UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE CIENCIAS MATEMÁTICAS
UNIDAD DE POST GRADO

Marco Conceptual de los Delitos Informáticos

TESIS Para optar el grado académico de MAGÍSTER EN COMPUTACIÓN E INFORMÁTICA

AUTOR
Luis Miguel Romero Echevarria

LIMA – PERÚ 2005

MARCO CONCEPTUAL DE LOS DELITOS INFORMÁTICOS

LUIS MIGUEL ROMERO ECHEVARRIA

Tesis presentada a consideración del cuerpo docente de la Facultad de Ciencias Matemáticas de la Universidad Nacional Mayor de San Marcos, como parte de los requisitos para obtener el Grado de Magíster en Computación e Informática.

Aprobado por:

Mg. Alfredo Alva Bravo
Presidente

Mg. Luz del Pino Rodríguez
Miembro

Mg. Roberto Calmet Agnelli
Miembro

Mg. Virginia Vera Pomalaza
Miembro

Mg. Luzmila Elisa Pro Concepción
Miembro Asesor

LIMA – PERÚ

Diciembre – 2005

FICHA CATALOGRÁFICA

ROMERO ECHEVARRIA, LUIS MIGUEL

Marco Conceptual de los Delitos Informáticos, (Lima) 2005.

ix, 138 p., 29,7 cm. (UNMSM, Maestría, Computación e Informática, 2005).

Tesis, Universidad nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas 1. Computación e Informática.

I. UNMSM/FdeCM II. Maestria (Serie).

AGRADECIMIENTOS:

A Dios por permitirme realizar este trabajo intelectual.

A mis padres quienes me infundieron la ética y el rigor que guían mi transitar por la vida.

A mi esposa e hijas por su comprensión durante los años que le dediqué a este trabajo de Tesis.

A mi asesora Luzmila por su asesoramiento científico y estímulo para seguir creciendo intelectualmente.

RESUMEN

MARCO CONCEPTUAL DE LOS DELITOS INFORMÁTICOS

LUIS MIGUEL ROMERO ECHEVARRIA

DICIEMBRE – 2005

Orientadora : Mag. Luzmila Elisa Pro Concepción

Título obtenido : Maestría en Computación e Informática

La tesis presenta una investigación sobre la propuesta de elaboración del Nuevo Marco Teórico de los Delitos Informáticos en el Perú y los aspectos que involucra su uso como apoyo teórico-científico para los operadores de justicia que actúan sobre los delitos informáticos (Policías, Fiscales y Jueces) y de otras instituciones y organizaciones comprometidos en la lucha contra dicha problemática. Se ha considerado como casos de estudio los marcos teóricos publicados por el INEI, Julio Núñez, Julio Téllez y Blossiers-Calderón, quienes hicieron público sus trabajos vía Internet. Se comienza esbozando el Estado del Arte de los Delitos Informáticos sustentados por los principales especialistas del tema y la metodología de trabajo en el desarrollo de la presente investigación. Esta última se inició con una investigación documental sobre el tema, sucedida por la aplicación del Método Histórico, seguida por una entrevista de opinión a los operadores de justicia de los delitos informáticos sobre el grado de aceptación del nuevo marco teórico propuesto y, por último, se presenta la nueva propuesta de un marco conceptual sobre los delitos informáticos; así como las conclusiones y recomendaciones para el uso y perfeccionamiento del nuevo marco teórico.

PALABRAS CLAVE: MARCO CONCEPTUAL
DELITO
INFORMÁTICA
OPERADOR

SUMMARY

CONCEPTUAL FRAME OF THE COMPUTER SCIENCE CRIMES

LUIS MIGUEL ROMERO ECHEVARRIA

DECEMBER – 2005

Orientation : Mag. Luzmila Elisa Pro Conception

Obtained Title : Masters in Computation and Computer Science

The thesis presents an investigation on the proposal of elaboration of the New Theoretical Frame of the Computer Science Crimes in Peru and the aspects that its use like support involves theoretical-scientist for the justice operators which they act on the computer science crimes (Police, Public prosecutors and Judges) and of other institutions and organizations jeopardize in the fight against problematic happiness. It has been considered as cases of study the theoretical marks published by the INEI, Julio Núñez, Julio Téllez and Blossiers-Calderón, that made public their works via Internet. It is begun outlining the State-of-the-art of the Computer science Crimes sustained by the main specialists of the subject and the methodology of work in the development of the present investigation. This last one began with a documentary investigation on the subject, happened by the application of the Historical Method, followed by an interview of opinion the operators of justice of the computer science crimes on the degree of acceptance of the new proposed theoretical frame and, finally, the new proposal of a conceptual frame appears on the computer science crimes; as well as the conclusions and recommendations for the use and improvement of the new theoretical frame.

KEY WORDS : CONCEPTUAL FRAME
CRIME
COMPUTER SCIENCE
OPERATOR

INDICE

INTRODUCCIÓN

Los delitos informáticos viene causando temor a nivel internacional, estos tipos de delincuentes se basan en el avance de la tecnología y los retos que representan para ellos, entre ser un hacker o cracker existe una línea muy delgada, el uso inadecuado de tecnología emergente hace que siempre estemos a la defensiva[1].

La presente tesis titulada "Marco Conceptual de los Delitos Informáticos", tiene como finalidad principal de convertirse en un instrumento teórico-científico de utilidad para los operadores de justicia que actúan sobre los delitos informáticos (Policías, Fiscales y Jueces) y como un aporte para la comunidad científica para encontrar respuestas sobre la problemática actual.

La humanidad no esta 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.

Lo que debemos evitar es que las personas que tienen conocimientos medios o altos de informática o computación y que vienen tomando conductas ilegales respecto a páginas web de personas naturales o jurídicas (empresas); conocidos como hackers, crackers o sus diversas modalidades,

---

[1] Prevención técnica y prevención legal de los delitos informáticos. Luis Romero. Mundo Internet 2005- Libro de Ponencias –Volumen I. España pp. 649

los mismos que tienen en tensión todos los sistemas informáticos poniendo en peligro la seguridad de la información que es patrimonio de las empresas.

En el contexto peruano, es necesario señalar que la comisión de los delitos informáticos acarrean la criminalidad informática, debiéndose entender a ésta como los actos que vulneran la ley vigente, es decir que se tipifique el delito en el Código Penal Peruano, señalándose las sanciones imponibles de acuerdo a la gravedad de la comisión, por lo que es necesario tener el marco conceptual claro para poder tipificarlo.

Lo que resulta incuestionable es que tenemos que asumir y estar preparados para enfrentarnos en algún momento la posibilidad de ser víctimas de un delito informático dado el creciente aumento en nuestros días de este tipo de ilícitos penales en donde inclusive el autor lo realiza incluso sin ánimo de lucro sino por el contrario por mera inquietud "lúdica" o de juego.

En nuestra realidad se hace necesaria, como una forma de dar solución al problema, responder a la siguiente interrogante: ¿Cuál el factor decisivo que contribuye al mejoramiento de la labor de los operadores de justicia (Policías, Fiscales y Jueces) quienes actúan sobre los delitos informáticos en el Perú?

Considerando la pregunta expuesta, el objetivo general del presente estudio se plantea en los siguientes términos:

Determinar el factor decisivo que contribuye al mejoramiento de la labor de los operadores de justicia (Policías, Fiscales y Jueces) quienes actúan sobre los delitos informáticos en el Perú.

Respondiendo a la consulta de investigación, la presente tesis se orienta a la investigación y elaboración del marco conceptual actual de los delitos informáticos en el Perú, con la ayuda del método científico de recolección y

análisis de datos, para enmarcar la normatividad de los delitos cometidos a través del procesamiento de información por medios electrónicos.

Para dar cumplimiento a dicho objetivo se efectuaron, diseños de investigación no experimental, en donde los principales instrumentos de investigación utilizados son el estudio documental sobre el estado del arte de los delitos informáticos y la aplicación del Método Científico de la Investigación de los Delitos, obteniendo la opinión de expertos sobre la propuesta del nuevo marco teórico de los delitos informáticos en el Perú.

El trabajo consta de cinco capítulos:

El Capítulo I Marco Teórico. Trata de aspectos tales como el planteamiento del problema, importancia y justificación del estudio; además del desarrollo de enfoques conceptuales, doctrinarios y legales sobre los delitos informáticos y las teorías vinculadas con el tema.

El Capítulo II Metodología. En este capítulo se ha seguido aspectos metodológicos que se exigen en la comunidad científico-intelectual, desde los paradigmas del positivismo. La metodología utilizada, objetivos de estudio e hipótesis.

CAPÍTULO III: La nueva propuesta de un Marco Conceptual sobre Delitos Informáticos. Luego de tener en claro los objetivos, variables, método a trabajar y de los aportes de los expertos, se dan las bases para la elaboración y presentación del nuevo marco Conceptual de los Delitos Informáticos en el Perú.

CAPITULO IV Análisis. Este capítulo tiene por finalidad verificar, mediante herramientas de análisis el cumplimiento o no de los objetivos de investigación y probar la validez de la tesis

CAPITULO V: Conclusiones y Recomendaciones. Con la validación de la hipótesis de trabajo se pudo llegar a establecer siete conclusiones y cinco recomendaciones que se deja a consideración de la crítica objetiva de la comunidad científica y de los lectores en general.

Por último se adjuntan los instrumentos y las fuentes bibliográficas que fueron de utilidad para la elaboración de la tesis.

CAPÍTULO I:

MARCO TEORICO

1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, la informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática".

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, 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 materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse.

Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer nuevos delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

El estudio de los distintos métodos de destrucción y/o violación del hardware y el software es necesario en orden a determinar cuál será la dirección que deberá seguir la protección jurídica de los sistemas informáticos, ya que sólo conociendo el mecanismo de estos métodos es posible encontrar las similitudes y diferencias que existen entre ellos. De este modo se pueden conocer los problemas que es necesario soslayar para conseguir una protección jurídica.

En consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, en base a las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter

personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje.

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 esta 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.

Pero, el desarrollo de la tecnología viene acompañada casi siempre de dolores de cabeza por su equivocado uso, inclusive de carácter moral y ético lo ha sido así siempre desde la implementación de la primera "Computer Personal Unit" o CPU, hasta la sorprendente clonación, no había razón para que se escapara la computadora.

La preocupación ha llegado a los hombres de leyes sobre todo ante el uso abusivo que determinadas personas pueden hacer de la gran base

de datos a la que puedan acceder e incluso crear y cuyo control se escapa cada día que pasa de nuestras manos.

El uso frecuente de computadoras y de la posibilidad de su interconexión a nivel global da lugar a un verdadero fenómeno de nuevas dimensiones denominado: "El Delito Informático".

Los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar estas nuevas formas delictivas, tal como sucedería en el caso de interferencia en una red bancaria para obtener mediante una orden electrónica un libramiento ilegal de fondos o la destrucción de determinados antecedentes de crédito o la supresión de datos contables por ejemplo para citar algunos casos.

En el contexto peruano, es necesario señalar que la comisión de los delitos informáticos acarrean la criminalidad informática, debiéndose entender a ésta como los actos que vulneran la ley vigente, es decir que se tipifique el delito en el Código Penal Peruano, señalándose las sanciones imponibles de acuerdo a la gravedad de la comisión, la misma que no define el delito informático. [2]

Los Delitos Informáticos están tipificados en el Perú; asimismo existen normas que indirectamente sancionan las conductas en las que se intervenga con hardware o software, como por ejemplo, la Ley de Derechos de Autor, regulada por el Decreto Legislativo N° 822, el que sanciona a los que copien, usen o adquieran un programa sin permiso del autor, sin mencionar en ningún momento que esto sería un Delito Informático; en segundo lugar tenemos la Resolución Ministerial N° 622-96-MTC/15.17, con la que se aprueba la Directiva N° 002-96-MTC/15.17 referida a los Procedimientos de Inspección y de Requerimiento de

[2] LOS DELITOS INFORMATICOS EN EL PERU Carlos La Torre, Estudiante, Universidad de Lima, Perú. http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=30 . Fecha de consulta: abril 2005.

Información relacionados al Secreto de las Telecomunicaciones y Protección de Datos, ordenándose con ella a las empresas de Telecomunicaciones a mantener en secreto la información de sus abonados o usuarios, sancionándose a la empresa si la información es entregada o la obtienen terceros mas no así a estos terceros.

Es necesario, mencionar que ha habido recientemente un adelanto en nuestra legislación, en lo referente a la aplicación del software y hardware, específicamente en la legislación civil, la que desarrolla el embargo de bienes, la que dice que cuando se embarguen hardware, es decir computadoras, debe darse tiempo, en pleno embargo, al propietario para que retire la información contenida en el software, ya que se está embargando la computadora y no la información contenida en ella; como se aprecia se está diferenciando desde el punto de vista legal los términos informáticos de aplicación mundial.

En el Perú está tipificado como se mencionó antes los Delitos Informáticos mediante Ley 27309 publicado el 17 de Julio del 2000, el mismo que es analizado posteriormente, define y regula las penas para la comisión de los delitos informáticos.

El tema plantea complejas aristas para el derecho y para los hombres dedicados a la creación, interpretación y aplicación de las leyes pues parece no haber sido suficientemente considerado.

La presente Tesis se orienta a la investigación y análisis de los marcos conceptuales actuales de los delitos informáticos, desde el punto de vista peruano y mediante un método de recolección de datos legales y policiales que tiene la finalidad de enmarcar la normatividad de los delitos cometidos mediante el procesamiento de información por medios electrónico, se da de manera clara la falta de un marco conceptual de

los delitos informáticos para su legislación e interpretación así como para su correcta investigación.

El mundo globalizado hace que la normatividad sea clara y abierta para su correcta adecuación al fenómeno de los delitos informáticos que vienen utilizando tecnologías emergentes para este ilícito fin.

El Marco conceptual mediante los canales correspondientes se hará llegar una copia al Poder Legislativo tendrá que ser analizado por un equipo multidisciplinario para que sirva para la elaboración de una ley marco de acuerdo al uso de tecnología actual para dar solución a este problema.

1.1. Formulación del problema

Al plantear la problemática de la investigación, se ha generado la imperiosa necesidad de realizar un estudio que se analice sistemáticamente lo siguiente:

¿Cuál es el factor decisivo que contribuye al mejoramiento de la labor de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en el Perú?

1.2. Sistematización del problema

1.2.1. ¿Qué son los delitos informáticos en el Perú?

1.2.2. ¿Cuál es la función de cada uno de los operadores de justicia de los delitos informáticos (Policías, Fiscales y Jueces)?

1.2.3. ¿Cuál es el estado del arte de la investigación de los delitos informáticos?

1.2.4. ¿Qué alternativa viable contribuye a dar solución al problema planteado?

1.3. Objetivos de la investigación

1.3.1. Objetivo General

Determinar el factor decisivo que contribuye al mejoramiento de la labor de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en el Perú.

1.3.2. Objetivos Específicos

1.3.2.1. Identificar y describir los delitos informáticos que se producen en el Perú.

1.3.2.2. Explicar el estado del arte de la investigación de los delitos informáticos.

1.3.2.3. Elaborar un nuevo marco conceptual de los delitos informáticos en el Perú que contribuya a solucionar el problema planteado en la tesis.

2. IMPORTANCIA Y JUSTIFICACIÓN

2.1. Importancia

El análisis del Nuevo Marco conceptual de los Delitos Informáticos se aproxima a una elaboración de un nuevo Marco Teórico para que pueda ser utilizado por los operadores de justicia que actúan sobre los delitos informáticos (Policías, Fiscales y Jueces). Además, el tema de tesis ha sido poco tratado por otros investigadores.

2.2. Justificación

El presente estudio determina el factor decisivo que contribuye al mejoramiento de la labor de los operadores de justicia (Policías, Fiscales y Jueces) de los delitos informáticos, lo cual posibilitará mejorar el tratamiento de la problemática en el Perú.

Las escasas investigaciones que se realizaron en los niveles académicos están referidas sólo a estudios superficiales y descriptivos sobre el tema.

Lo que se busca es plantear alternativas de solución al problema de conceptualización e identificación. Y por último, al concluir con la investigación se está en condiciones de hacer las recomendaciones tendientes a seguir adecuando el marco teórico de acuerdo a los cambios de modalidades de los delitos informáticos.

3. LOS DELITOS INFORMATICOS

3.1. Definición

La palabra "**delito**", deriva del vocablo delictum del verbo delinquere, a su vez compuesto de linquere, dejar y el prefijo de. En la connotación peyorativa, se toma como linquere viam o rectam viam: dejar o abandonar el buen camino".

Para Ignacio Villalobos (1975)[3], el Delito "es un acto humano típicamente antijurídico y culpable".

[3] DERECHO PENAL MEXICANO. Villalobos, Ignacio. Editorial Porrúa, S.A. México 1975. pp. 650.

Según el artículo 11° del Código Penal Peruano dice que "Son delitos y faltas las acciones u omisiones dolosas o culposas penadas por la ley".

Esta noción de delito es especialmente formal, y no define cuáles sean sus elementos integrantes. Sus elementos integrantes son:

- El delito es un acto humano, es una acción (acción u omisión).
- Dicho acto humano ha de ser antijurídico, ha de estar en oposición con una norma jurídica, debe lesionar o poner en peligro un interés jurídicamente protegido.
- Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.
- El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

Como se puede observar de las definiciones anteriormente citadas, se hace abstracción de la imputabilidad, ya que ésta implica la capacidad de ser sujeto activo del delito, o sea, no es un comportamiento propio del delito. La imputabilidad no es mencionada, por tratarse de una referencia al delincuente, no al delito. La imputabilidad como concepto penal se reduce a la capacidad de ser activo del delito, con dos referencias: a) un dato de orden objetivo, constituido por la mayoría de edad dentro del derecho penal, que puede o no coincidir con la mayoría de edad civil o política y; b) un dato de orden subjetivo, el que expresado en sentido llano se reduce a la normalidad mental, normalidad que comprende la capacidad de querer y comprender "el significado de la acción".

Para Blossiers-Calderón (2000) "**La informática** es la ciencia tanto teórica como práctica en el tratamiento de la información. Nos permite elaborar, conservar y recuperar la información en forma significativa.

La informática permite manejar gran volumen de información procesando en forma rápida aquello que es repetitivo, simplificando el trabajo del hombre; se le puede dar el concepto según la comunidad de lenguajes de programación (2004)[4] como la ciencia que estudia los ordenadores.

El concepto de informática viene dado de la unión de dos palabras Información y automática.

En inglés se habla de conceptos tales como Computer Science, Electronic Data Processing, etc.

"Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".

Concepto de informática según el diccionario académico de la lengua española: Podemos entender el concepto de informática como aquella ciencia encargada de estudiar los ordenadores y su capacidad para procesar y almacenar información y datos.

En sus inicios, la informática facilitó los trabajos repetitivos y monótonos del área administrativa, gracias a la automatización de esos procesos, lo que a su vez trajo como ventaja una disminución de los costos.

[4] http://lenguajes-de-programacion.com/concepto-de-informatica.shtml. Fecha de consulta: 05 de Julio 2005

Dentro del concepto de informática, su principal función es facilitar información oportuna y veraz, lo cual facilita la toma de decisiones a nivel empresarial.

El delito Informático implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional tales como: robo, hurto, fraude, falsificaciones, 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.

En la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe una concepto propio de los llamados delitos informáticos; pero ya son muchos los autores que manifiestan su opinión a favor de la existencia del delito informático.

El destacado doctrinario en la materia, el doctor Julio Téllez Valdez, conceptualiza al delito informático en forma típica y atípica, entendiendo a la primera como a "las conductas típicas, antijurídicas y culpables, en las que se tienen a las computadoras como instrumento o fin" y a las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". VIII Congreso Iberoamericano de Derecho e Informática, Cancún y Distrito Federal, México, Noviembre 2000. [5]

[5] Soto, Alberto "Argentina: Delitos Informáticos" Alfa-Redi org-Revista de derecho informático. http://www.alfa-redi.org/revista/data/52-3.asp 10 de abril del 2005.

Por otra parte, Nidia Callegari (1985)[6] define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

El italiano Carlos Sarzana (2001)[7] lo determina como "cualquier comportamiento criminógeno en el que la computadora está involucrada como material, objeto o mero símbolo". De otro lado, Rafael Fernández Calvo (España) lo describe como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando el elemento informático o telemático contra los derechos y libertades de los ciudadanos".

Julio Núñez (2005) sostiene que los Delitos informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático. Para este autor 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.[8]

Asimismo, el Departamento de Investigación de la Universidad de México califica de delitos informáticos a "todas aquellas conductas ilícitas, susceptibles de ser sancionadas por el

[6] Callegari, Nidia. Delitos Informáticos y Legislación en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 Jul-Sep 1985. P.115.
[7] SARZANA, Carlos. "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Roma, Italia. P.53.
[8] Julio Núñez Perú: Los Delitos Informáticos Alfa - Redi: Revista de Derecho Informático Martes, 15 Marzo del 2005 ISSN 1681-5726 http://www.alfa-redi.org/revista/data/17-2.asp (2004)

Derecho Penal, que hacen uso indebido de cualquier medio informático". [9]

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

Así, en la actualidad, el "arma del crimen" pasa a ser una serie de bytes, y los delitos se pueden cometer por control remoto desde cientos o miles de kilómetros, a lo que habría que añadir que en este tipo de crímenes las pruebas se han visto desvirtuadas por la naturaleza de la comunicación[10]

3.2. Definición de la ONU

La ONU sostiene que "la delincuencia informática es difícil de comprender o conceptualizar plenamente. A menudo, se la considera una conducta proscrita por la legislación y/o la jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito; se dirige a las propias tecnologías de la computación y las comunicaciones; o incluye la utilización incidental de computadoras en la comisión de otros delitos".

La ONU expresa que "por delito cibernético se entiende todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos. En principio, el concepto abarca

[9] Müller Hugo. "Los Delitos Informáticos en el Código Penal Peruano" Revista Nº 36 de la PNP Pp. 5 Perú http://www.pnp.gob.pe/culturales/revista_81/pag_36_40.pdf (2004)
[10] Prevención y detección de delitos informáticos - Debra Littlejohn Shinder -Ed. Anaya Multimedia -1ª edición - Mayo 2003

todo delito que puede cometerse en un medio electrónico. En este marco, la palabra delitos denota formas de comportamiento generalmente definidas como ilegales o que probablemente serán declaradas ilegales en breve plazo".

Entre las especificaciones que plantea la ONU aparecen dos subcategorías de delitos informáticos:

a. El delito cibernético en sentido estricto, o delito informático, que contempla todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y los datos procesados por ellos, y

b. Delito cibernético en sentido extenso (delito relacionado con computadoras), que incluye todo comportamiento ilícito realizado por medio de un sistema o una red informáticos o en relación con ellos, incluidos los delitos como la posesión, el ofrecimiento o distribución ilegales de información por medio de un sistema o una red informáticos.

Veamos algunas cuestiones puntuales. La posesión, ofrecimiento o distribución ilegal de información incluiría seguramente la copia ilegal de contenidos amparados ya por leyes de copyright, lo cual está contemplado en otras normas jurídicas, por lo que no es necesario trabajar sobre eso. Lo mismo ocurre con los "datos personales", que se encuentran amparados bajo las leyes de habeas data.

Mientras que por el lado del delito cibernético en sentido estricto, la dificultad aparece claramente cuando el informe de

ONU comienza a explicar de qué se trata esto diciendo por ejemplo que se debe tipificar como delito el "acceso no autorizado, a veces denominado piratería informática", cuando es públicamente conocido que cualquier administrador de redes puede estar en la franja límite de este delito mientras está probando la seguridad de las mismas. Por otro lado, el uso de la palabra "pirata" en un documento de este tenor muestra un nivel de exageración extraordinario al comparar este tipo de acciones con la piratería, que según el diccionario es un acto de vandalismo por parte de piratas, un ladrón que recorre los mares para robar. No se puede tipificar en estos casos lo que se denomina "piratería" como robo, ya que en ninguno de estos casos que se mencionan como "piratería", las personas se "apropian de bienes ajenos" por lo mismo que el documento señala en su comienzo: "los datos como tales sólo pueden controlarse mediante operaciones lógicas y no mediante actos físicos, por lo que resulta difícil tratarlos en estado puro, en el ámbito legal, como si fueran objetos tangibles."

Así, el tema de los ciberdelitos y el ciberterrorismo es particularmente compleja y provoca fuertes discusiones sobre la tipificación de nuevos delitos que no necesariamente son nuevos, sino que son los mismos delitos ya tipificados pero ejecutados a través de medios innovadores. Toda discusión en este sentido debería enmarcarse en reales mecanismos de control de quienes tendrían capacidad de ejercer vigilancia y considerar como fundamento de toda nueva normativa la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y el Pacto Internacional de Derechos Civiles y Políticos.[11]

[11] Bestiario de la Sociedad de la información. Beatriz Busaniche. D-Sur Periodismo libre digital Uruguay http://www.d-sur.net/bbusaniche/index.php?p=23 Fecha de consulta: noviembre 2004.

3.3. Características

De acuerdo con lo enunciado por el Dr. Julio Téllez Valdez[12] en su libro intitulado "Derecho Informático" podemos destacar las siguientes características:

a. Son conductas criminógenas de cuello blanco, en tanto que solo un determinado número de personas, con conocimientos profesionales o técnicos, pueden llegar a cometerlas.

b. Son acciones ocupacionales, ya que generalmente se ejecutan cuando el sujeto se encuentra en pleno trabajo.

c. Son acciones de oportunidad, en cuanto se aprovecha la ocasión presentada.

d. Provocan serias pérdidas económicas, ya que casi siempre producen grandes beneficios a quienes los realizan.

e. Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundos y sin una necesaria presencia física del ejecutante pueden llegar a consumarse.

f. Son muchos los casos y pocas las denuncias debido a la falta o escasa regulación por parte del Derecho y prestigio de la empresa agraviada.

---

[12] Julio Téllez Valdés "Derecho Informático", Editorial Mc Graw Hill. México. 1996.

g. Debido a su carácter técnico presentan grandes dificultades para su comprobación.

De acuerdo a lo investigado, se pueden agregar:

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

b. Ofrecen facilidades para su comisión a los menores de edad.

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

d. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Por lo anterior, se puede apreciar que los que cometen este tipo de ilícitos, son personas con conocimientos sobre la informática y cibernética, los cuales, se encuentran en lugares estratégicos o con facilidad para poder acceder a información de carácter delicado, como puede ser a instituciones crediticias o del gobierno, empresas o personas en lo particular, dañando en la mayoría de los casos el patrimonio de la víctima, la cual, por la falta de una ley aplicable al caso concreto, no es denunciada quedando impune estos tipos de conductas antisociales; siendo esto alarmante, pues como se mencionó en líneas precedentes este tipo de acciones tienden a aumentar y ser más comunes, por lo que se pretende en la presente investigación, es crear una conciencia sobre la necesidad urgente de regular estas conductas, ya que debe ser legislado de una manera seria y honesta, recurriendo a las

diferentes personalidades del conocimiento, tanto técnico en materia de computación, como en lo legal, ya que si no se conoce de la materia, difícilmente se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular

3.4. Clasificación

Para María de la Luz Lima (1984)[13], en su trabajo sobre "Delitos Electrónicos" los clasifica en tres categorías, a saber:

a. Los que utilizan la tecnología electrónica como método
b. Los que utilizan la tecnología electrónica como medio y;
c. Los que utilizan la tecnología electrónica como fin.

Como método, los individuos utilizan métodos electrónicos para llegar a un resultado ilícito. Como medio, son aquellas conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo. Y Como fin, son las dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla

La mayoría de los estudiosos en la materia clasifican a este tipo de acciones de dos formas, como instrumento o medio y como fin u objeto. Aún así autores como el tratadista penal italiano Carlos Sarzana mencionan que estos ilícitos pueden clasificarse en atención a que producen un provecho para el autor y provocan un daño contra la computadora como entidad física y que procuren un daño a un individuo o grupos, en su integridad física, honor o patrimonio.

[13] LIMA DE LA LUZ, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984. Pp.100.

Julio Téllez Valdés (1996)[14], clasifica a los delitos informáticos:

a. **Como Instrumento o medio**, dichas conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito; por ejemplo, la falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera), la variación de los activos y pasivos en la situación contable de las empresas, la planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera), el "robo" de tiempo de computadora, la lectura, sustracción o copiado de información confidencial, el aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas, la alteración en el funcionamiento de los sistemas (virus informáticos) y el acceso a áreas informatizadas en forma no autorizadas entre muchas más.

b. **Como Fin y Objeto**. En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física, los cuales pueden ser la programación de instrucciones que producen un bloqueo total al sistema, la destrucción de programas por cualquier método, el daño a la memoria, o el atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).

3.5. Tipos de Delitos Informáticos reconocidos por las Naciones Unidas[15]

[14] DERECHO INFORMATICO. Téllez Valdés Julio.Edt. Mc Graw Hill. México, Segunda Edición 1996.pp.283.
[15] http://delitosinformaticos.com/delitos/delitosinformaticos2.shtml Consulta Junio 2005

Existen tres tipos de delitos informáticos reconocidos por las Naciones Unidas, reseñados en la Figura N° 1:

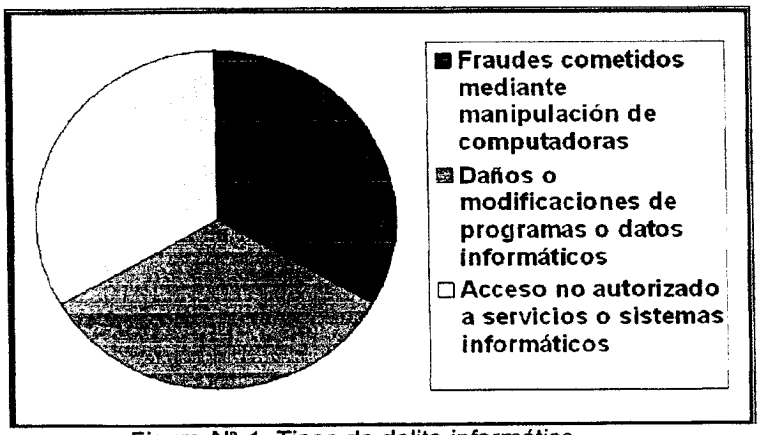


Figura N° 1. Tipos de delito informático

Sus variantes y cuáles son los tipos de fraudes más comunes cometidos mediante manipulación de computadoras:

Tipos de Delitos Informáticos Conocidos por Naciones Unidas	
Delitos	***Características***
Fraudes cometidos mediante manipulación de computadoras	
Manipulación de los datos de entrada	Este tipo de fraude informático conocido también como sustracción de datos, representa el delito Informático mas común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
La manipulación de programas	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya,

	que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
Manipulación de los datos de salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo mas común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
Fraude efectuado por manipulación informática	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.
Falsificaciones Informáticas	
Como Objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada
Como instrumentos	Las computadoras pueden utilizarse también pare efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas; pueden hacer copias de alta resolución, modificar documentos e incluso crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas o datos computarizados	
Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legitima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco pare que transfiera continuamente dinero a una cuenta ilícita.
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en

	donde se halla la bomba.
Acceso no autorizado a Sistemas o Servicios	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático.
Piratas informáticos o Hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
Reproducción no autorizada de programas informáticos de protección Legal.	Esta puede entrañar una perdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

4. ESTADO DEL ARTE DE LA INVESTIGACIÓN SOBRE LOS DELITOS INFORMATICOS

Luego de hacer una exhaustiva revisión bibliográfica sobre el tema de los delitos informáticos se mencionan los trabajos realizados por los investigadores: Melvin Leonardo Landaverde Contreras, Joaquín Galileo

Soto Campos y Jorge Marcelo Torres Lipe, de la Universidad de El Salvador (Octubre de 2000), quienes llegaron a concluir que:

- "Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

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

- Nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

- La responsabilidad del auditor informático no abarca el dar solución al impacto de los delitos o en implementar cambios; sino más bien su responsabilidad recae en la verificación de controles, evaluación de riesgos, así como en el establecimiento de recomendaciones que ayuden a las organizaciones a minimizar las amenazas que presentan los delitos informáticos.

- La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información (comunicación remota, Interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

- El Instituto Nacional de Estadística e Informática (INEI-2001), órgano rector de los Sistemas Nacionales de Estadística e Informática peruano, publico el documento "DELITOS INFORMATICOS", en el marco de la colección "Seguridad de Información".

- Dicha publicación registra en ocho capítulos, la evolución histórica de los delitos informáticos, los casos mas sonados de crímenes utilizando la computadora.

- Presenta además, los usos de las nuevas tecnologías, riesgos y oportunidades, que surgen del comercio electrónico, como: delitos en Internet, responsabilidad del proveedor, medios de prevención y control en Internet y los conflictos jurisdiccionales.

En relación a los Delitos Informáticos, se precisan los conceptos de fraude y delito, se estudia la diversa terminología asociada a los delitos informáticos, se presenta las peculiaridades de la criminalidad informática. También describe al tipo de delincuente informático y los tipos de delitos reconocidos por las Naciones Unidas, así como la estrategia internacional de represión.

Es importante destacar el estudio del impacto económico y social de los delitos informáticos, las acciones de prevención, así como las políticas y

medidas de seguridad de información, que incluyen las acciones antes y después de una intromisión y la auditoria de la seguridad informática.

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

MailxMail.com[16] al ofrecer un curso gratuito sobre delitos informáticos por Internet pone a disposición de sus alumnos un Manual sobre delitos informáticos .En dicho manual se concluye que:

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

- Nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

[16] MailxMail.com es una iniciativa de "Open E-learning", consistente en ofrecer formación gratuita por Internet. Ver en: http://www.mailxmail.com Fecha consulta: enero – abril 2005

- La responsabilidad del auditor informático no abarca el dar solución al impacto de los delitos o en implementar cambios; sino más bien su responsabilidad recae en la verificación de controles, evaluación de riesgos, así como en el establecimiento de recomendaciones que ayuden a las organizaciones a minimizar las amenazas que presentan los delitos informáticos.

- La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información (comunicación remota, Interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

Miguel Estrada en su libro "Delitos Informáticos"[17] sostiene que: "Para concluir con esta aproximación a un tema de gran interés y de preocupación, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (microprocesadores, inteligencia artificial, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

[17] Ver en: http://www.universidadabierta.edu.mx/Biblio/E/Estrada%20Miguel-Delitos%20informaticos.htm

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

Finalmente, debe destacarse el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas".

5. MARCO LEGAL

5.1. Principales legislaciones de los delitos informáticos en el mundo

5.1.1. **ALEMANIA.** Para hacer frente a la delincuencia relacionado con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

1. Espionaje de datos. 2.- Estafa Informática. 3.- Falsificación de datos probatorios. 4.- Alteración de Datos. 5.- Sabotaje Informático. 6.- Utilización abusiva de cheques o tarjetas de crédito.

Cabe mencionar que esta solución fue también adoptada en los Países Escandinavos y en Austria.

Alemania también cuenta con una Ley de Protección de Datos, promulgada el 27 de enero de 1977, en la cual, en su numeral primero menciona que "el cometido de la protección

de datos es evitar el detrimento de los intereses dignos de protección de los afectados, mediante la protección de los datos personales contra el abuso producido con ocasión del almacenamiento, comunicación, modificación y cancelación (proceso) de tales datos. La presente ley protege los datos personales que fueren almacenados en registros informatizados, modificados, cancelados o comunidades a partir de registros informatizados".

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos.

5.1.2. **AUSTRIA**. Ley de reforma del Código Penal del 22 de diciembre de 1987, la cual contempla los siguientes delitos:

1. Destrucción de Datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

2. Estafa Informática. (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.

5.1.3. **CHILE**. Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona: Artículo 1° "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo". Artículo 2° " El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio". Artículo 3°" El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado". Artículo 4° " El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

5.1.4. **ESTADOS UNIDOS**. Cabe mencionar, la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030). Que modificó al Acta de Fraude y Abuso Computacional de 1986. Dicha acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo

transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año de prisión.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos; específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen.

Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple que se debe entender como acto delictivo.

Es interesante también señalar que el Estado de California, en 1992 adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta ley de 1994.

5.1.5. **FRANCIA**. Las disposiciones penales están contempladas en sus numerales del 41 al 44, los cuales contemplan lo siguiente: Artículo 41"

El que hubiere procedido o mandado proceder a la realización de tratamientos automatizados de información nominativa sin que hubieran sido publicados los actos reglamentarios previstos en el artículo 15 o formuladas las denuncias previstas en el artículo 16, supra, será castigado con pena de privación de libertad de seis meses a tres años y con pena de multa de 2 000 a 200 000 francos, o con una sola de estas dos penas. Asimismo, el tribunal podrá ordenar

la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos, en las condiciones que determinare y a expensas del condenado".

Artículo 42" El que hubiere registrado o mandado registrar, conservando o mandando conservar informaciones nominativas con infracción de las disposiciones de los artículos 25, 26 y 28, será castigado con pena de privación de libertad de uno a cinco años y con pena de multa de 20 000 a 2000 000 francos, o con una de estas dos penas.

Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos en las condiciones que determine, y a expensas del condenado.

Artículo 43. "El que habiendo reunido, con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento, informaciones nominativas cuya divulgación tuviere como efecto atentar contra la reputación o la consideración de la persona o la intimidad de la vida privada; hubiere, sin autorización del interesado y a sabiendas, puesto tales informaciones en conocimiento de una persona que no estuviere habilitada para recibirlas a tenor de las disposiciones de la presente ley o de otras disposiciones legales, será castigado con pena de privación de libertad de dos a seis meses y con pena de multa de 2000 a 20000 francos, o con una de las dos penas.

El que por imprudencia o negligencia, hubiere divulgado o permitido divulgar informaciones de la índole de las que se mencionan en le párrafo anterior, será castigado con pena de multa de 2000 a 20000 francos. Artículo 44 "El que, disponiendo de informaciones nominativas con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento las hubiere desviado de su finalidad, según la misma hubiera sido definida, bien en el acto reglamentario previsto en el artículo 15, supra, o en las denuncias formuladas en aplicación de los artículos 16 y 17, bien en una disposición legal, será castigado con pena de privación de libertad de uno a cinco años y con multa de 20 000 a 2000 000 francos".

5.2. Los delitos informáticos en el Código Penal peruano

Hasta antes de la promulgación de la mencionada ley, el Código Penal Peruano hacía alusión a una modalidad de hurto agravado, tipificado en el Artículo 186, que podía catalogarse como una figura de delito informático, configurado cuando el hurto se cometía mediante la utilización de sistemas de transferencia electrónica de fondos; de la telemática, en general; o, se violaban claves secretas.

El Código Penal Peruano, al incorporar la figura del delito informático, no establece una definición genérica del mismo.

CODIGO PENAL PERUANO

Ley 27309 del 26 de junio del 2000

CAPÍTULO X - DELITOS INFORMÁTICOS

Artículo 207-A.- Delito Informático

El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Artículo 207-B.- Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras

El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

Hasta aquí podemos comentar que la ley que incorpora los delitos informáticos al Código Penal Peruano ha considerado únicamente dos tipos genéricos, de los que se desprende una serie de modalidades. Para ello, el legislador se ha basado en el criterio del uso de la computadora como instrumento o medio y en el de su utilización como fin u objetivo.

El primer tipo genérico lo encontramos en el Art. 207.o-A, que describe una conducta criminógena que se vale de la computadora para la comisión del ilícito penal.

Un ejemplo de ello lo constituyen los fraudes cometidos en perjuicio de las instituciones bancarias o de cualquier empresa por personal del área de sistemas que tiene acceso a los tipos de registros y programas utilizados. También se encuadra el fraude efectuado por manipulación informática, es decir, cuando se accede a los programas establecidos en un sistema de información y se les manipula para obtener una ganancia monetaria.

Otras modalidades son la falsificación informática, que consiste en la manipulación de la información arrojada por una operación de consulta en una base de datos; el acceso no autorizado a sistemas o servicios; la reproducción no autorizada de programas informáticos de protección legal, conocida como piratería; entre otras.

El segundo tipo genérico lo encontramos en el Art. 207.o-B, donde se enmarcan las conductas criminógenas dirigidas a la utilización, interferencia o ingreso indebido a una base de datos con el fin de alterarla, dañarla o destruirla.

Artículo 207-C.- Delito informático agravado

En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.

2. El agente pone en peligro la seguridad nacional.

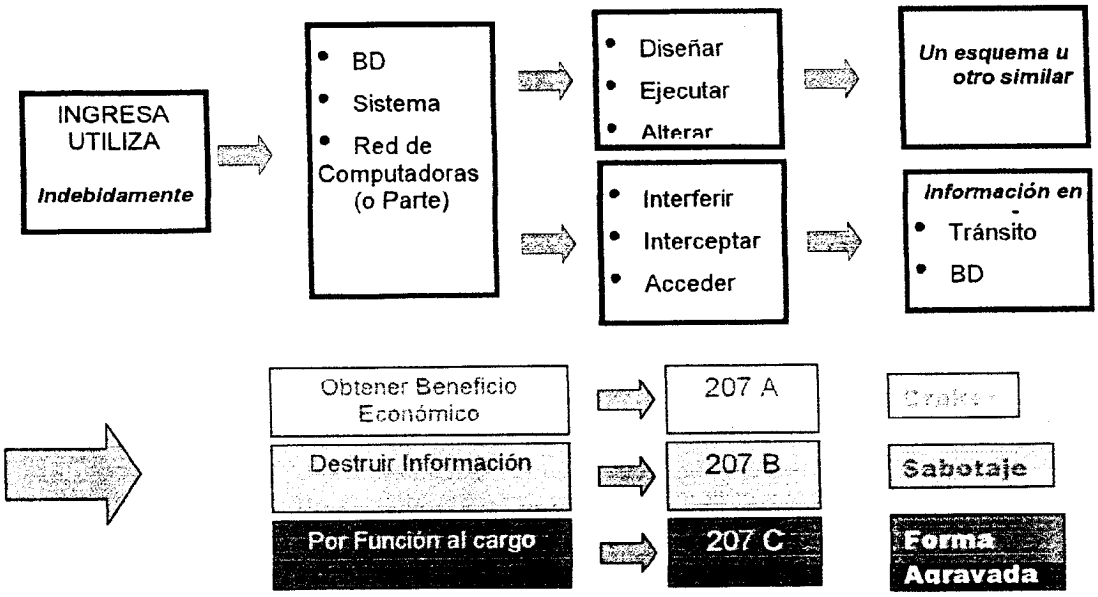


Fig.2 Esquematización de los Delitos Informáticos[18]

5.3. Delitos conexos a los delitos informáticos en el Perú

El INEI (2001)[19] manifiesta que "en el ordenamiento jurídico peruano, se tipifican los siguientes delitos que tienen aplicación directa en el campo informático, y que se considera que están dentro del concepto general de los delitos informáticos:

[18] Luis Romero y otros – Curso de Investigación de Delitos Informáticos – Dirección de Investigación Criminal PNP 2003. Lima Perú.
[19] INEI. "Delitos Informáticos". Colección Seguridad de la Información. Perú 2001. Pp.127

5.3.1. Delito de Violación a la Intimidad.

En nuestro Código Penal está tipificado en el artículo 154 el Delito de violación a la intimidad, y establece que: "el que viola la intimidad de la vida personal y familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios será reprimido con pena privativa de libertad no mayor de dos años. La pena será no menor de uno ni mayor de tres y de treinta a ciento veinte días cuando el agente revela la intimidad conocida de la manera antes prevista".

El artículo 157 del Código Penal precisa que "el que indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida intima de una o más personas será reprimido con pena privativa de libertad no menor de un año ni mayor de cuatro años. Si el agente es funcionario o servidor público y comete delito en ejercicio del cargo, la pena será no menor de tres años ni mayo de seis e inhabilitación". La base de datos computarizados consideramos que están dentro del precepto de "cualquier archivo que tenga datos", en consecuencia está tipificado el delito de violación a la intimidad utilizando la informática y la telemática a través del archivo, sistematización y transmisión de archivos que contengan datos privados que sean divulgados sin consentimiento.

5.3.2. Delito de Hurto agravado por Transferencia Electrónica de Fondos, telemática en general y empleo de claves secretas.

El artículo 185 del Código Penal establece que aquella persona que "... para obtener provecho, se apodera ilegítimamente de un bien total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equipara a bien mueble la energía eléctrica, el gas, el agua y cualquier otro elemento que tenga valor económico, así como el espectro electromagnético".

El artículo 186 del Código Penal , segundo párrafo numeral 3 - modificado por la ley 26319- dispone además "la pena será no menor de cuatro años ni mayor de ocho si el hurto es cometido mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas". El delito de hurto agravado por transferencia electrónica de fondos tiene directa importancia en la actividad informática.

El sistema de transferencia de fondos, en su conjunto, se refiere a la totalidad de las instituciones y prácticas bancarias que permiten y facilitan las transferencias interbancarias de fondos. El desarrollo de medios eficientes de transmisión de computadora a computadora de las órdenes de transferencia de fondos ha fortalecido el sistema. Los niveles de calidad y seguridad de las transferencias interbancarias de fondos se han ido acrecentando conforme el avance de la tecnología, no obstante la vulnerabilidad a un acceso indebido es una "posibilidad latente" por tanto

además de los sistemas de seguridad de hardware , software y comunicaciones ha sido necesario que la norma penal tenga tipificada esta conducta criminal.

Uno de los medios de transferencia electrónica de fondos se refiere a colocar sumas de dinero de una cuenta a otra, ya sea dentro de la misma entidad financiera o una cuenta en otra entidad de otro tipo, ya sea pública o privada. Con la frase "telemática en general" se incluye todas aquellas transferencias u operaciones cuantificables en dinero que pueden realizarse en la red informática ya sea con el uso de Internet, por ejemplo en el Comercio Electrónico o por otro medio. Cuando se refiere a "empleo de claves secretas" se está incluyendo la vulneración de password, de niveles de seguridad, de códigos o claves secretas.

5.3.3. Delito de Falsificación de Documentos Informáticos.

El Decreto Legislativo 681 modificado por la Ley 26612, es la norma que regula el valor probatorio del documento informático, incluyendo en los conceptos de microforma y microduplicado tanto al microfilm como al documento informático. El artículo 19 de esta norma establece que: "la falsificación y adulteración de microformas, microduplicados y microcopias sea durante el proceso de grabación o en cualquier otro momento, se reprime como delito contra la fe pública, conforme las normas pertinentes del Código Penal".

Las microformas que cumplidos los requisitos técnicos (equipos y software certificados que garantizan inalterabilidad, fijeza, durabilidad, fidelidad e integridad de documentos micrograbados) y formales (que procesos de

micrograbación sean autenticados por un depositario de la fe pública, por ejemplo el fedatario juramentado en informática) sustituyen a los documentos originales para todos los efectos legales.

En el Código Penal Peruano entre los delitos contra la fe pública, que son aplicables a la falsificación y adulteración de microformas digitales tenemos los siguientes:

i) Falsificación de documentos. "El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de dos ni mayor de diez años..." (Artículo 427 del CPP.). Tratándose de microformas digitales su falsificación y/o adulteración son sancionados con la misma pena.

ii) Falsedad ideológica "El que inserta o hace insertar , en instrumento público , declaraciones falsas concernientes a hechos que deben probarse con el documento, con el propósito de emplearlo como si la declaración fuera conforme a la verdad, será reprimido si de uso puede resultar algún perjuicio , con pena privativa de libertad no menor de tres ni mayor de seis años.." (Artículo 428 del C.P.). Hay que tener en cuenta que la microforma digital de un documento público tiene su mismo valor, por tanto puede darse el caso de falsedad ideológica de instrumentos públicos contenidos en microformas digitales.

iii) Omisión de declaración que debe constar en el documento. "El que omite en un documento público o privado declaraciones que deberían constar o expide duplicados con igual omisión al tiempo de ejercer una función y con el fin de dar origen a un hecho u obligación , será reprimido con pena privativa de libertad no menor de uno ni mayor de seis" (Artículo 429 del C.P.). Para que tenga valor probatorio y efecto legal una microforma digital tiene que cumplir requisitos formales y técnicos. El requisito formal consiste en que debe ser autenticado por depositario de la fe pública (fedatario juramentado o notario) el proceso técnico de micrograbación y que las copias de esos documentos deben ser certificados, por lo cual una omisión de las declaraciones que por ley deben incluirse podría configurar esta figura delictiva.

5.3.4. Delito de Fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos.

Puesto que en el patrimonio de la persona están incluidos tanto bienes materiales (hardware) como inmateriales (software, información, base de datos, etc.) esta figura delictiva puede aplicarse al campo informático según interpretación del artículo 198° inciso 8 del Código Penal, establece que : "será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años el que, en su condición de fundador, miembro del directorio o del consejo de administración o del consejo de vigilancia, gerente, administrador o liquidador de una persona jurídica, realiza, en perjuicio de ella o de terceros, cualquiera de los actos siguientes: Usar en provecho propio o de otro, el patrimonio de la persona (inciso 8). Esta figura podría aplicarse, en este

orden de ideas, tanto al uso indebido de software, información, datos informáticos, hadware u otros bienes que se incluyan en el patrimonio de la persona jurídica.

5.3.5. Delito contra los derechos de autor de software.

Con respecto a los delitos contra los derechos de autor de software, debe tenerse en cuenta que "...sobre la naturaleza jurídica y la tutela que apunta el derecho de autor sobre el software hay acuerdo general. Y no puede ser de otro modo, debido a la trascendencia que tiene, dado que la transgresión de índole penal ala actividad intelectual constituye no sólo una agresión a la propiedad del autor y afecta los intereses de la cultura, sino que conforma también un ataque al derecho moral sobre la paternidad de la obra".

Con la dación del Decreto Legislativo 822, se modificó el Código Penal y se han aumentado las penas, con respecto a la legislación peruana anterior, así tenemos:

i) Que el artículo 217° del Código Penal Peruano establece que "será reprimido con pena privativa de libertad no menor de dos ni mayor de seis años y con treinta a noventa días-multa, el que con respecto a una obra,...o una grabación audiovisual o una imagen fotográfica expresada en cualquier forma, realiza cualquiera de los siguientes actos, sin la autorización previa y escrita de autor o titular de los derechos.

a) la modifique total o parcialmente.

b) La reproduzca total o parcialmente, por cualquier medio o procedimiento.

c) La distribuya mediante venta, alquiler o préstamo público.

d) La comunique o difunda públicamente por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.

e) La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.

Aquí se están garantizando bajo la protección los derechos patrimoniales; en los contratos de licencia de uso de software se contemplan el respeto de estos derechos y también en la Ley de Derecho de Autor que anteriormente hemos tratado. La autorización previa y escrita del titular, generalmente en la activad empresarial se instrumenta en una licencia de uso de software.

ii) Que el Artículo 218° del Código Penal Peruano dispone que "la pena será privativa de libertad no menor de dos ni mayor de ocho años y sesenta a ciento veinte días-multa cuando:

a) Se de a conocer a cualquier persona una obra inédita o no divulgada, que haya recibido en confianza del titular del derecho de autor o de alguien en su nombre, sin el consentimiento del titular.

b) La reproducción, distribución o comunicación pública se realiza con fines de comercialización, o alterando o

suprimiendo, el nombre o seudónimo del autor, productor o titular de los derechos.

c) Conociendo el origen ilícito de la copia o reproducción, la distribuya al público, por cualquier medio, la almacene, oculte, introduzca al país o la saca de éste.

d) Se ponga de cualquier otra manera en circulación dispositivos, sistemas, esquemas o equipos capaces de soslayar otro dispositivo destinado a impedir o restringir la realización de copias de obras, o a menoscabar la calidad de las copias realizadas; o capaces de permitir o fomentar la recepción de un programa codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no estén autorizados para ello.

e) Se inscriba en el Registro del Derecho de Autor la obra,... como si fuera propia, o como de persona distinta del verdadero titular de los derechos.

Los supuestos tratados en este artículo se refieren tanto a derecho morales como patrimoniales, que por su gravedad (atentar contra el derecho de paternidad, comercializar o distribuir copias ilegales, registrar en forma indebida el software) se amplía la pena hasta ocho años. En la anterior legislación la pena mayor por este tipo de delitos era de cuatro años, actualmente se ha aumentado a ochos años. Estos tipos penales, parten del supuesto que no hay consentimiento o autorización del titular de los derechos para ello; de existir una licencia de uso y cumplirse con sus términos y condiciones, no se tipificaría este delito.

iii) Que el Artículo 219° del Código Penal Peruano, establece que: "será reprimido con pena privativa de libertad no menor de dos ni mayor de ocho años y sesenta a ciento ochenta días-multa, el que con respecto a una obra, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena".

La apropiación de autoría ajena, de reputarse una obra que no es de uno como propia, también se aplica la software, más aún con las opciones tecnológicas para su copia, que incluyen equipos de cómputo, cada vez más sofisticados y el uso de herramientas en Internet.

iv) Que el Artículo 220° del Código Penal Peruano, dispone que: " será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a trescientos sesentaicinco días-multa:

a) Quien se atribuya falsamente la calidad de titular originario o derivado, de cualquiera de los derechos protegidos en la legislación del derecho de autor y derechos conexos y, con esa indebida atribución, obtenga que la autoridad competente suspenda el acto de comunicación, reproducción o distribución de la obra, interpretación, producción, emisión o de cualquier otro de los bienes intelectuales protegidos.
e) Si el agente que comete cualquiera de los delitos previstos... posee la calidad de funcionario o servidor público.

Una de las preocupaciones de los creadores de software, al registrar su obra en el Registro Nacional de Derecho de Autor de INDECOPI, es que se tiene que entregar, entre otros requisitos, el programa fuente, se cuestionan que sucede si lo copian sin su consentimiento. Dado que el depósito es intangible, los funcionarios que cometieran estos delitos estarían dentro de este tipo penal y podrían ser pasibles de pena privativa de libertad hasta ocho años

6. FUNCIONES DE LOS OPERADORES DE JUSTICIA DE LOS DELITOS INFORMATICOS EN EL PERÚ.

6.1. Funciones de los operadores de justicia de la Policía Nacional[20]

Funciones Básicas:

- Función PREVENTIVA para garantizar la seguridad y tranquilidad pública.
- Función INVESTIGATIVA frente a la conexión de delitos y faltas.
- Función PROTECTORA de los derechos y patrimonios públicos y privados.
- Función de AUXILIO frente a pedidos de las actividades.
- Función CONCILIADORA frente a conflictos menores que se constituyen infracciones legales.

[20] PNP. "Organización y funciones" http://www.pnp.gob.pe/organizacion/funciones.asp Fecha de consulta: 5 de junio del 2005

- Otra que la Constitución y las leyes le asignen.

En la Constitución Política del Perú (1993), en su artículo 166 se establece que: La Policía Nacional tiene por finalidad fundamental garantizar, mantener y restablecer el orden interno. Presta protección y ayuda a las personas y a la comunidad. Garantiza el cumplimiento de las leyes y la seguridad del patrimonio público y del privado. Previene, investiga y combate la delincuencia. Vigila y controla las fronteras.

6.2. Funciones de los Fiscales del Ministerio Público

En la Constitución Política del Perú de 1993, en el capítulo X (del Ministerio Público), en los Artículo 159, explican la labor de los operadores de justicia, expresándose textualmente lo siguiente: "Corresponde al Ministerio Público:

1. Promover de oficio, o a petición de parte, la acción judicial en defensa de la legalidad y de los intereses públicos tutelados por el derecho.

2. Velar por la independencia de los órganos jurisdiccionales y por la recta administración de justicia.

3. Representar en los procesos judiciales a la sociedad.

4. Conducir desde su inicio la investigación del delito. Con tal propósito, la Policía Nacional está obligada a cumplir los mandatos del Ministerio Público en el ámbito de su función.

5. Ejercitar la acción penal de oficio o a petición de parte.

6. Emitir dictamen previo a las resoluciones judiciales en los casos que la ley contempla.

7. Ejercer iniciativa en la formación de las leyes; y dar cuenta al Congreso, o al Presidente de la República, de los vacíos o defectos de la legislación.

6.3. Funciones de los Jueces del Ministerio de Justicia[21]

En el Reglamento de Organización y Funciones de las Cortes Superiores menores especifica las funciones siguientes: Artículo 5° "La Corte Superior de Justicia, es el órgano jurisdiccional de dirección, gestión y constituye la máxima instancia jurisdiccional del Poder Judicial en su respectivo Distrito Judicial.

La Corte Superior de Justicia está conformada por:

- Presidente de la Corte Superior.
- Vocales Superiores.
- Jueces.
- Personal de apoyo administrativo y jurisdiccional.

Artículo 8° Es finalidad de la Corte Superior de Justicia:

[21] Corte Superior de Justicia. "Reglamento de Organización y Funciones de las Cortes Superiores de Justicia que cuentan con menos de seis salas superiores" http://www.pj.gob.pe/CortesSuperiores/ROF_CSJ_SIN_CED.doc Revisado el 5-de junio 2005

1. Administrar justicia con criterios de equidad, predecibilidad y transparencia; enmarcada en los principios de la moralidad y la ética.

2. Actuar con autonomía e independencia, garantizando el pleno respeto a la Constitución y las Leyes.

3. Constituirse en instrumento fundamental para la vigencia del Estado de Derecho en el país; así como para la preservación de las libertades y demás derechos fundamentales de la persona humana.

Artículo 9º Su competencia comprende el Distrito Judicial correspondiente. Sus atribuciones y funciones se extienden dentro del territorio del mismo Distrito.

7. TEORÍAS VINCULADAS CON EL TEMA DE ESTUDIO

7.1. Diferentes posturas en cuanto a la regulación de los delitos informáticos

7.1.1. Primera Postura: No existe el delito informático.

En Europa, algunos Estados han regulado en sus códigos penales o leyes especiales, el denominado "delito informático". En España, un gran sector de la doctrina penalista, consideran incluso inadecuada hablar de la existencia como del nomen iuris de "delito informático".[22]

[22] En el actual Código Penal de 1995, o en Leyes penales especiales o las extra-penales, como la LORTAD (Ley Orgánica No. 5, sobre la regulación del tratamiento automatizado de los datos de carácter personal de Octubre 29 de 1992).

El principio penal universal de nullum crimen, nulla poena, sine lege, estima que no habiendo ley que tipifique una conducta delictiva relacionada con la informática como bien jurídico protegido específico, ni que se haya determinado una pena para tales conductas, no existe delito ni pena por las acciones tentadas o consumadas en el campo de la informática.

Así mismo, algunos autores desechan el principio de la analogía de la teoría general del delito para aplicarlo a esta clase de delitos, pues consideran, que éste sólo será aplicable cuando beneficie a un "encausado", pero no para crear nuevos delitos, como se pretende por quienes se encuentran en la vasta vereda de la normativización.

7.1.2. Segunda Postura: Posición ecléctica.

Sin embargo, otros autores entienden que si bien no se puede hablar de delitos informáticos en la actualidad, la protección jurídica goza de solidez en la legislación penal, aunque, por la aparición de estos nuevos fenómenos tecnológicos ésta ha tenido que ampliar su interpretación a las conductas actuales.

7.1.3. Tercera Postura: El delito informático existe doctrinalmente.

Doctrinalmente se acepta la existencia del delito informático, tras analizar los contenidos normativos de otras latitudes

como el ordenamiento jurídico-penal español. En efecto, se estudia la posibilidad de estructurar un nuevo bien jurídico denominado de la "información sobre la información", como un bien que comporta por sí sólo un valor (económico, de empresa o ideal), relevante y digno de tutela jurídico-penal. Este valor será tan importante como para que la conducta humana sea calificada jurídicamente y pueda imponérsele una sanción correspondiente.

En estos tiempos, este derecho fundamental a la información o "derecho a ser informado", consiste en que toda persona tiene derecho no sólo a comunicar sino a "recibir" de las autoridades del Estado o las personas jurídicas públicas o privadas información concreta, oportuna y veraz dentro de los límites de la Constitución y el Ordenamiento Jurídico. No es simplemente la "otra cara" del derecho a comunicar la información, ni a emitir libremente sus ideas y opiniones, en forma verbal o escrita, valiéndose de Prensa e Imprenta o de otro medio, sin sujeción a censura previa, como estaba previsto en las Constituciones Históricas sino un derecho autónomo, complejo, dinámico, público y democrático, por el cual, el Estado debe proteger a quien ocupa la posición de sujeto pasivo de la libre discusión de las ideas (opiniones e información) y a quien participa en él activamente como un emisor de las mismas.

La universalización de los medios de comunicación social, el cúmulo de información que se emite y recibe es cada día mayor y los ciudadanos están expuestos en ese flujo constante de ida y venida de toda clase de información relevante y no únicamente aquella llamada con "valor económico de empresa".

Por su parte el acceso a la información como derecho fundamental de toda persona, se reconoce en incansables legislaciones con relación a los derechos personalísimos de la intimidad, la propia imagen, el honor y el pleno ejercicio de los derechos fundamentales.[23]

7.2. Teoría de la Sociedad de Riesgos de Urlich Beck

El conocido sociólogo Ulrich BECK ha puesto de manifiesto, en su Risikogesellschaft, que las sociedades modernas aparecen actualmente como verdaderas "sociedades del riesgo", en las cuales los efectos adversos del desarrollo de la tecnología, la producción y el consumo adquieren nuevas dimensiones y provocan riesgos masivos a los ciudadanos, los ejemplos más característicos los ubicamos en el tráfico vehicular, la comercialización de productos peligrosos o la contaminación ambiental.

En la dogmática penal actual hay un nuevo paradigma: el de la "sociedad de riesgos"[24]. Se dice que la sociedad actual es una sociedad de riesgos, en la que se admiten, evidentemente dentro de ciertos límites, los riesgos que derivan del tráfico rodado, ferroviario y aéreo, de la utilización de gases, de la existencia de centrales nucleares, necesarias para facilitar energía eléctrica, pero que amenazan parte de la civilización, la producción y comercialización de productos de carácter alimenticio en grandes cantidades, con grave riesgo para los consumidores, la manipulación genética, con peligro de

[23] LORTAD y Dec.1332/94, artículos.12 y ss..
[24] Ulrich Beck, *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Frankfurt, 1986; Pérez del Valle, C., "Sociedad de riesgos y reforma penal", *Poder Judicial*, núms. 43-44 (1996), pp. 61

selección de razas, a través de la creación de seres humanos por clonación, etc. Esta innegable realidad exige la comprensión de la sociedad. Son riesgos exigidos por la modernización e industrialización de la sociedad, que sin duda plantean y seguirán planteando nuevas necesidades al Derecho penal a lo largo de los próximos años[25].

Pues bien, como un claro fenómeno asociado a estos "nuevos riesgos" de la sociedad, se encuentra la informática[26]. No cabe duda que la informática proporciona muchos beneficios, pero, al mismo tiempo, origina no pocos riesgos, porque al generar una abundante información, en poco tiempo y en un espacio muy reducido, puede afectar a la esfera privada del individuo. En este sentido, la existencia de bancos de datos personales y su posible manipulación puede afectar a la intimidad de las personas. En España, afortunadamente, la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, de 29 de octubre 1992, proporciona la protección administrativa de esta información, cuidando por el uso de dichos datos personales.

7.3. Perfil Psicológico del delincuente informático

7.3.1. **La Universidad Tecnológica Metropolitana de Chile (2002),** realiza la siguiente caracterización del delincuente informático:

---

[25] Hilgendorf, "Gibt es ein "Strafrecht der Risikogesellschaft?", *Neue Zeitschrift für Strafrecht* (NStZ), pp. 10

[26] Mir Puig (ed.), *Delincuencia informática*, Barcelona, 1992; Sieber, *Computer und Recht*, 1995; González Rus, "Protección penal de sistemas. Elementos, datos, informaciones, documentos y programas informáticos", *Estudios Jurídicos, Ministerio Fiscal*, Madrid, 1997, pp. 517.

- Caracterización casi mítica del perfil del delincuente informático. Adolescentes con un coeficiente intelectual alto, y ausentes de toda conciencia de estar obrando mal. (síndrome de Robin Hood)

- Mito, ya que una gran cantidad de casos, son cometidos por sujetos que trabajan en el mundo de la informática, de edad superior, y no necesariamente muy inteligentes.

- Empleados de confianza, por la actividad que realizan o por el tiempo que llevan en la empresa.

- Además, existen los delincuentes a distancia

7.3.2. **Claudio Magliona (2003)** opina que: "se ha venido realizando una caracterización casi mítica respecto del perfil del delincuente informático, basándose en los primeros casos de estudiantes americanos que fueron dados a conocer, en que se trataba de adolescentes con un coeficiente intelectual alto, y ausentes de toda conciencia de estar obrando mal".

El prototipo de delincuentes informáticos descrito por la mayoría de los autores, caracterizaba al sujeto activo de estos delitos como jóvenes cuyas edades fluctuaban entre los 18 y 30 años de edad, en su mayoría varones, solteros, sin antecedentes penales, inteligentes, motivados por su profesión y por el desafío técnico.

Esto no constituye más que un mito, por cuanto una gran cantidad de casos de gran gravedad, son cometidos por

sujetos que trabajan en el mundo de la informática, de edad superior, y ni la mitad de inteligentes.

En la actualidad, una buena parte de las conductas informáticas delictivas se lleva a cabo por personas vinculadas de algún modo a las empresas, como empleados de confianza, técnicos, especialistas en programación, y, en general, todo tipo de personas con acceso material a las instalaciones de procesamiento de datos. Suelen ser empleados de confianza por el tiempo que llevan en la empresa o por el tipo de trabajo que desempeñan en ella, y conocen las debilidades del sistema.

Sin perjuicio de lo anterior, Internet permite que hoy concurran como sujetos activos de los delitos informáticos los "delincuentes a distancia", quienes desde cualquier país del mundo pueden atentar contra un sistema de tratamiento de información.

Con el aporte de la obra criminológica del sociólogo norteamericano Sutherland, en las corrientes estructuralistas, se pone de manifiesto la relación clase social - delito en términos de características según el estatus social, de comisión delictiva y de reacción social.

Los criminales informáticos o vándalos electrónicos en su generalidad son de sexo masculino, de 18 a 30 años de edad, con características de ser un empleado de confianza en la empresa en la que desenvuelve sus funciones, posee necesariamente conocimientos técnicos en computación[27].

[27] En Renato Jijena. Impunidad y Delito Informático. http://www.delitosenlared.org, 16 de marzo de 1996.

Estos agentes, responden a motivaciones dispares, generalmente el "animus delicti" es motivado por razones de carácter lucrativo, por la popularidad que representa este actuar en la sociedad moderna o por simple diversión "hackers", o por la intención de que su actuar puede responder al deseo de destruir o dañar un sistema informático, desestabilizando el normal desenvolvimiento en la institución o empresa "crakers". Ambos causan perjuicios aL sistema informático, lo que varia es la intencionalidad en su comisión.

Estos agentes poseen varias características semejantes a los delincuentes de cuello blanco ya que ambos sujetos activos poseen un cierto estatus socioeconómico, no pudiendo explicarse su comisión por mala situación económica o pobreza, ni por carencia de recreación, o por baja educación, ni por poca inteligencia.

La comisión de estas formas de delinquir, ofrecen al "delincuente informático" facilidades de tiempo y espacio para la consumación del hecho, ya que no existe la necesidad de presencia física.

7.3.3. Por último, Espiñeria Sheldon & Asociados (2004) en su trabajo sobre delitos informáticos, señalan que las Estadísticas demuestran que las personas que cometen delitos informáticos poseen generalmente las siguientes características:

- En general son personas que no poseen antecedentes delictivos.

- La mayoría de sexo masculino.
- Actúan en forma individual.
- Poseen una inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos; actitud casi deportiva en vulnerar la seguridad de los sistemas, características que suelen ser comunes en personas que genéricamente se las difunde con la denominación "hackers".
- Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en sí mismo.
- También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.
- Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras y motivadas.

7.4. Perfil de la víctima.

7.4.1. **La Universidad Tecnológica Metropolitana de Chile (2002),** señala las siguientes características de la victimas de los delitos informáticos:

- Personas jurídicas. Bancos, compañías de seguros, empresas públicas y privadas.

- No denuncian los delitos por temor a pérdida de imagen corporativa (seriedad, solvencia y seguridad). Solución mediante medidas internas (despidos o aumentos de medidas de seguridad).

- Situación favorece a delincuentes. (generalmente no se denuncian los delitos, se llega a un acuerdo con el delincuente).

7.4.2. Según Claudio Magliona (2003), las víctimas de estos delitos son generalmente personas jurídicas. Se trata, usualmente, de bancos, compañías de seguros, empresas públicas y privadas, sin importar si cuentan o no con medidas técnicas de protección. Una vez que estas asociaciones detectan las conductas ilícitas de las cuales han sido objeto, suelen no denunciar los delitos por temor a sufrir una pérdida en su imagen corporativa. No están dispuestas a perder la imagen de seriedad, solvencia y seguridad, y antes de ver sus debilidades expuestas, prefieren solucionar el problema mediante la aplicación de medidas internas, como despidos o aumento de medidas de seguridad. Por supuesto, esta actitud no hace sino favorecer a los delincuentes, quienes continuarán con sus conductas con la mayor impunidad.

CAPITULO II:

METODOLOGIA DE INVESTIGACION

Dada la naturaleza del tema de estudio, y los objetivos específicos propuestos, con los cuales se pretende describir y especificar características y rasgos del fenómeno objeto de análisis, se seleccionó una investigación del tipo Descriptivo explicada por Hernández, Fernández, y Baptista (2003,p:117).

El presente trabajo fue organizado desde un punto de vista metodológico en atención a los modelos epistemológicos-positivistas. El fundamento esencial de esta corriente filosófica consiste en hacer tangible la realidad que se pretende estudiar, sin que por esta razón, se experimenten modificaciones en el objeto que se estudia. Lo que es posible, ya que el positivismo sostiene como concepto teórico, que fuera de un individuo no existe una realidad social externa y objetiva de forma preconcebida.

El enfoque de estudio estará orientado por la investigación histórica-bibliográfica de los marcos teóricos existentes que tratan sobre los delitos informáticos, en el ámbito nacional e internacional que sirvieron de base para la elaboración de la propuesta de un nuevo marco teórico actualizado sobre los delitos informáticos en el Perú.

Se recurre al análisis, sistematización de fuentes documentales que se encuentran las bases de datos de las instituciones y organizaciones del

gobierno y archivos privados de empresarios. El trabajo de archivo ha tenido un avance previo con los proyectos de tesis que precedieron en nuestra investigación. En esta última etapa de investigación ubicamos las fuentes bibliográficas de otros tratadistas del tema, como es el caso del INEI, Julio Núñez, Julio Téllez y Blossiers- Calderón, entre los más destacados.

1. HIPOTESIS

En el Perú, la aplicación de un marco conceptual actualizado contribuye al mejoramiento de la labor de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos.

2. MÉTODOS Y DISEÑO DE LA INVESTIGACIÓN

En el nivel descriptivo que incluye un análisis del contexto y su relación con el objeto de estudio se aplicó la metodología positivista con el uso de las técnicas cuantitativas de investigación. Por ello se utilizó de manera combinada, fundamentalmente los siguientes métodos: método inductivo-deductivo, analítico-sintético y el método de la entrevista.

Se utilizaron fuentes primarias y fuentes secundarias.

Las dos primeros métodos indicados corresponden a la investigación científica en general, mientras que el último se utiliza preferentemente en el campo de las Ciencias Sociales; cabe además, tener presente que en su aplicación dichos métodos no se manejan como compartimientos estancados, sino que más bien se apoyan mutuamente para una mejor comprensión y análisis de las variables e indicadores considerados en la investigación.

Señalamos a continuación una breve reseña de cada una de ellos.

2.1. Método Inductivo-Deductivo

Este es un método científico que consta de dos etapas o momentos; la primera etapa nos permite arribar a conclusiones o teorías generales, a partir de los datos específicos encontrados en una investigación determinada. A esta forma metodológica, llamamos inducción; a la inversa, se dará la deducción, cuando en base a la teoría general previamente formulada, podemos explicar los datos o fenómenos específicos encontrados en una investigación concreta o en un proceso de observación de ciertos hechos o acontecimientos.

En general, todas las ciencias emplean este método, por ello es un método de aplicación universal. Al respecto, dice Mario BUNGE que no es sostenible la dicotomía de las ciencias deductivas/ciencias inductivas[28]; significando este, que ambos componentes de este método se dan simultáneamente y no de manera separada.

El proceso inducción/deducción o el proceso inmerso, se encuentran presentes en la formulación de objetivos e hipótesis en el análisis de los resultados de la encuesta y en la formulación de las conclusiones. La teoría general y los datos empíricos se implican mutuamente en los aspectos de la investigación realizada.

---

[28] BUNGE, Mario "La Ciencia, Su Método y su Filosofía". Ed. Siglo XXI. Buenos Aires. 1983. Pág. 25.

2.2. El Método Analítico-Sintético

En la aplicación de este método, según DESCARTES, debe considerarse los siguientes pasos ó etapas[29]:

1. No admitir como verdadera cosa alguna que no sea reconocida con evidencia como tal;

2. Dividir cada una de las dificultades que se examinan, en tantas partes como se pudiera y fuera requerido, para mejor resolverlas;

3. Conducir ordenadamente los pensamientos, comenzando por los objetos más simples y más fáciles de conocer; para ascender poco a poco, gradualmente, hasta el conocimiento de los más compuestos, y suponiendo asimismo un orden entre aquellos que se preceden naturalmente los unos a los otros.

4. Al aplicar este último paso realizamos la síntesis; en cambio la etapa inmediatamente anterior significa el análisis.

2.3. El Método de la Entrevista

Consiste en el conjunto de procedimientos utilizados para verificar en el terreno o sea en la realidad social los objetivos e hipótesis formulados. Dichos procedimientos son entre otros: elaboración de un plan de investigación, definir la entrevista, entre otros.

---

[29] DESCARTES, René. "El Discurso del Método". Pág. 40.

Algunos autores como Gino Germani, la consideran no como un método sino como una forma de organizar el trabajo de campo en la investigación sociológica. [30]

Entrevista temática es una buena elección si, porque:

El objeto de estudio no se conoce muy bien; el problema y el objetivo del estudio pueden ser revisados durante el proyecto.
El "rango" de las respuestas no puede ser conocido con anticipación. Algunos encuestados pueden presentar puntos de vista que sean nuevos y desconocidos para nosotros.

Necesitamos la opción de presentar preguntas adicionales basadas en la información de los encuestados.

Las preguntas están relacionadas con el conocimiento tácito o los puntos de vista personales (actitudes, valores, creencias, etc.), de los encuestados.

Podemos permitirnos el tiempo suplementario y el coste de entrevistas y viajes. Algunos de los encuestados tienen dificultades para expresarse por escrito[31].

Se busca publicar un informe que sea fácil de leer e interese al público en general.

2.4. El Método Histórico

El método histórico es aquel que rellena los vacíos de los hechos y acontecimientos, apoyándose en un tiempo, quizá

[30] GERMANI, Gino "La Sociología Científica" Pág. 32.
[31] Benito Bermejo , Métodos interrogativos de investigación. 24.ene.2005. http://www2.uiah.fi/projects/metodi/264.htm Fecha de consulta: mayo 2005

artificialmente reconstruido, pero que asegura una continuidad y una trama en los fenómenos.[32]

Hayman nos dice que "a causa de la importancia que tiene comprender el pasado, para el progreso en la educación del futuro, la investigación con su estrategia histórica ocupa un lugar importante en el campo de la investigación educacional... la investigación histórica es una de las metodologías generales de investigación en el campo educacional". (Hayman, 1974, p. 8).

Hockett, que es citado por Hayman, señala tres pasos esenciales en la realización de una investigación histórica: a) revisión de los datos, 2) evaluación (o crítica) de los datos, 3) preparación de un informe escrito en el cual se presenten los hechos más notables y su interpretación (Hayman p. 83).

En el caso concreto de la presente investigación, el objeto de estudio estuvo constituido por el análisis comparativo de los principales marcos teóricos existentes y que tienen cierta vigencia en el mundo académico latinoamericano y en especial en el Perú. En cuanto al diseño metodológico cuanti-cualitativo utilizado, este dio las pautas para la elaboración de un nuevo marco conceptual de los delitos informáticos en el Perú que contribuye a solucionar el problema planteado en la tesis.

[32] Abarca, Ramón. "El Trabajo Intelectual: Una Metodología". Universidad Católica de Santa María. Perú. Pp. 125. http://www.ucsm.edu.pe/rabarcaf/trintm04.htm

3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

3.1. Técnicas

Las técnicas que se utilizan en la presente investigación son las siguientes:

- Bibliográfica
- Entrevista
- Análisis e interpretación

Sólo de modo referencial mencionamos algunos concep resumidos respecto de las técnicas mencionadas[33].

3.1.1. Bibliografía

Se refiere a los procedimientos que nos permitieron obtener las citas, resúmenes y comentarios de las obras consultadas.

3.1.2. La Técnica de la entrevista

Se aplicó la entrevista "directiva" o estructurada, porque las preguntas formuladas aparecían en cuestionarios previamente elaborados.

3.2. Instrumentos

Los instrumentos de recolección de datos se constituyeron en fichas bibliográficas y fichas de contenido, que sirvieron para

[33] GOODE, William y HAAT, Paul. "Métodos de Investigación Social". Cap. XIII

identificar y recolectar la bibliografía, apoyándonos de papel y lápiz, libreta de anotaciones.

Es importante resaltar que para la validación del nuevo marco teórico, el Método Delphi se constituyó en una herramienta instrumental apropiado mediante la consulta a expertos.

CAPÍTULO III:

LA NUEVA PROPUESTA DE UN MARCO CONCEPTUAL SOBRE LOS DELITOS INFORMATICOS

1. PAUTAS PARA LA ELABORACIÓN DE UN MARCO TEÓRICO CONCEPTUAL

Según la Dra. Katia Medina Calderón (2004)[34], el proceso se inicia con una revisión de la literatura pertinente, incluyendo datos sobre investigaciones previas, informes, conceptos y definiciones teóricas que den fundamento al problema planteado. Para la elaboración del marco teórico y conceptual de referencia, se requiere conocer e interrelacionar tres niveles básicos de información:

1.1. Primer Nivel

Este nivel que se denomina de información teórica, se requiere el conocimiento y el dominio de las teorías científicas o

[34] Profesora de la Facultad de Odontología de la UNMSM

enfoques teóricos existentes sobre el problema de investigación.

Comprende a todos los trabajos publicados en libros, revistas especializadas, tesis, monografías, artículos periodísticos, etc. Esta información es muy importante porque en ella encontramos diferentes análisis teóricos y enfoques conceptuales, estudios analizados y procedimientos con los cuales el investigador no está familiarizado.

1.2. Segundo Nivel

Comprende la información estadística proveniente de diferentes fuentes y dependencias. Los datos se encuentran en libros, revistas, folletos y también en archivos públicos y privados.

1.3. Tercer Nivel

Comprende a la información empírica primaria o directa, obtenida a través de la aplicación de encuestas, cuestionarios, entrevistas o experimentos de laboratorio. Para lograr este propósito se debe realizar uno o varios contactos con el objeto de estudio (mediante la relación con una muestra representativa de la población) y detectar según los objetivos formulados las propiedades que pretendemos conocer.

Los tres niveles son necesarios y deben ser continuamente retroalimentados y reajustados conforme avanza el proceso de investigación. Para ello, es conveniente revisar la bibliografía y organizar y sistematizar la información empírica.

2. EL NUEVO MARCO TEÓRICO DE LOS DELITOS INFORMÁTICOS EN EL PERÚ

2.1. Definición de los Delitos Informáticos

Los delitos informáticos son todas aquellas conductas y acciones utilizadas por una persona o grupo de personas que con el pleno uso de su(s) facultad(es) físicas y mentales y, mediante el uso indebido de cualquier medio informático o telemático, tienden a provocar un perjuicio a cualquier persona natural o jurídica.

2.2. Características de los Delitos Informáticos

Para las características de los delitos informáticos consideramos como vigentes aporte del mexicano Julio Téllez Valdez, para quien los delitos informáticos presentan las siguientes características principales:

- Son conductas criminales de cuello blanco.
- Son acciones ocupacionales.
- Son acciones de oportunidad.
- Provocan serias pérdidas económicas.
- Ofrecen posibilidades de tiempo y espacio.
- Son muchos los casos y pocas las denuncias..
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

2.3. Tipos de Delitos Informáticos

Se señala los tipos de delitos informáticos tomando como referencia a los tipos reconocidos por las Naciones Unidas y de la Enciclopedia Wikipedia (http://es.wikipedia.org) y los aportados, los mismos que se presentan en la siguiente tabla:

1. Fraudes cometidos mediante manipulación de computadoras.	Manipulación de los datos de entrada
	Manipulación de programas
	Manipulación de los datos de salida
	Fraude efectuado por manipulación informática
2. Falsificaciones informáticas.	Como objeto
	Como instrumentos
3. Daños o modificaciones de programas o datos computarizados.	Sabotaje informático
	Virus
	Gusanos
	Bomba lógica o cronológica
	Acceso no autorizado a servicios y sistemas informáticos
	Piratas informáticos o hackers
	Reproducción no autorizada de programas Informáticos de protección legal

DELITO	CARACTERISTICAS
4. Otros tipos	
Acceso no autorizado	Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
Infracción al copyright de bases de datos	Uso no autorizado de información almacenada en una base de datos.
Interceptación de e-mail	Lectura de un mensaje electrónico ajeno.
"Pesca" u "olfateo" de claves secretas	Los delincuentes suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio. Los "sabuesos" utilizan prógramas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otros delitos, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

Estafas electrónicas	La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.
Estratagemas	Los estafadores utilizan diversas técnicas para ocultar computadoras que se "parecen" electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos.
Juegos de azar	El juego electrónico de azar se ha incrementado a medida que el comercio brinda facilidades de crédito y transferencia de fondos en la red. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias. Además, no se puede garantizar un juego limpio, dadas las inconveniencias técnicas y jurisdiccionales que entraña su supervisión.
Transferencias de fondos	Engaños en la realización de este tipo de transacciones.

Espionaje	Se ha dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto de los Estados Unidos, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera.
Terrorismo	Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
Narcotráfico	Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
Delitos contra la privacidad	Grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos.
Pornografía infantil	Se denomina pornografía infantil a toda representación de menores de edad de cualquier sexo en conductas sexualmente explícitas. Puede tratarse de representaciones visuales o incluso sonoras.
Phising	Tiene el objetivo de conseguir datos confidenciales de usuarios (número de tarjetas de créditos, contraseñas, etc.) a través de e-mail y sitios web fraudulentos[35]

Fuentes: Naciones Unidas, Universidad Autónoma de Santo Domingo (Rep. Dominicana), Wikipedia, apote.

[35] El delito Informático; los nuevos métodos de suplantación, engaño y robo. José Manuel Crespo Mundo Internet 2005- Libro de Ponencias –Volumen I. España pp. 609

2.4. Tipo legal del Delito Informático

2.4.1. **Sujeto Activo**, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados. Puede darse el caso que el sujeto activo que, aunque no desarrolle actividades laborales, sea una persona que "entra" a un sistema informático con intenciones delictivas, por ejemplo cuando desvía fondos de las cuentas bancarias de sus clientes.

2.4.2. **Sujeto Pasivo**, o víctima de delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.

CAPITULO IV: ANALISIS

1. ANALISIS DE LOS MARCOS TEORICOS SOBRE LOS DELITOS INFORMÁTICOS

	INEI	JULIO NUÑEZ	JULIO TELLEZ	BLOSSIERS- CALDERON
Definición de Delitos Informáticos	"No existe una definición en el cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe un concepto propio de los llamados delitos informáticos." Pero se han formulado conceptos funcionales atendiendo a realidades concretas de cada país."	Delitos informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático. 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.,	Julio Téllez señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".	"Si desearíamos delimitar un concepto podríamos decir que el delito informático es toda acción consciente y voluntaria que provoca un perjuicio a persona natural o jurídica sin que necesariamente conlleve a un beneficio material para su autor, o que por el contrario produce un beneficio ilícito para su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión interviene indispensablemente de forma activa dispositivos normalmente utilizados en las actividades informáticas."

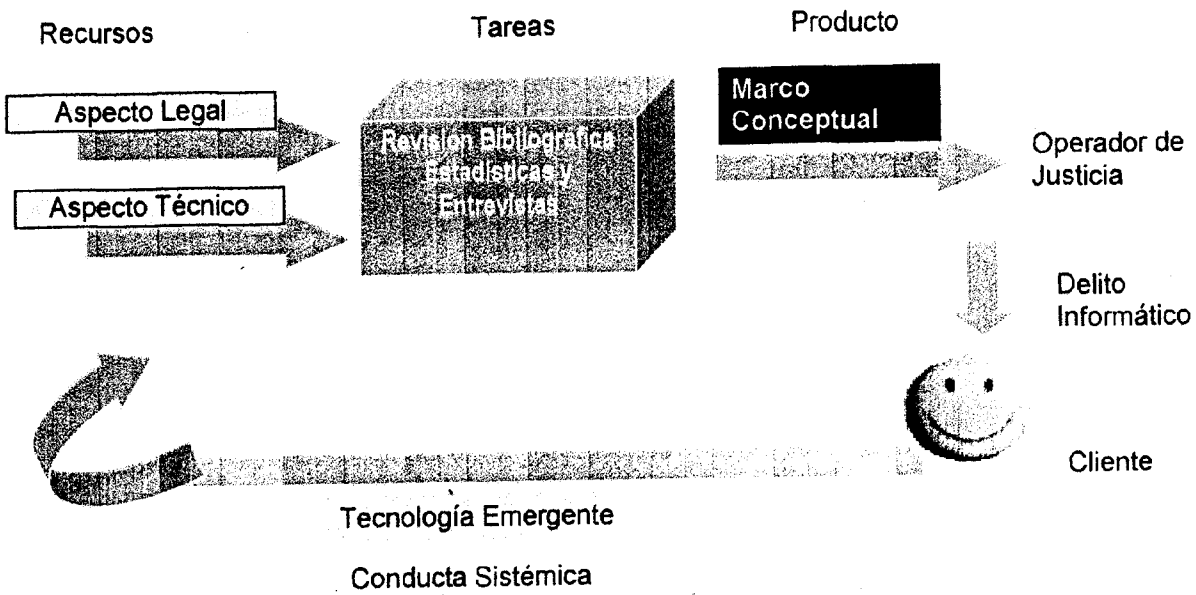
Características	No presenta la caracterización de los delitos informáticos.		Según Téllez Valdez, este tipo de acciones presentan las siguientes características principales: a. Son conductas criminales de cuello blanco b. Son acciones ocupacionales c. Son acciones de oportunidad, d. Provocan serias pérdidas económicas. e. Ofrecen posibilidades de tiempo y espacio. f. Son muchos los casos y pocas las denuncias, g. Son muy sofisticados. h. Presentan grandes dificultades para su comprobación. i. En su mayoría son imprudenciales. j. Ofrecen facilidades para su comisión a los menores de edad. k. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.	• Acumulación de la Información • Inexistencia de Registros Visibles • Falta de Evidencias en la Alteración de Datos y Programas • Eliminación de las Pruebas • Especialidad del Entorno Técnico • Dificultad para Proteger Ficheros o Archivos • Concentración de Funciones del personal sobre la seguridad. • Falta de Controles Internos de Seguridad.- • Carencia de Controles del Personal Técnico.- • Dispersión Territorial de los Puntos de Entrada al Sistema • Interdependencia de Redes de Transmisión

Clasificación	De acuerdo a las conductas catalogadas pueden ser: 1. Fraude por manipulaciones de una computadora contra un sistema de procedimiento de datos; 2.Espionaje informático y robo de software; 3.Sabotaje informático; 4. Robo de servicios; 5. Acceso no autorizado a sistemas de procesamiento de datos, y 6. Ofensas tradicionales en los negocios asistidos por computador. Otra clasificación, es la que sigue: 1. Delitos económicos vinculados a la informática; 2. Ofensas por medios informáticos contra los derechos individuales de la persona: 3. Ataques por medio de la informática contra intereses supraindividuales:	En la clasificación de los delitos informáticos menciona a Julio Téllez Valdés	Julio Téllez Valdés clasifica los delitos informáticos en atención a dos criterios: como instrumento o medio, o como fin u objetivo. • i) Como instrumento o medio. En esta categoría tenemos a las conductas criminales que se valen de las computadoras Como método, medio o símbolo en la comisión del ilícito, por ejemplo : • ii) Como fin u objetivo. En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física	Pueden dividirse en tres grandes grupos: a) Aquellos que se cometen con el uso indebido o manipulación fraudulenta de elementos informáticos de cualquier tipo. b) Acciones físicas que atenta contra la integridad de los equipos informáticos destinado a causar un perjuicio no sólo por destrucción de activos sino para paralizar sus actividades. c) Los delitos relacionados con la propiedad intelectual o copia indebida de programas informáticos generalmente de manera informal. A su vez se clasifican en: 1. Manipulación desde una Computadora a un Sistema de Procesamiento de Datos 2. Espiar, Fisgonear y Robar de Software 3. Sabotaje Informático 4. Robo de Servicios 5. Acceso No Autorizado a

				Sistemas de Procesamiento de Datos 6 Defraudación en los negocios asistidos por un Computador
Tipos de Delincuentes Informáticos	1. Sujeto Activo, posee ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos 2. Sujeto Pasivo, o víctima de delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.			SUJETO ACTIVO Son los que realizan el acto ilícito, Poseen habilidades para el manejo de los sistemas , aunque no desarrollen actividades laborales, de manera que el sujeto activo está dado por la persona que "entra" a un sistema informática con intenciones delictivas, por ejemplo cuando desvía fondos de las cuentas bancarias de sus clientes. SUJETO PASIVO Es el ente sobre el cual recae la conducta de acción, generalmente conectados a otros sistemas En este caso se encuentran personas naturales. De otro lado las personas jurídicas entre las que podemos citar bancos, compañías, etc.

Tipos de delincuentes informáticos	Hacker; Cracker; o "rompedor", Phreaker: Virucker; Pirata Informático.			1. Introducción de datos falsos o data diddling 2. El caballo de troya 3. El salame, redondeo de cuentas o " rounding down". 4. Uso indebido de programas "superzapping" 5. Puertas falsas o " traps doors" 6. Bombas lógicas 7. Ataques asincronicos 8. Recojo de información residual o "scavenging". a) el scavenging físico: b) el scavenging electrónico: 9.divulgación no autorizada de datos o data leakcage 10. Acceso a áreas no autorizadas o piggyn baking 11. Suplantación de la personalidad 12. Pinchado de líneas 13. Hurto de tiempo 14. Simulación e imitación de modelos 15. Piratas o "hackers". 16. Crackers 17. Phreakers 18. Los virus 19. Gusanos 20. Delitos de connotación sexual por Internet.

OPERACIONALIZACION DEL MARCO CONCEPTUAL DE LOS D.I.



CAPITULO V:

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Se puede afirmar que los delitos informáticos en el Perú, son todas aquellas conductas y acciones utilizadas por una persona o grupo de personas que con el pleno uso de su(s) facultad(es) físicas y mentales y, mediante el uso indebido de cualquier medio informático o telemático, tienden a provocar un perjuicio a cualquier persona natural o jurídica.

2. Los delitos informáticos presentan las siguientes características principales:
   - Son conductas criminales que sólo un determinado número de personas con ciertos conocimientos puede llegar a cometerlas.
   - Son acciones ocupacionales.
   - Son acciones de oportunidad..
   - Provocan serias pérdidas económicas.
   - Ofrecen posibilidades de tiempo y espacio y sin una necesaria presencia física pueden llegar a consumarse.
   - Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
   - Son muy sofisticados.
   - Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
   - Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

3. Entre los tipos de delitos informáticos destacan: La manipulación de los datos de entrada, la manipulación de programas, manipulación de los datos de salida, el fraude efectuado por manipulación informática, falsificaciones informáticas, daños o modificaciones de programas o datos computarizados, acceso no autorizado, infracción al copyright de bases de datos, interceptación de e-mail, "pesca" u "olfateo" de claves secretas", estafas electrónicas, estratagemas, juegos de azar, transferencias de fondos, espionaje, terrorismo, narcotráfico, delitos informáticos contra la privacidad y pornografía infantil.

4. En la tipología de los delitos informáticos se destacan: Los sujetos activos y los sujetos pasivos.

5. Es viable e imprescindible reactualizar constantemente el marco teórico de los delitos informáticos para que se constituya en un instrumento eficaz para los operadores de justicia que intervienen en la lucha contra los delitos informáticos en el Perú.

RECOMENDACIONES

1. La propuesta de la elaboración y constante reestructuración del marco conceptual de los delitos informáticos en el Perú, que es una necesidad reclamada por los operadores de justicia, merece ser considerada en la agenda de trabajo de la comunidad académica debido al impresionante incremento de los delitos informáticos en el país.

2. Se sugiere que a corto plazo se realice un estudio multidisciplinario y cuanti-cualitativista sobre el tema en mención para lograr resultados importantes y que deriven en alternativas eficaces para la implantación de políticas y programas de prevención de los delitos informáticos.

3. Además se recomienda a los docentes informáticos que promuevan e incentiven en sus alumnos el deseo e interés por ahondar en la investigación de las nuevas modalidades de delitos informáticos que van

apareciendo paralelamente a los avances tecnológicos y científicos en el campo de la informática.

4. Por último, se exhorta tanto al gobierno ejecutivo como a los legisladores congresistas que muestren signos de sensibilización sobre la problemática tratada mediante la legislación y promulgación de leyes que se fundamenten en marcos teóricos vigentes sobre los delitos informáticos.

BIBLIOGRAFIA

1. Amadeo Gadea, Sergio Luis [2001]. Informática y Nuevas Tecnologías. Madrid, Editorial La Ley, 463 pp. Col. Derecho de las Telecomunicaciones.

2. Aparicio Salom, Javier [2000]. Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal. Madrid, Aranzadi.

1. Blossiers, Juan José y Calderón Sylvia B. "Delitos Informáticos: Camino a la Impunidad " Pp. 34

2. Callegari, Nidia. Delitos Informáticos y Legislación en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 Julio-Agosto-Septiembre. 1985. P.115.

3. Carlón Ruiz, Matilde [2000]. Régimen jurídico de las telecomunicaciones. Una perspectiva convergente en el estado de las autonomías. Madrid, La Ley, 563 pp. Col. Derecho de las Telecomunicaciones.

4. Corredoira, Loreto (ed) [1998]. Los retos jurídicos de la información en Internet. Madrid.

5. Cousido González, María del Pilar [2001]. Derecho de la comunicación audiovisual y de las telecomunicaciones. Madrid, Colex, 320 pp.

6. Davara, Miguel Ángel [2000]. La protección de los intereses del consumidor ante los nuevos sistemas de comunicación electrónica. Madrid, CEACCU. Capítulo 1.4 "La vulnerabilidad de los datos", págs. 29-31.

7. Desantes Guanter, José María y Soria, Carlos [1991]. Los límites de la información. Madrid, Asociación de la Prensa. Col. Cuadernos de Periodistas No. 2, 126 pp.

8. Escobar de la Serna, Luis [1997]. Manual de Derecho de la Información. Madrid, Dykinson, 688 pp.

9. Freixas Gutiérrez, Gabriel [2001]. La protección de datos de carácter personal en el derecho español. Barcelona, Bosch, 394 pp.

10. García Castilleio. Ángel [2000]. "La regulación de los contenidos audiovisuales en Internet" en Revista Actualidad y Cyberlaw, diciembre.

11. González Ballesteros, Teodoro [1999]. Diccionario jurídico para periodistas. Madrid, C.E. Ramón Areces, 1007 pp.

12. González Quintanilla, "Derecho Penal Mexicano. (Parte General)". José Arturo. Editorial Porrúa, S.A. México 1993. pp. 504.

13. Gore, Albert [1993]. "La Infraestructura Nacional de Datos (NII) de Estados Unidos de América: Agenda para la Acción (Informe Gore)", en Novática número 110 (julio- agosto de 1994). Traducción de Rafael Fernández Calvo.

14. 20. Herrán Ortíz, Ana Isabel [2002]. El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales. Madrid, Dykinson.

15. INEI. "Delitos Informáticos". Colección Seguridad de la Información. Perú 2001. Pp.127

16. La Torre, Carlos. "Los Delitos Informáticos en el Perú".Universidad de Lima, Perú. http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=30 (2004)

17. Lima de la Luz, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984. Pp.100.

18. Mundo Internet 2005- X Congreso: Internet, telecomunicaciones y sociedad de la Información. Libro de Ponencias –Volumen I. España. 13 al 15 de abril 2005.

19. Méndez, Carlos. Metodología. Guía para elaborar diseños de investigación en Ciencias Económicas, Contables y Administrativas. México, Ed. Mc Graw Hill, 1983, 156 pág.

20. Müller Hugo. "Los Delitos Informáticos en el Código Penal Peruano". Revista Nº 36 de la PNP Pp. 5 Perú http://www.pnp.gob.pe/culturales/revista_81/pag_36_40.pdf (2004)

21. Muñoz Machado, Santiago [2000]. La regulación de la red. Poder y derecho en Internet. Madrid, Taurus.

22. Núñez, Julio. "Perú: Los Delitos Informáticos" Alfa - Redi: Revista de Derecho Informático Martes, 15 Marzo del 2005 ISSN 1681-5726 http://www.alfa-redi.org/revista/data/17-2.asp (2004)

23. ONU. "Delitos Informáticos" Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 18 a 25 de abril de 2005, Bangkok (Tailandia)

24. Ruiz Carrillo, Antonio [2001]. La protección de datos de carácter personal. Barcelona, Bosch. Capítulo V Apartado 24 y Apéndices II-c).

25. Sarzana, Carlos. "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Roma, Italia. 1979. P.53.

26. Soto, Alberto "Argentina: Delitos Informáticos" Alfa-Redi org-Revista de derecho informático. http://www.alfa-redi.org/revista/data/52-3.asp 10 de abril del 2005.

27. Téllez Aguilera, Abel [2002]. La protección de datos en la Unión Europea. Madrid, Edisofer, 303 pp.

28. Téllez, Julio. "Derecho Informático". Edt. Mc Graw Hill. México, Segunda Edición 1996.pp.283.

29. Ulrich Beck, "Risikogesellschaft. Auf dem Weg in eine andere Moderne", Frankfurt, 1986; Pérez del Valle, C.,

30. Villalobos, Ignacio. "Derecho Penal Mexicano". Editorial Porrúa, S.A. México 1975. pp. 650.

31. Velázquez Bautista, Rafael [2002]. Derecho de tecnologías de la información y las comunicaciones (T.I.C.). Madrid, Editorial Colex, 303 pp. Capítulo II: Tratamiento de datos personales.

DIRECCIONES TELEMATICAS

Delitos Informáticos y Seguridad
http://www.uned.ac.cr/SEP/maestriasydoc/maestrias/propintelec/enlaces.htm

Information Society Policy Office
http://europa.eu.int/ISPO/Welcome.html
http://europa.eu.int/ISPO/infosoc/telecompolicy/

Brigada de investigación Tecnológica
http://www.mie.es/policia/bit/index.htm

National Infraestructure Protection Center (Cybernotes)
http://www.nipc.gov/cybernotes/cybernotes.htm

Convenio Europeo sobre el Cibercrimen
http://convetions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=22/12/01

European Police Office (EUROPOL)
http://www.europol.eu.int/home.htm

Cybercrime (US Department of Justice)
http://www.cybercrime.gov

Business Software Alliance
http://www.bsa.org

International Relations and Security Network
http://www.ins.ethz.ch/linkslib/

Anti-Corruption Network for Transition Economies
http://www.nobribes.org

Financial Action Task Force on Money
http://www.oecd.org/fatf/

International Chamber of Commerce
http://www.iccwbo.org/

International Criminal Police Organization (ICPO-Interpol)
http://www.interpol.int

Transparency International (TI)
http://www.transparency.org

USA Department of State: Global Forum on Fighting Corruption
http://www.usinfo.state.gov/topical/econ/integrity/

World Bank: anti-corruption
http://www.worldbank.org/publicsector/anticorrupt/

Delitos Informáticos
http://www.delitosinformaticos.com

Delitos informáticos reconocidos por la ONU
http://www.seguridad-la.com/e_delitos_un.htm

Asociación para el Progreso de las Comunicaciones en Internet y las TIC
http://www.apc.org

Secretaría de Estado de Telecomunicaciones y Sociedad de la Información de España http://www.setsi.mcyt.es

ANEXOS

Consultar el capitulo completo en formato impreso