toda intromisión de terceros.

[68] D´Alessio, Andres Jose , ob. Cit. p .239

2. Acción

Entendemos por amenaza cualquier acto mediante el cual el sujeto activo sin motivos legítimos afirma que deliberadamente quiere causarle a otra persona un mal futuro. Este mal futuro debe ser dependiente de la voluntad del sujeto que amenaza. Se utiliza como instrumento o medio para anunciar a la víctima del daño ya sea en su persona, intereses, o afectos cualquiera de los soportes tecnológicos de internet como ser correo electrónico, mensajes de textos , entre otros.

Debe necesariamente tratarse de un daño ilegitimo, es decir, que no esté obligado a sufrir y futuro.

El anuncio debe ser grave, injusto e idóneo. Como grave se entiende de posible realización y de entidad suficiente para amedrentar. Por injusto, que el mal no tiene por qué ser soportado por la victima. Y por último la idoneidad hace referencia a que el anuncio debe tener capacidad suficiente para crear el estado de alarma en la victima.

No podemos dejar de aclarar que el mal tiene que ser formulado de manera tal que sea inteligible como amenaza para el sujeto pasivo, o sea tiene que entender que se lo está amenazando.

En la coacción el autor hace uso de amenazas pero con un propósito, el de obligar a otro a hacer, no hacer o a tolerar algo. Siempre contra su voluntad. Analizando particularmente la injusticia de la amenaza coactiva vemos que esta puede provenir de la injusticia del daño anunciado o de la finalidad perseguida por el sujeto activo.

No olvidemos que en este caso, también el medio empleado para el logro de la mencionada finalidad es el uso de internet, medios informáticos y dispositivos de alta tecnología.

3. **Elemento subjetivo**:

Se exige el dolo directo, por parte del sujeto activo en ambas figuras.

Que obre con conocimiento que está amenazando, y querer hacerlo con el fin de amedrentar, o en el caso de la coacción, que el autor realice la acción con el propósito de obligar a la víctima a hacer, o no hacer o tolerar algo contra su voluntad, siempre utilizando como medio la tecnología.

Amparadas en el anonimato del ciberespacio, muchas personas intimidan a otras mediante correo electrónico, mensajes de texto, o por medio de los espacios de redes sociales.

El más común, de este tipo de delitos, es la amenaza de muerte.

Le siguen la extorsión y la divulgación de hechos que afectan el honor de las víctimas.

Los casos, que se registran en este tipo de delitos van en aumento, y no son fáciles de investigar. El principal obstáculo, que se presenta, es el anonimato que brinda el mundo virtual.

En el caso de los mensajes de texto de telefonía celular, las personas que cometen el ilícito suelen utilizar líneas que no puedan ser identificadas o enviarlos desde las páginas web de las compañías de telefonía móvil.

En internet, es muy común habilitar una casilla de correo con datos falsos. De esa manera, las amenazas o intentos de extorsión no pueden ser rastreados con facilidad, ya que los datos ingresados para abrir la casilla no corresponden a una persona de existencia real.

Sin contar que además, en la mayoría de los casos, los mails se envían desde un ciber o desde una oficina de trabajo, lo que complica aún más la identificación.

El temor que las amenazas provocan en las víctimas, también juega en contra, ya que estas tienden a borrar este tipo de mensajes, y así se pierden las pruebas que la Policía y la Justicia necesitan.

Capítulo III

Nuevas formas de atentar contra la privacidad y la comunicación.

La Constitución Nacional en el artículo 18 dispone que la correspondencia y los papeles privados sean inviolables. Los Tratados Internacionales, con igual jerarquía a la Constitución de acuerdo al artículo 75 inciso 22, protegen la correspondencia y los papeles privados. Así lo establecen el Pacto de San José de Costa Rica (art. 11, inc. 2º), el Pacto Internacionales de Derechos Civiles y Políticos (art. 17), la Declaración Universal de Derechos Humanos (art. 12), y la de Derechos y Deberes del Hombre (art. X).

Asimismo, el Código Civil en el artículo 1071 bis. Establece que *"el que arbitrariamente se entrometiere en la vida ajena (…) será obligado a cesar en tales actividades"* y la ley de propiedad intelectual (11.723) en los arts. 31 a 35 resguarda el derecho a la propia imagen.

Aunque muchas sean las normas que protejan este bien jurídico, tan preciado como es la intimidad, la legislación, tenía grandes grietas en ciertos aspectos, como ser los referidos a las correspondencias informáticas y a los documentos electrónicos.

Desde que aparecieron estas nuevas formas de comunicación, antes impensadas, su masividad en tan poco tiempo, y la capacidad de achicar distancias, provocó ventajas, pero a la vez fue utilizado como un terreno fértil, para vulnerar derechos, espiar la vida ajena o sabotear redes, empresas y organismos.

En 1998 el sitio de la corte suprema de justicia de la nación, fue "hackeado", a lo que el magistrado Sergio Torres, del juzgado federal N °12 respondió que existe un "claro vacío legal" para juzgar delitos informáticos.

Los miembros de la Corte presentaron una denuncia por daños y presunta asociación ilícita. La respuesta del juez Torres giró en torno a la imposibilidad de tipificar como delito ese tipo de conductas: "una página web no puede asimilarse al concepto de cosa. Ello es así en tanto y en cuanto, por su naturaleza, no es un objeto corpóreo ni puede ser detectado materialmente", para concluir que solo las "personas", los "animales" y las "cosas" están protegidos por el Código Penal.

Según el magistrado, las páginas de Internet no encajan en ninguna de las tres categorías: serían "elementos inmateriales", laguna que ya fue llenada desde la promulgación de la ley 26.388.

El caso Lanata, es el primer fallo argentino que consideró equiparado al correo electrónico con la correspondencia epistolar.

En 1999, Edgardo Héctor Martolio inició una querella penal contra el periodista Jorge Ernesto Lanata por los delitos de violación de correspondencia y publicidad de correspondencia con fundamento en los arts.153 y 155 del Código Penal.

La causa comenzó cuando Martolio demandó a Lanata por haber publicado, en la revista “Veintiuno”, los textos de cinco e-mails que circularon por el correo interno del diario Perfil días antes de su cierre.

Ante dicho tribunal, Lanata, planteó un incidente de excepción de falta de acción por hecho atípico, al no encontrarse específicamente incluidos en el Código Penal Argentino, el que fue rechazado con fecha 2 de agosto de 1999.

Los fallos establecieron que tanto el artículo 153 como el art.155 del Código Penal, dejaron abierta la descripción típica a los "despachos de otra naturaleza" y a cualquier "otro papel privado"; pudiendo considerarse equiparado entonces el correo electrónico a la correspondencia tradicional.

Finalmente, la Sala VI de la Cámara Criminal y Correccional equiparó el e-mail con el correo epistolar tradicional. El tribunal estableció que: “El avance de la tecnología en este sentido, pareciera haber dejado en la obsolescencia el bien jurídico que tutela el Capítulo III, Titulo V del Código Penal, en especial a los artículos que se ocupan de la protección de los papeles privados y la correspondencia. Pero queda claro que el tan difundido e-mail de nuestros días es un medio idóneo, certero y veloz para enviar y recibir todo tipo de mensajes, misivas, fotografías, archivos completos, es decir, amplía la gama de posibilidades que brindaba el correo tradicional al usuario que tenga acceso al nuevo sistema.

Los documentos emitidos por la Unión Europea en los últimos años, consideran al correo electrónico como un servicio de transmisión y conducción de señales por las redes y se incentiva el uso de este medio de comunicación en las nuevas relaciones humanas, ya sea en forma privada o laboral.

La velocidad e inmediatez, su naturaleza multi-mediática (envío de cualquier tipo de archivos, imágenes y videos), la posibilidad de remitirlo a varios destinatarios simultáneamente y el bajo costo convirtieron al correo electrónico en una herramienta de uso masivo.

El artículo 153 del Código Penal, incorporó la comunicación electrónica y la expresión "indebidamente" en el tipo penal, para disipar dudas respecto a “requerir la finalidad dolosa del autor del delito y reafirmar la hermenéutica tendiente a considerar excluidos del delito a quienes en procura de mejorar el servicio que prestan a sus usuarios, activan mecanismos de protección, tales como antivirus, filtros o algoritmos de

desvío de correo electrónico para evitar lo que se conoce como spam o la recepción de correos no deseados por sus clientes".

La oportuna reforma de estos artículos del Código Penal evita dejar sin amparo a situaciones tan delicadas como la vulneración de correspondencia en soporte electrónico, la alteración de sitios web y acceso, manipulación y difusión arbitrarias de informaciones confiadas al resguardo de bases de datos personales.

Además debe destacarse una vez más la trascendencia que reviste la definición amplia del término *documento*: "toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión".

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

1. Protección de la privacidad

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Según la Real Academia Española[69] , un sistema operativo es un programa o conjuntos de programas que efectúan la gestión de los procesos básicos de un proceso informático, y permite la normal ejecución del resto de las operaciones.

Un sistema informático es el conjunto de hardware, software y de un soporte humano, el sistema informático emplea una computadora con dispositivos programables para capturar, almacenar y procesar datos.[70]

Cuando se utilizan los datos de manera legitima y legal, en términos de seguridad de redes se considera que los datos pasan por tres pasos fundamentales cada uno de ellos de forma ordenada: 1) autenticación 2) autorización y 3) auditoría.

Autenticación[71]:

Es la seguridad del ordenador, es el proceso de intento de verificar la identidad digital del remitente de una comunicación como de una petición para conectarse. En web de confianza, autenticación[72] es un modo de asegurar que los usuarios son quienes ellos dicen que son.

Autorización:

Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de ella.

Auditoria:

Es aquí donde la red registra todos y cada uno de los accesos a los recursos que realiza el usuario autorizado o no[73].

Primero se chequea si existe o no el usuario y si la contraseña coincide o no coincide con la base de datos, lógicamente si coinciden logra acceder sin problemas, en cambio si la contraseña es incorrecta o el usuario no se encuentra en la base de datos se informa que los datos son incorrectos y es imposible su acceso.

Pero existen casos , en los que se producen accesos no autorizados , producto de la explotación de una vulnerabilidad en el sistema

[69] www.buscon.rae.es, Diccionario de la Lengua Española, vigesima segunda edición.

[70] www.wikipedia.org

[71] ↑ Griego: *αυθεντικός* = verdadero o genuino, de ' los authentes' = el autor

[72] Con este mismo sentido se ha creado modernamente el verbo *autentificar*, que se considera también válido; Diccionario panhispánico de dudas,

[73] Htpp://es.wikipedia.org

del servidor , o en algunas de sus aplicaciones , o en la utilización de algún otro método como malware, sniffer, ingeniería social , fuerza bruta , entre otros . Y es aquí donde se ve afectado el derecho a la intimidad.

2. **Bien jurídico protegido** :

En este caso la tutela se centra en el contenido mismo que soporta un dato o sistema informático siendo confidencial para su titular que de alguna manera o por cualquier motivo no lo hace público y limita su acceso a personas autorizadas.

Lo que se intenta resguardar es aquella información de carácter confidencial, y es así que lo ubicamos dentro del derecho de la intimidad que recepta nuestra constitución nacional en los artículos 18 y 19.

Las recientes reformas a nuestro ordenamiento de fondo, en materia de delitos informáticos, contemplan dos figuras de acceso indebido, no autorizado o ilegitimo a sistemas informados

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

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

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros

Por ultimo no podemos dejar de mencionar que la ley de habeas data, ley 25.326, incorporo dos artículos al cuerpo normativo penal en el que se tipifican nuevas conductas relacionadas con la protección de los datos personales contenidos en archivos de bases de datos.

De esta manera las intromisiones informáticas alcanzan por primera vez protección penal, consagrando así la protección de la privacidad de los archivos informáticos respectos de intrusos, son los típicos casos de hacking.

Esta figura no requiere modificación alguna de los datos ni que sea borrado, adulterado, agregado, o copiado sino que es suficiente la intromisión.[74]

A pesar de esta nueva incorporación todavía resulta insuficiente, ya que por el momento, solamente son resguardados de la intromisión, los datos personales y no así aquellos casos en los que particularmente se vulneran sistemas o datos informáticos que no reúnen las características para ser denominados datos personales propiamente dichos, que son aquellos que son protegidos con la confidencialidad.

La confidencialidad de datos, se refiere precisamente a datos confidenciales, ya que si los datos de hallan en archivos securizados, pero no son confidenciales, sino públicos por encontrarse en lugar de acceso irrestricto, no se configuraría el delito[75].

El interés por los temas relacionados con el derecho a la intimidad ha renacido en nuestro medio, como consecuencia de las agresiones que el ámbito privado de las personas sufre en la actualidad, provenientes de la utilización de las más recientes técnicas electrónicas, que permiten penetrar impunemente en todos los ambientes habitualmente reservados a la privacidad.

Los medios técnicos han ampliado enormemente las posibilidades de trasgresión de la intimidad de las personas y, en consecuencia, las leyes deben adaptarse para protegerla eficazmente.

Esta sofisticación de las posibilidades de trasgresión hace que en la actualidad el derecho a la intimidad deba ser estudiado en forma multidisciplinaria: constitucional, penal, administrativa, civil y procesal, pues su naturaleza participa de todas esas ramas del derecho, y requiere tanto la protección de una ley especial, en el derecho interno, como un nuevo derecho internacional en la materia, que regule la transferencia de datos entre los países, así como las restantes injerencias arbitrarias a la vida íntima de las personas que se cometen desde países extranjeros.

[74] Palazzi , Pablo A. , derecho y nuevas tecnologías año 3 Numero especial 4-5

[75] Dayenoff, jurisprudencia, esquema de defensa, 8va edición reformada y actualizada , editora A-Z, BS As, 2003.p.404.

3. **Antecedentes constitucionales del derecho a la intimidad**:

Las primeras manifestaciones del derecho de las personas a gozar de un ámbito íntimo se presentan históricamente frente al poder del Estado. Ante los allanamientos arbitrarios de domicilio, se plantea la protección del ámbito doméstico, limitando los poderes estatales con garantías jurisdiccionales.

Es así que al otorgar la monarquía inglesa la Carta Magna, en el año 1215, se establece la inviolabilidad del domicilio, y es a partir de este antecedente que el constitucionalismo de los siglos XVIII y XIX establece la protección de las libertades fundamentales.

En nuestro derecho constitucional originario, la protección de la intimidad de los habitantes frente a los poderes públicos se concreta en dos direcciones: por una parte, se consagra la inviolabilidad del domicilio y de los papeles privados (CN, artículo 18); y por otra, se establece el interés público como límite a la injerencia en la vida privada de las personas (CN, artículo 19), disposición esta última que protege, aunque sin mencionarlo, el derecho de las personas a la autonomía, es decir, a conducirse libremente en todas aquellas materias que no afecten el interés social.

La reforma de 1994, al incorporar al texto de la ley suprema, las disposiciones del Pacto de San José de Costa Rica (Convención Americana sobre Derechos Humanos), le ha conferido al derecho a la intimidad el rango de libertad constitucionalmente garantizada. El artículo 11 de la convención establece: "1.- Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2.- Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3.- Toda persona tiene derecho a la intimidad es todo aquello que el individuo tiene derecho de sustraer al conocimiento público. Es un área protegida en torno a su persona física, a su círculo familiar, a su tranquilidad personal y a su autonomía de acción, que le confiere acciones para evitar toda intromisión en la misma.

Incluye, además, el derecho de controlar la información que se ha puesto en poder de terceros, el cual es protegido mediante el habeas data.

La evolución constante de las tecnologías dirigidas a la comunicación, la telefonía, las cámaras de vigilancia, los dispositivos de escucha, la computación, los correos electrónicos, la Internet, las bases de datos públicas y privadas y la posibilidad de su comercialización, ha obligado a establecer nuevos medios de protección de la intimidad de las personas.

No cabe hoy día la menor duda, que los medios electrónicos actualmente disponibles permiten todo tipo de intromisiones en la vida íntima de las personas, a punto tal que debemos reconocer que, de una

forma u otra, se ha restringido el ámbito concreto en que se puede gozar de intimidad.

Por ello, no puede limitarse la investigación del fenómeno únicamente a las comunicaciones electrónicas, pues el ámbito en que las nuevas tecnologías permiten invadir las áreas de intimidad es mucho mayor, y por ello, las personas deben contar con adecuada protección de la misma frente a todas las tecnologías actualmente disponibles.

4. Afectación de la intimidad a través de comunicaciones electrónicas

Podríamos limitar el alcance del término comunicaciones electrónicas a su forma más corriente y masiva de trascender en la sociedad, es decir, a los correos electrónicos.

Pero las comunicaciones electrónicas son mucho más.

Los correos electrónicos resultan sólo una especie dentro del género "mensajes de datos" entendidos como toda información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares .

Frente a los avances tecnológicos se abre un vasto abanico de posibilidades que permiten intromisiones en la vida íntima de las personas, que obligan a establecer nuevos y adecuados sistemas de protección, tanto técnicos como jurídicos.

Así y conforme adelantamos, la privacidad de los individuos puede verse afectada tanto por:

a) la violación de sus correos electrónicos;

b) el almacenamiento de sus datos personales en bases públicas o privadas;

c) la transmisión de tales datos personales;

d) la captación y derivación de comunicaciones remotas;

e) la publicación en Internet de información vinculada a su esfera íntima, o la aparición de fotografías reales o adulteradas por procesos técnicos, entre otros.

5. Las nuevas figuras de la era informática: Hackers, crackers, phreakers

La era informática ha generado nuevas figuras en materia de delitos contra la intimidad, la libertad, la propiedad y la fe pública: los hackers, crakers y phreakers.

Se denomina hacker a la persona que, valiéndose de medios informáticos y de telecomunicaciones, accede remotamente y en forma no autorizada a sistemas de información cuyo acceso le está vedado. Su

motivación es el simple deseo de quebrantar el sistema y ve en ello un desafío a su intelecto.

Realiza esta actividad sin intención de provocar daño en las cosas, aunque ocasionalmente y de manera accidental puede destruir información o dañar los sistemas.

Cracker, se utiliza para denominar a la persona que, por idénticos medios, accede a sistemas de información que le son vedados, pero con la intención de provocar un daño o apoderarse indebidamente de información.

Phreacker es la persona que, para llevar a cabo la actividad de hacker o de cracker, utiliza indebidamente líneas telefónicas puesto que, más allá del valor de los pulsos telefónicos utilizados, su motivación es evitar ser rastreado por el software específico diseñado al efecto. Uno de los problemas fundamentales relacionados con estas actividades es la casi imposibilidad de probar que el sistema ha sido vulnerado y de identificar al autor.

Subcapitulo1:

Derecho a la información y sobre la información

Los constantes avances tecnológicos en materia informática han propiciado la aparición de nuevos conceptos, generando asimismo la modificación de otros tantos, enriqueciéndolos en la mayoría de ocasiones, así el contenido del término "información", que según la definición de la Real Academia de la Lengua Española significa: "enterar, dar noticia de algo" y que en términos legos hubiera significado tan sólo una simple acumulación de datos, se ha ampliado, transformándose como advierte Gutiérrez Francés: "en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico"[76].

Hoy en día no resulta suficiente poseer la información, es necesario además tener la capacidad de almacenarla, tratarla y transmitirla eficientemente, de allí que "la información" deba ser entendida como un proceso en el cual se englobe los tres supuestos:

1-almacenamiento,
2-tratamiento,
3-transmisión

El derecho a la información, nace en el mismo momento que un dato cualquiera puede ser comunicable. Los datos sobre las personas y los patrimonios pertenecen a quienes le competen, aunque no sea su autor.

El derecho sobre la información puede entrar en conflicto con el derecho a la información. En el caso de los datos personales, el orden jurídico puede otorgar a las personas, como ocurre de hecho bajo la legislación francesa, la facultad de oponerse a la inclusión de ciertos datos en un archivo o base de datos, y su consecuente divulgación. La mayor parte de los datos, sin embargo son públicos, y por lo tantos accesibles a todos en un Estado de derecho en el cual se reconoce el pluralismo de la información y la libre investigación científica.

La propiedad de los datos, sería, un derecho frágil debido a la "inmaterialidad" de su objeto, y a la facilidad con que aquél puede ser vulnerado mediante la divulgación del dato.

El derecho a la información es el de recolectar los datos públicos para crear libremente el bien-información. No puede aplicarse a una información privada, pero da derecho a obtener un acceso libre e igual a tal información, desde que ella se haga pública.

La tesis expansiva del concepto de propiedad a la información, no goza, por cierto, de general aceptación. La información no debe ser tratada

[76] www.wikipedia.com, enviado por: Victor Hugo Quijada Tacuri

necesariamente como una mercancía, sino como un recurso común, y por lo tanto no le es aplicable el concepto de propiedad.

1. **Bien jurídico protegido**

La información es el bien jurídico protegido de este tipo de delitos.

Es advertido, todavía, por la doctrina y jurisprudencia penal que todavía falta tipicidad respecto a algunas acciones relacionadas con las nuevas tecnologías.

La información ha sido un factor fundamental en la existencia humana. En el mundo moderno el acceso a la información es un derecho que puede ser ejercido libremente por cualquier persona. Salvo, cuando por su uso puedan afectarse otros derechos, como ser el derecho a la intimidad, el patrimonio económico, la libre competencia o la seguridad de un estado.

El bien jurídico tutelado en los delitos informáticos, es la información en sí misma, su titularidad, autoría, integridad, disponibilidad, seguridad, transmisión, confidencialidad.

Quizás el fundamento de elevar a rango de bien jurídico, a la información, en los delitos informáticos, estaba dado porque en nuestros días es un bien que interesa y concierne a la sociedad toda.

Capítulo IV:

Daño informático. Formas de cometerlo.

Los avances técnicos y científicos, la intensificación de las relaciones humanas, el desarrollo de los medios de comunicación y la aparición de las relaciones de consumo, nos presentan un panorama diferente en el que los daños se han incrementado.

Los beneficios derivados de aquellos avances característicos de la era posmoderna, imponen la asunción de necesarios riesgos y costos y la posibilidad de sufrir alguno de esos "nuevos daños" que exige a los operadores jurídicos, la labor de encontrar nuevos caminos para atender a estos problemas.

El daño informático se puede definir como toda lesión o menoscabo causado a un derecho subjetivo o interés legítimo mediante la utilización de medios electrónicos destinados al tratamiento automático de la información

Como señala Lorenzetti, el surgimiento de la era digital ha suscitado la necesidad de repensar importantes aspectos relativos a la organización social, a la democracia, a la tecnología, a la privacidad y a la libertad. En el campo de la responsabilidad por daños, el tema es de gran interés por los múltiples aspectos que encierra: la afectación de la libertad de expresión, la ubicación de un responsable, la jurisdicción aplicable, la causalidad, la garantía del crédito de la víctima[77].

Para poder entender este delito informático, primero debemos hacer unas pequeñas aclaraciones respecto a que se denomina daño, en forma general.

Daño es el detrimento, perjuicio o menoscabo en el patrimonio, en la persona[78] , en los bienes, en el honor, fama, consideración, etc.[79] .

Otras definiciones de doctrinarios hacen referencia a que se trata del atentado producido sobre el patrimonio de una persona, causando un perjuicio que se conduce con la pérdida misma de la cosa, o disminución de su valor.

Evidentemente el alcance de estas definiciones es demasiado abarcativa, por lo que deberemos, por nuestra materia de estudio desentrañar el alcance y sentido de la norma penal aplicable, primero a la figura básica de daño, de nuestro código penal.

---

[77] Lorenzetti, Ricardo Luis, "La responsabilidad por daños en Internet", en "Derecho Privad. Homenaje al Dr. Alberto Bueres", Oscar Ameal (director), Buenos Aires, Hammurabi, 2.001, pág. 1.707 y sgtes.

[78] http://www.bibliojuridica.org/libros/1/364/14.pdf, Barros, Enrique (2006). *Tratado de la responsabilidad extracontractual*, Editorial Jurídica de Chile.

[79] De León , Gonzalo, diccionario de derecho romano, Bs As, 1962

El capítulo VII, del Código Penal argentino trata del delito de daños, dentro de los que afectan el derecho de propiedad. En el Código Penal argentino el delito de daños está contemplado en su forma simple, en el artículo 183, que castiga con 15 días a 1 año de prisión al que destruya, inutilice, hiciere desaparecer, o de cualquier modo ocasione un daño a una cosa mueble o inmueble o a un animal que le sea ajeno, ya sea en forma total o parcial. Solo se aplicará este precepto si no se configura un delito que conlleve mayor pena.

El daño como delito, surge cuando la Revolución Francesa consagró a la propiedad privada y su respeto, como un bien fundamental, y pasible de pena a quien la agravie, y no solo de sanción civil con indemnización de daños y perjuicios. El Código francés de 1810 ya lo incorporó como figura penal.

En la legislación romana el daño injustamente causado estuvo contemplado en la Lex Aquilia, cuyo capítulo primero condenaba a quien matare a un esclavo de otro, o a un animal cuadrúpedo gregario, no propio, con el máximo valor que hubiera alcanzado en el año anterior al hecho dañoso. El capítulo III condenaba cualquier otro tipo de daño con el máximo valor que la cosa hubiera tenido, en los 30 días anteriores al daño cometido. No había sanciones penales, sino solo resarcitorias.

En el año 2008 los avances tecnológicos obligaron a agregar un párrafo al artículo, a través de la ley 26.388, para castigar de igual modo los daños informáticos, comprendiendo la destrucción o inutilización de datos, programas, documentos, o sistemas informáticos; o también a quien con el fin de causar daño, venda, distribuya, haga circular o introduzca en un sistema informático, un programa cualquiera.

1. **Bien jurídico protegido**

Nuestro código penal no contiene una definición de lo que debe entenderse por cosa, por lo tanto debemos recurrir al código civil:

“las cosas son sujetos materiales susceptibles de tener un valor. Las disposiciones referentes a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de apropiación, art 2311. Los objetos inmateriales susceptibles de valor, e igualmente las cosas, se llaman bienes, el conjunto de los bienes de una persona constituye su patrimonio, art 2312.

Con la sanción de la ley 26.388, queda claro que se persigue penalmente a quien dirija su ataque contra datos, documentos, programa o sistemas informáticos.

El Código Penal argentino regula los delitos contra la propiedad en su título VII, donde el concepto de propiedad como bien jurídico protegido se acerca al concepto contemplado en la garantía constitucional del art 17, conteniendo el dominio y demás relaciones reales, así como las facultades que se tiene sobre los bienes, provenientes de los derechos personales.

A partir de la reforma al art 183 del código penal, el alcance protectorio es aún mayor, debiendo hacerse extensivo este amparo a aspectos tales como la privacidad de las personas, seguridad supraindividual, los que pueden ser atacados mediante conductas consistentes en: destrucción y alteración de datos, tiempo de inoperatividad de los sistemas, incumplimiento de tareas solicitadas y mala imagen pública con el consiguiente perjuicio económico[80].

Para configurar el delito se requiere entonces que la cosa no sea propia, al menos en parte, por ejemplo, el caso de que se halle en condominio. Debe además tener un dueño, aunque la haya perdido[81].

También debe el daño no ser momentáneo sino que debe perdurar cierto tiempo, y que se necesite cierta inversión de tiempo y dinero para que pueda arreglarse[82].

El daño debe ser un fin en sí mismo.[83]

Se admite la tentativa, si el delito no llegare a consumarse[84].

Los agravantes del delito de daños están contemplados en el artículo 184, castigándose con prisión de 3 meses a 4 años si ocurren los siguientes supuestos:

Si el daño se cometiera en sistemas informáticos destinados a la prestación de servicios de salud, de provisión o transporte de energía, de medios de transporte, de comunicaciones, o en cualquier otro servicio público[85].

2. **Acción** [86]

La acción típica consiste en dañar, al igual que en la figura básica, pero lo distintivo está en el bien jurídico protegido, en el objeto sobre el cual recae la conducta criminosa.

[80] Luz Clara Bibiana, Manual de derecho informático, Nova tesis, Bs As, 2001, ps 118-120.

[81] PONENCIA N* 4 Responsabilidad por daños derivados de Internet (Reparación y prevención de los daños) Por Claudio Fabricio Leiva, Buenos Aires, 9 y 10 de Junio de 2005- Facultad de Derecho - Univ. de Buenos Aires

[82] Hilda Juarez, página de internet la guía del derecho 2000, el 17 de septiembre de 2009

[83] Hilda Juarez, página de internet la guía del derecho 2000, el 17 de septiembre de 2009

[84] Luz Clara Bibiana, Manual de derecho informático, Nova tesis, Bs As, 2001, ps 118-120.

[85] Hilda Juarez, página de internet la guía del derecho 2000, el 17 de septiembre de 2009

[86] Gabriel H. Tobares Catala, Maximiliano J. Castro Arguello, Delitos informaticos, editorial Advocatus, diciembre 2009

Configura el delito, cuando el autor: alterare, destruyere o inutilizare, datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños art 10 de la ley 26.388.

Se entiende por alterar, a cambiar la esencia o forma de algo; por destruir, a deshacerla o arruinarla de manera total o parcial, alterando su naturaleza o estructura; por inutilizar, a alterar su naturaleza o estructura, pero de forma que deje de ser apta para la función que estaba destinada.[87]

En el proyecto de ley 64/2002 proponía que para que se configurase el delito de daño informático, el autor del hecho debía "maliciosamente destruir, inutilizar, modificar, borrar, hacer inaccesible (…), como podemos observar se exigía que la conducta sea dolosa, por ello maliciosamente, pero la reforma, ignoró ese aspecto, con lo que doctrinarios consideran que en cuanto al tipo subjetivo se respetó la sistemática de la figura básica del art 183 C.P.

Aunque algunos estudiosos del derecho no dejan de afirmar que la reciente reforma al Código Penal sólo reprime la comisión de delitos dolosos, es decir, aquellos producidos con la intención y voluntad de producir el daño.

Puede decirse que el daño informático responde estructuralmente a todas las características propias del daño genéricamente considerado, lo cual posee la trascendente virtualidad de sujetar la figura en cuestión a la totalidad de los principios comunes y generales del régimen de responsabilidad civil[88].

La existencia de una forma particularizada en la producción del daño, utilización de medios automáticos para el procesamiento de la información, justifica plenamente el tratamiento específico del problema.

La utilización de medios automáticos o electrónicos es el instrumento idóneo para la producción del daño informático[89].

La expresión "medios electrónicos" pretende superar en amplitud y comprensividad a las variadas construcciones doctrinarias que referencian a computadoras, ordenadores, etc., por cuanto aparece suficientemente extensa como para receptar la evolución vertiginosa de la

[87] D´Alessio, Andrés José, código penal comentado y anotado. Parte especial, La Ley, Bs As, 2006, p.567.

[88] Calderón, Maximiliano Rafael. Hiruela, María del Pilar, "La prevención y reparación del daño informático", en "Derecho de Daños. Economía. Mercado. Derechos Personalísimos", op. cit., pág. 375 y sgtes.

[89] Gabriel H. Tobares Catala, Maximiliano J. Castro Arguello, Delitos informaticos, editorial Advocatus, diciembre 2009

tecnología y la técnica, que, en breves espacios temporales, podría dejar tales expresiones obsoletas[90].

El tratamiento informatizado de datos es propiamente el objeto de la informática, determinando el contenido de las operaciones efectuadas en utilización de sistemas de computación; es la sustancialidad de este aspecto que resulta definitiva de la informatización del daño, particularizándolo en relación a otros usos alternativos posibles mediante los mismos medios electrónicos[91].

.

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

Se puede diferenciar dos grupos de daños: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos

No son pocos los problemas que acarrea la determinación del o de los sujetos responsables por los daños derivados de Internet.

Debemos individualizar los sujetos que, de distintas maneras, intervienen en el fenómeno que representa Internet. Entre esos sujetos, se encuentran el usuario, el autor del contenido, los proveedores de información, los proveedores de servicios y hosting y los proveedores de acceso a Internet.

Existe pluralidad de sujetos actuando en redes, unidos por contratos conexos, en los que parece difícil imputar responsabilidad a uno de ellos por la actuación de otros. Por lo tanto hay que distinguir varios supuestos:

1-Un sujeto que accede a una página web puede celebrar un contrato en el que el otro contratante se obliga a una prestación que realiza por intermedio de varios sujetos que el obligado selecciona. Hay un contrato, una obligación, una parte pasivamente obligado. En este caso, el obligado responde por los sustitutos, auxiliares o dependientes que utilizó para el cumplimiento de la obligación.

2-Un sujeto que accede a una página puede contratar un servicio que es realizado por varios sujetos; se da en el caso un contrato, una obligación y una pluralidad de sujetos pasivamente obligados.

[90] Calderón, Maximiliano Rafael. Hiruela, María del Pilar, "Daño informático y derechos personalísimos", op. cit., pág. 368.

[91] Lorenzetti, Ricardo Luis, "La responsabilidad por daños en Internet", op. cit., pág. 1.714 y 1.715.

En este caso, no hay un sujeto que responde por los auxiliares que él eligió, sino varios sujetos en paridad, entre los cuales puede haber mancomunación o solidaridad.

3-Un sujeto que accede a la página puede celebrar varios contratos con varios sujetos. Es el supuesto más frecuente, porque la página aparece como un producto fragmentado objetiva y subjetivamente y en el caso existen varios contratos que causan varias obligaciones diferentes.

En este caso, cada obligado no responde, ni mancomunada ni solidariamente por las obligaciones contraídas por otros sujetos en otros contratos, porque se aplica el efecto relativo de los contratos, que no pueden obligar ni perjudicar a terceros que no han intervenido en ellos.

En la responsabilidad extracontractual, la conducta ilícita es desempeñada de modo autónomo por uno de los sujetos y el problema reside en si es posible o no imputar a los otros que tienen algún vínculo con el autor.

Entre los sujetos no hay una relación de dependencia que permita afirmar la existencia de una garantía por el hecho ajeno, lo cual requiere esfuerzos mayores y más complejos en orden a los fundamentos.

También en este ámbito de responsabilidad la cuestión gira alrededor de la imputación basada en el control y la apariencia[92].

3. **Formas agravadas**

La ley 26.388 al disponer en su art 11 la sustitución del art 184 del código de fondo, admite una nueva gama de conductas que atentan contra programas o sistemas informáticos públicos.

Art. 11.- Sustitúyase el artículo 184 del Código Penal, por el siguiente

"Artículo 184.- La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2. Producir infección o contagio en aves u otros animales domésticos;

3. Emplear substancias venenosas o corrosivas;

[92] Lorenzetti, Ricardo Luis, "La responsabilidad por daños en Internet", pág. 1.715.

4. Cometer el delito en despoblado y en banda;

5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos,documentos, programas o sistemas informáticos públicos;

6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público."

5. **La prevención del daño informático**.

Quizás uno de los desafíos del momento para el ordenamiento jurídico consista, precisamente, en dar respuestas acordes a situaciones en las que la reparación del daño queda relegada a un segundo plano, adquiriendo protagonismo la cuestión de “prevenir” o “evitar” el daño.

Advierte Matilde Zavala de González: “En obras tradicionales sobre responsabilidad por daños se estudiaban sus presupuestos, con algún descuido sobre las consecuencias prácticas en lo atinente a la prevención del daño. Ello se explica en buena medida porque los riesgos actuales de dañosidad han aumentado hasta niveles antes no concebibles.

El principio de eficacia exige considerar con suma atención los resultados y no sólo los presupuestos de las instituciones jurídicas. Dentro de aquellos, adquiere valor prioritario el no dañar, impidiendo la causación de perjuicios injustos.

Lorenzetti asevera que la responsabilidad por daños tiene efectos distributivos que ya nadie niega y su análisis se transforma inmediatamente en un análisis de cuestiones públicas: si un consumidor compra un producto y tiene una falla en virtud de la cual sufre daños, tiene una pretensión indemnizatoria; el derecho privado clausura el debate mediante un análisis histórico del problema: la determinación de la responsabilidad en la causación del perjuicio.

El cambio de óptica operado en el Derecho de Daños ha dado un rol protagónico a la justicia distributiva: la preocupación del legislador y del intérprete es proteger al débil jurídico, la víctima que ha sufrido un daño en forma injusta.

El Derecho de Daños es la especialidad desde la cual surgen los grandes principios de la prevención del daño como una faceta importante y diferenciada de la función reparadora tradicional; sin embargo, ese nacimiento en el derecho de fondo presenta hondas raíces en el derecho constitucional, y vinculaciones ineludibles con el derecho procesal.

Se destaca que la singular relevancia económica propia del fenómeno informático, sumada a la generalización del empleo de ordenadores en todos los ámbitos de la sociedad, tiene como consecuencia la necesidad aún más imperiosa de enfatizar el aspecto preventivo de la responsabilidad, a los efectos de evitar crisis financieras en las empresas responsables de una reparación, que terminen generando inconvenientes de gravedad en la economía nacional y sobre todo en la estructura social y laboral.

Como medidas de prevención, podrían adoptarse:

Control estatal de la actividad informática, mediante la creación de un registro específico relativo a las redes y banco de datos, consignando expresamente el fin que ellos persiguen y los datos que pueden contener.

Constitución de una autoridad de aplicación, que tenga facultades para habilitar, regular y cancelar determinadas inscripciones registrales.

Articulación procesal de acciones protectoras, como el hábeas scriptum, el hábeas data y la acción de oposición.

Si bien toda actividad humana genera en función de las circunstancias márgenes de riesgo de daño para terceros, aún la más inofensiva, en materia de prevención de daños informáticos, la cuestión radica en descifrar dónde poner el límite para mensurar cuándo ella pueda o no ser limitada, en aras de prevenir el riesgo de daño que engendra a terceros.

5. **Conductas dirigidas a causar daños físicos**

El primer grupo comprende todo tipo de conductas destinadas a la destrucción física del hardware y el software de un sistema, como causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc. estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

6. **Conductas dirigidas a causar daños lógicos[93]**

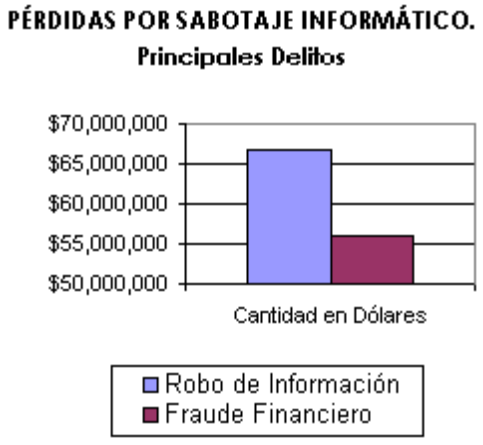
Se refiere a todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático[94].

Se lo puede cometer de diversas maneras, desenchufando la máquina, con la que se está trabajando, borrando, modificando documentos o utilizando los más complejos programas de destrucción lógica.

Estos programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada. Sin pretender realizar una clasificación rigurosa de estos métodos de destrucción lógica, podemos distinguir:

Bombas lógicas (time bombs)[95]: En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo, o por la aparición de determinada señal, como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.

La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa.



[96]

[93] Gabriel H. Tobares Catala, Maximiliano J. Castro Arguello, Delitos informaticos, editorial Advocatus, diciembre 2009

[94] Gabriel H. Tobares Catala, Maximiliano J. Castro Arguello, Delitos informaticos, editorial Advocatus, diciembre 2009

[95] Gabriel H. Tobares Catala, Maximiliano J. Castro Arguello, Delitos informaticos, editorial Advocatus, diciembre 2009

[96] Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Delitos Informáticos, Universidad de El Salvador, Octubre de 2000

Las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados informaron $66.708,000) y el fraude financiero (53 encuestados informaron $55.996,000)[97].

[97] Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Delitos Informáticos, Universidad de El Salvador, Octubre de 2000

Capítulo V

Seguridad contra los delitos informáticos[98].

Hoy en día, muchos usuarios no confían en la seguridad de Internet.

En 1996, IDC Research realizó una encuesta en donde el 90% 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, u otros datos importantes que afecten su economía, o vida privada o laboral.

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 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 las realizan.

La privacidad o confidencialidad, es el más obvio de los aspectos y se refiere a que la información solo puede ser conocida por individuos autorizados.

Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos.

La integridad de datos

La integridad 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 y lo borre.

[98] Gabriel h, Tobares Catala, Maximiliano Castro Arguello, Delitos Iinformáticos, advocatus

La disponibilidad de la información

se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Medidas de seguridad de la red

Existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que se debe hacer es diseñar una política de seguridad. En ella, definir quiénes tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas, y preocuparse de hacerlas cambiar periódicamente cortafuegos.}

Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Una de las maneras drásticas de no tener invasores es la de poner murallas. Los mecanismos más usados para la protección de la red interna de otras externas son los firewalls o cortafuegos.

Se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según nuestras indicación.

Firma digital[99]

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 la particularidad de estar equiparada a la firma manuscrita:

“Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia. (Art 3)”

Cuando se habla de contrataciones electrónicas, existe un problema que se repite en distintas operaciones, y que es tratado por muchos doctrinarios, como es la dificultad para identificar a las partes.

Existen distintos sistemas de identificación, como ser la tarjeta magnética, que tiene el riesgo que sea utilizado por otro sujeto; la clave magnética; el número de código, todos estos con el mismo inconveniente

[99] Go course, INFORMATICA JURIDICA, Cristina González Unsueta, año 2009, Universidad siglo21,

que puede ser usado por otro, la palabra de orden; el reconocimiento del timbre de la voz ;la impresión digital; el reconocimiento y memorización de la firma del usuario; y la firma digital, con los efectos jurídicos que produce en nuestro derecho presumiendo la autoría del mensaje (ley 25.506).

La firma digital resulta de un procedimiento matemático, que implementado de manera correcta garantiza no solo la autenticidad del documento sino la comprobación del emisor. Esta firma no necesita otros medios de prueba en caso de conflicto, es una presunción "iuris et de iure"[100].

Su particularidad es que es una clave asimétrica, de doble encriptación, tiene una clave pública y una privada[101].

Sin lugar a dudas la firma digital es lo más segura para contratar electrónicamente.

Por eso las empresas deberían comenzar a incorporar mecanismos para que la firma digital sea posible de ser usas en sus transacciones.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por él.

No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas.

Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo[102].

Estas distintas medidas de protección no tienen por qué ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos

[100] Go course, INFORMATICA JURIDICA, Cristina González Unsueta, año 2009, Universidad siglo21
[101] Go course, INFORMATICA JURIDICA, Cristina González Unsueta, año 2009, Universidad siglo21
[102] Go course, INFORMATICA JURIDICA, Cristina González Unsueta, año 2009, Universidad siglo21

sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

La reciente reforma hecha a nuestro código penal, está dirigida a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

El Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos, señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada[103].

Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos[104]:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

[103] ESTRADA GARAVILLA MIGUEL, DELITOS INFORMÁTICOS, Universidad Abierta

[104] Egil Emilio Ramírez Bejerano, Ana Rosa Aguilera Rodríguez, LOS DELITOS INFORMÁTICOS. TRATAMIENTO INTERNACIONAL, Mayo 2009

Conceptualizaciones propias de la materia.

Delito informático:

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún.

Daño informático:

Se denomina así a todo ataque, borrado, destrucción o alteración intencional de dichos bienes intangibles. Asimismo, la incriminación tiende también a proteger a los usuarios contra los virus informáticos, caballos de Troya, gusanos, bombas lógicas y otras amenazas similares.

Firma digital:

Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. La firma digital no implica que el mensaje esté encriptado, es decir, que este no pueda ser leído por otras personas; al igual que cuando se firma un documento holográficamente este sí puede ser visualizado por otras personas.
El procedimiento utilizado para firmar digitalmente un mensaje es el siguiente: el firmante genera mediante una función matemática una huella digital del mensaje. Esta huella digital se encripta con la clave privada del firmante, y el resultado es lo que se denomina firma digital la cual se enviará adjunta al mensaje original. De esta manera el firmante va a estar adjuntando al documento una marca que es única para ese documento y que sólo él es capaz de producir.
El receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación y que el firmante es quién dice serlo a través del siguiente procedimiento: en primer término generará la huella digital del mensaje recibido, luego desencriptará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo.

Seguridad informática:

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.

Informática:

Ciencia que estudia el tratamiento automático de la información en computadoras, dispositivos electrónicos y sistemas informáticos.

Proviene del francés informatique y fue acuñado por el ingeniero Philippe Dreyfus en 1962. Formó una conjunción entre las palabras "información" y "automatique".

Ip:

Protocolo para la comunicación en una red a través de paquetes conmutados, es principalmente usado en Internet. Los datos se envían en bloques conocidos como paquetes de un determinado tamaño .El envío es no fiable.

Los paquetes poseen una cabecera con información sobre la máquina de origen y la de destino (sus direcciones IP), con esta información los enrutadores determinan por dónde enviar la información. Cada paquete de un mismo archivo puede enviarse por diferentes rutas dependiendo de la congestión del momento.

Computadora

Una computadora o computador (del latín computare -calcular-), también denominada ordenador (del francés ordinateur, y éste del latín ordinator), es una máquina electrónica que recibe y procesa datos para convertirlos en información útil. Una computadora es una colección de circuitos integrados y otros componentes relacionados que puede ejecutar con exactitud, rapidez y de acuerdo a lo indicado por un usuario o automáticamente por otro programa, una gran variedad de secuencias o rutinas de instrucciones que son ordenadas, organizadas y sistematizadas en función a una amplia gama de aplicaciones prácticas y precisamente determinadas, proceso al cual se le ha denominado con el nombre de programación y al que lo realiza se le llama programador. La computadora, además de la rutina o programa informático, necesita de datos específicos (a estos datos, en conjunto, se les conoce como "Input" en inglés o de entrada) que deben ser suministrados, y que son requeridos al momento de la ejecución, para proporcionar el producto final del procesamiento de datos, que recibe el nombre de "output" o de salida. La información puede ser entonces utilizada, reinterpretada, copiada, transferida, o retransmitida a otra(s)

persona(s), computadora(s) o componente(s) electrónico(s) local o remotamente usando diferentes sistemas de telecomunicación, pudiendo ser grabada, salvada o almacenada en algún tipo de dispositivo o unidad de almacenamiento.

Dispositivo

Aparato, artificio, mecanismo, artefacto, órgano, elemento de un sistema.

En las computadoras los distintos dispositivos conectados a ellas deben ser reconocidos por el sistema operativo y para ello se utilizan controladores (drivers).

En el nuevo ordenamiento se establece que el término "**documento**" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (art. 77 Código Penal).
Los términos "**firma" y "suscripción**" comprenden la firma digital, la creación de una firma digital o firmar digitalmente (art. 77 Código Penal).
Los términos "**instrumento privado**" y "**certificado**" comprenden el documento digital firmado digitalmente (art. 77 Código Penal).

Conclusión

A medida que iba realizando el trabajo me encontré con ciertas dificultades referidas a la búsqueda de información, ya que el derecho informático es una rama muy nueva y en constante formación, y por otra parte la ley 26.388, fue sancionada hace apenas un año.

Otras de las limitaciones que tuve que superar fue la gran cantidad de creencias, y datos que no era correctos, que se barajaban, sobre todo, los referido a que sobre internet no había ninguna legislación, dejando entrever que era un paraíso sin leyes, o que no se realizaban investigaciones ya que era imposible encontrar verdaderos culpables.

Quede asombrada al ver cuáles son los números económicos que se barajan, referidos a sabotaje informático, y cuántos son los usuarios que casi a diario se encuentran con dificultades referida al tema, con un virus, con la sorpresa que su cuenta ha sido violada, por nombrar algunas de las modalidades más comunes.

Es imprescindible , que la sociedad toda tome medidas para frenar el avance de este tipo de delitos, que al ser casi de especialistas, quedamos muy afuera de una protección, con solo tomar recaudos normales, por eso, una medida acertada seria formar a los usuarios, para que estén preparados.

Debido a la naturaleza de estos delitos, se hace muy difícil su tipificación, para que todas sus modalidades queden comprendidas, tantos las presentes como unas posteriores que se pueden formar. Esto ocurre porque la constante innovación tecnológica en muchos casos es más rápida que el dinamismo que la ley requiere, para hacer frente es este tipo de delitos.

Podríamos afirmar que no estamos ante la presencia de un crimen perfecto, pero sí de delitos muy difíciles de investigar en algunos casos, por eso es necesario, que se potencie la seguridad informática y que sean más estrictos los controles sobre el uso de ésta tecnología tan masiva.

Pero no podemos dejar de admitir que los beneficios que otorgan los progresos tecnológicos, la finalidad para los que fueron creados, muchas veces son tergiversados, provocando una desnaturalización de su esencia.

La utilidad que le de cada usuario, a veces traspasa el ámbito de lo privado, y atenta contra bienes jurídicos protegidos. Es ahí donde la ley 26.388, esta para atacar a los responsables del delito.

Anexo

LEY 26551 CÓDIGO PENAL
Modificación
sanc. 18/11/2009; promul. 26/11/2009; publ. 27/11/2009

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

Art. 1.- Sustitúyase el artículo 109 del Código Penal de la Nación, por el siguiente:

Art. 109.- La calumnia o falsa imputación a una persona física determinada de la comisión de un delito concreto y circunstanciado que dé lugar a la acción pública, será reprimida con multa de pesos tres mil ($ 3.000.-) a pesos treinta mil ($ 30.000.-). En ningún caso configurarán delito de calumnia las expresiones referidas a asuntos de interés público o las que no sean asertivas.

Art. 2.- Sustitúyase el artículo 110 del Código Penal de la Nación, por el siguiente:

Art. 110.- El que intencionalmente deshonrare o desacreditare a una persona física determinada será reprimido con multa de pesos mil quinientos ($ 1.500.-) a pesos veinte mil ($ 20.000.-). En ningún caso configurarán delito de injurias las expresiones referidas a asuntos de interés público o las que no sean asertivas. Tampoco configurarán delito de injurias los calificativos lesivos del honor cuando guardasen relación con un asunto de interés público.

Art. 3.- Sustitúyase el artículo 111 del Código Penal de la Nación, por el siguiente:

Art. 111.- El acusado de injuria, en los casos en los que las expresiones de ningún modo estén vinculadas con asuntos de interés público, no podrá probar la verdad de la imputación salvo en los casos siguientes:

1) Si el hecho atribuido a la persona ofendida, hubiere dado lugar a un proceso penal.

2) Si el querellante pidiera la prueba de la imputación dirigida contra él.

En estos casos, si se probare la verdad de las imputaciones, el acusado quedará exento de pena.

Art . 4.- Derógase el artículo 112 del Código Penal de la Nación.

Art . 5.- Sustitúyase el artículo 113 del Código Penal de la Nación, por el siguiente:

Art. 113.- El que publicare o reprodujere, por cualquier medio, injurias o calumnias inferidas por otro, será reprimido como autor de las injurias o calumnias de que se trate, siempre que su contenido no fuera atribuido en forma sustancialmente fiel a la fuente pertinente. En ningún caso configurarán delito de calumnia las expresiones referidas a asuntos de interés público o las que no sean asertivas.

Art . 6.- Sustitúyase el artículo 117 del Código Penal de la Nación, por el siguiente:

Art. 117.- El acusado de injuria o calumnia quedará exento de pena si se retractare públicamente, antes de contestar la querella o en el acto de hacerlo. La retractación no importará para el acusado la aceptación de su culpabilidad.

Art . 7.- Comuníquese al Poder Ejecutivo nacional.

JOSE J. B. PAMPURO. EDUARDO A. FELLNER. Enrique Hidalgo. Juan H. Estrada

Bibliografía

- Código penal, editorial Estudio, edición, 2006
- Dayenoff David Elbio, Código Penal comentado, Ed. a-Z, año 2000.
- Fernández Delpech, Horacio, Derecho Informático, internet http://www.hfernandezdelpech.com.ar
- Gabriel h, Tobares Catala, Maximiliano Castro Arguello, delitos informaticos, advocatus
- http://es.wikipedia.org
- http://www.delitosinformaticos.com
- http://www.delitosinformaticos.com.ar
- http://www.delitosinformaticos.info
- http://www.infobaeprofesional.com
- http://www.infoleg.gov.ar
- http://www.lagaceta.com.ar
- http://www.lanacion.com.ar
- http://www.rae.es/rae
- Joaquín V. Gonzalez, Manual de la Constitución Argentina, 6ta. Edición, Nro. 157.
- LIMA de la LUZ, María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrua. México. Enero-Julio 1984
- Maximiliano Octavio Davies, Lorena Elbaum, Derecho Penal 1.
- Melvin Leonardo Landaverde Contreras, Joaquín Galileo Soto Campos Jorge Marcelo Torres Lipe , Delitos Informáticos, Universidad de El Salvador, Octubre de 2000.
- 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 informáticas, Viena, 8 a 17 de mayo, 2001.
- Núñez, Ricardo, Manual de Derecho Penal parte especial
- Quiroga Lavie, Humberto. Constitución nacional comentada, editorial Rubinzal.
- Ramos, Los Delitos contra el honor,
- Revista Express, Catamarca, 2010, informática forense de Microsoft business
- Sebastián Soler; Tratado de Derecho Penal Argentino, Ed. TEA, año 1992
- TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996
- Terán lomas, Roberto a. m., derecho penal. Parte general, t, 1.,pag 318,
- Torres, de Neuquén, penal parte especial, edición 2006
- Trabajo de investigación realizado por Ricardo Levene (nieto) y Alicia Chiaravalloti,. Publicado en el Vl Congreso Latinoamericano en 1998, en Colonia, Uruguay.
- www.seguridadydefensa.com

- ZAFFARONI, Eugenio Raúl, Manual de Derecho Penal, Parte General, Ediar, 2005
- Gabriel H. Tobares Catala, Maximiliano J. Castro Arguello, Delitos informaticos, editorial Advocatus, diciembre 2009.
- Revista Internauta de Práctica Jurídica, PRINCIPIOS DE CRIMINOLOGÍA ,Dr. Mario Eduardo Corigliano, Agosto-Diciembre 2006
- Egil Emilio Ramírez Bejerano, Ana Rosa Aguilera Rodríguez, LOS DELITOS INFORMÁTICOS. TRATAMIENTO INTERNACIONAL, Mayo 2009

"Delitos Informáticos"

Resumen

En esta tesis final de graduación, se llevará a cabo una investigación exhaustiva de un nuevo tipo de delito, llamados "delitos informáticos", para ello vamos a analizar la doctrina específica, como así también la ley 26.388, que modifica el Código Penal de la República Argentina. Vamos a demostrar por qué son llamados "delitos de cuello blanco", por qué es tan difícil su investigación y llegaremos a una conclusión acerca del impacto que este tipo de delitos provoca en la sociedad. Para introducirnos en el estudio de esta nueva forma delictual, respetaremos la trilogía planteada por la ONU para reconocer a esta clase de delitos. Vamos a analizar las principales formas de comisión de cada delito, las características y sujetos activos y pasivos. Nos centraremos sobre todo en la presentación y descripción de los medios de comisión, aquellos medios informáticos que hacen posible estos delitos que tanto daño producen en los sistemas informáticos de todo el mundo, así como en el patrimonio de los particulares.

"COMPUTER CRIMES"

Abstract

In this final thesis Graduation, we will conduct a thorough investigation of a new type of crimes, called "computer crimes", for this we will analyze the specific doctrine as well as 26,388 law amending the Penal Code of Argentina. We will demonstrate why they are called "white collar crime," why is it so difficult to research and come to a conclusion about what is the impact that this type of crime on society. To introduce the study of this new type of crime, we will respect the trilogy raised by the UN for recognize each type of crime. We will analyze the main forms of commission of each offense, characteristics, and active and passive subjects. We will focus particularly on the presentation and description of the means of commission, those storage media that make possible the commission of these crimes that much damage occur in large computer systems worldwide, as well as cause pecuniary damages.

Formulario descriptivo del Trabajo Final de Graduación

Identificación del Autor

Apellido y nombre del autor:	**Haarscher Agustina**
E-mail:	**Agustina_haarscher@hotmail.com**
Título de grado que obtiene:	**ABOGADA**

Identificación del Trabajo Final de Graduación

Título del TFG en español	**"Delitos Informáticos"**
Título del TFG en inglés	**"Computer Crimes"**
Tipo de TFG (PAP, PIA, IDC)	
Integrantes de la CAE	**Abogados. José Lago - Maximiliano Davies**
Fecha de último coloquio con la CAE	**22/12/2011**
Versión digital del TFG: contenido y tipo de archivo en el que fue guardado	**CD**

Autorización de publicación en formato electrónico

Autorizo por la presente, a la Biblioteca de la Universidad Empresarial Siglo 21 a publicar la versión electrónica de mi tesis. (marcar con una cruz lo que corresponda)

utorización de Publicación electrónica: Inmediata

☐ **si, inmediatamente**

☐ **Si, después de ….. mes(es)**

☐ **no autorizo**

_____

firma del alumno