UNIVERSIDAD DE PANAMA

VICERRECTORIA DE INVESTIGACION Y POSTGRADO

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

Programa de Maestria en Derecho con Especializacion

en Ciencias Penales

Consideraciones Politico Criminales en torno a la Delincuencia Informática y el Delito de Daños

Por

Campo Elias Munoz Arango

Trabajo de Graduación para optar al grado de Magister en Derecho con especializacion en Ciencias Penales

Panama

2010

A mis Padres, Carlos Enrique y Virginia del Carmen,

por su amor y apoyo incondicional.

A mi Abuelo, Campo Elías, por su cariño y sus sabios consejos,

y a la memoria de mi abuela Matita.

A familia, Nadia Patricia y Lucas Andrés,

con el amor, de ayer, hoy y siempre.

A Dios todopoderoso, por todo lo bueno que ha hecho en mi vida.

Al profesor, Dr. Raúl Sanjúr, por sus orientaciones y por las experiencias compartidas.

A la Sección de Informática Forense, del Instituto de Medicina Legal, por su cooperación e información sobre la realidad actual de la delincuencia informática, indispensable en la culminación de la presente investigación.

INDICE GENERAL

CAPÍTULO 3

MARCO METODOLÓGICO

CAPÍTULO 4

ANÁLISIS E INTERPRETACIÓN DE DATOS

INDICE DE GRAFICAS

Delitos Informáticos Investigados

RESUMEN

Esta investigación de tipo documental tiene como propósito analizar la información escrita a nivel nacional e internacional, especialmente de la doctrina extranjera en lo que se refiere al delito de daños y su relación con la delincuencia informática. El analizar códigos penales extranjeros y la doctrina penal moderna ha sido de mucho provecho para esta investigación ya que podemos observar las carencias de nuestra legislación en comparación con el resto de América latina y de Europa. El carácter descriptivo de esta investigación nos ha permitido relatar la legislación internacional, para lograr entender qué corregir en la legislación panameña, a fin de cómo se descubre de los datos relacionados a delitos informáticos, la falta de denuncias de estos delitos. De investigación se ha obtenido como resultado, el entender que en Panamá, el delito de daños solo se relaciona con los delitos informáticos, en el sentido de que se enfoca en la utilización de tecnológicas para cometer el delito. Igualmente encontramos que de la mala estructura del delito en el Código Penal de 2007, no tenemos una tutela exacta sobre el sabotaje informático lo cual hace que en la realidad no se hagan denuncias de estos casos de sabotaje informático, cuando es una realidad encontrada en las estadísticas que en los últimos años ha habido un aumento de delitos cometidos con la ayuda de una computadora. Resulta necesario modificar el Delito de Daños en el Código Penal para que se cree de manera autónoma un delito de sabotaje informático, dentro del título de los delitos contra la seguridad informática insertados en el Código Penal, estructurando de manera separada en el código los daños sobre una computadora hechos de manera física de aquellos que suponen el uso de una computadora.

SUMMARY

This documentary research aims to analyze the written information that has been made nationally and internationally, especially the foreign doctrine in regard to the crime of Damages as it relates to computer crime. The analysis of foreign penal codes and modern penal doctrine has been of great use for this research because we can observe what our legislation lacks compared to the rest of Latin America and Europe. The distinctiveness of this research has allowed us to relate to international law, to ensure correct understanding of Panamanian law, as the data related computer crime showed underreporting of these crimes. As a result of the research, we understand that in Panama, the crime of damages only relates to the crime, in the sense that it focuses on using technology to commit the crime. Also found that the poor structure of the crime in the Criminal Code of 2007, we have no accurate guardianship of computer sabotage which makes the reporting of cases of computer sabotage not common, when it is a reality encountered in the statistics that in recent years there has been an increase in crimes committed with the aid of a computer. It is necessary to amend the Crime of Damages in the Criminal Code for the creation of an autonomous crime of computer sabotage, in the title of computer security crimes found in the Criminal Code, structuring of the code separately in damages on a computer made of physically and those that involve the use a computer.

CAPÍTULO 1

ASPECTOS GENERALES DE LA INVESTIGACIÓN

1.1 Planteamiento del Problema

Los avances tecnológicos han llevado al Derecho Comparado a castigar diversas formas de delincuencia informática, entre otros, aquellos hechos cometidos mediante la manipulación de computadoras y daños o modificaciones de programas o datos computarizados que no aparecían comprendidas en las tradicionales figuras delictivas de esas legislaciones.

En el Código Penal de 22 de septiembre de 1982 y en el vigente de 22 de mayo de 2007 no se castigan estas nuevas formas de criminalidad, en particular en el delito de daño, por lo que en esta investigación pretendemos plantear la necesidad de incorporar estas nuevas formas de criminalidad, constitutivos también de un ataque contra el patrimonio, que requieren de nuevas formas de protección.

Lo anterior, es necesario por razones de seguridad jurídica, y también por cuestiones relacionadas con el quantum de la pena, dado que en la actualidad, en nuestra legislación no existe relación entre el acto y el bien jurídico lesionado. A manera de ejemplo podemos mencionar los daños ocasionados por los virus informáticos, la manipulación de información y la destrucción de soportes electrónicos, etc., aspectos que en los últimos años han devenido en extremo perjudiciales, y onerosos por lo cual se hace necesario examinar esta materia o problemática, a fin de hacer los correctivos

necesarios.

En la actualidad en Panamá, a fin de delimitar la competencia de los delitos contra la seguridad informática, el Ministerio Público mediante resolución No. 19 de 10 de julio de 2008, determino que estos hechos delictivos serían del conocimiento de la fiscalía denominada: Fiscalía de delitos contra la propiedad intelectual y la seguridad informática, aunque debe quedar claro que aquí no se incluyen en general los demás comportamientos delictivos relacionados con delitos informáticos.

Por otro lado, debe recordarse que los delitos contra la seguridad informática, han sido incorporados en el Capítulo Primero "Delitos contra la seguridad informática" del Titulo VIII, "De los delitos contra la seguridad jurídica de los medios electrónicos" del Código Penal de 2007.

Frente al panorama anteriormente expuesto, nos formulamos las siguientes preguntas de investigación:

¿Existe en la República de Panamá, algún tipo de entidad especializada en la persecución de los Delitos Informáticos?

¿De qué manera puede ser afectado el Derecho a la propiedad, por parte de la delincuencia informática?

¿Está estructurado el Delito de Daños en el Código Penal Panameño del 22 de mayo de 2007, de manera que permita perseguir un acto de sabotaje informático?

¿Qué entiende por Delito Informático la Doctrina del Derecho Penal?

¿En qué se diferencia al Delito Informático y la Delincuencia Informática desde la perspectiva del Derecho Penal Moderno?

¿En qué medida el Derecho Comparado puede coadyuvar a fin de que nuestra legislación se actualice de cara a la persecución del sabotaje informático?

1.2 Enunciado

El delito de sabotaje informático como variación de los delitos informáticos, necesita estar incorporado en nuestra legislación Penal vigente, con la finalidad de tutelar correctamente el patrimonio desde la perspectiva tecnológica, evitando que se trate como un simple delito de daños a la propiedad cuando la realidad de esta figura delictiva exige al Derecho Penal adecuar la legislación con respecto a los avances tecnológicos, así como también requiere por parte del Órgano Judicial y del Ministerio Público contar con las herramientas e infraestructura necesaria para el tratamiento de estos delitos.

1.3 Objetivos

1.3.1 General

Identificar las entidades especializadas en la persecución de los delitos informáticos.

Determinar el alcance de la afectación, del bien jurídico protegido, "patrimonio económico", en los daños ocasionados por la delincuencia informática.

1.3.2 Específicos

Verificar si el acto de sabotaje informático esta estructurado en el delito de daños consagrado en el Código penal de 2007, para efectos de responsabilidad penal.

Analizar dogmáticamente las nociones de delito informático.

Deslindar el delito informático y la delincuencia informática desde la perspectiva del derecho penal moderno.

Evaluar la normativa a nivel del Derecho Comparado con miras a actualizar la regulación y el tratamiento jurídico de los delitos informáticos.

1.4 Alcance o Delimitación del problema

Este estudio en principio se circunscribe ante todo a nuestra Legislación Penal Patria; no obstante, por la naturaleza y especialidad del tema, es necesario complementarla con legislación y Doctrina Extranjera, especialmente la Española dentro de Europa y países como Argentina, Colombia y México dentro de América. Como también recabar información idónea sobre la investigación de los delitos informáticos y en específico aquellos relacionados al Patrimonio y al delito de daños en Panamá.

1.5 Limitaciones

La información, para hacer esta investigación resulta a veces ser una limitante, ya que debido a naturaleza de constante cambio en materia relacionada con tecnologías de la información, en momentos resultará difícil saber si el material recabado esta actualizado y si su fundamentación es la correcta. El problema del idioma, puede llegar a ser un problema, aunque limitando la investigación sobre material en inglés y español se puede hacer una condensación del material que no afectará la investigación, debido a que las obras más importantes relativas a esta materia y sus autores usualmente son traducidos al español.

Igualmente es importante resaltar el factor tiempo ya que dentro de esta investigación, la naturaleza del objeto tutelado, los datos personales, denotan un constante movimiento de actualización y renovación legal, lo cual hace importantísimo realizar esta investigación teniendo en cuanta la posibilidad que las legislaciones internacionales estudiadas están sujetas a constante revisión y actualización, lo que hace posible que dentro del proceso de investigación una ley que se utilizare como base teórica dentro del transcurso de la investigación fuese derogada y cambiada por otra. Lo cual obliga a tener en cuenta la posibilidad de que durante el proceso de investigación, elementos importantes de la tesis pueden ser modificados o derogados en algunos casos, por lo cual es importante revisar constantemente las fuentes de información.

1.6 Justificación del problema

Esta investigación tiene como propósito en principio, el estudio tiene como fin lograr que dentro de nuestro país, se capte la importancia de proteger y tutelar por parte del Estado, lo relativo a la protección del patrimonio, en lo que hace referencia al delito de daños cuando este se relaciona con los delitos informáticos.

Supone así proponer que la Doctrina panameña entre a discutir como lograr tal tutela, en todas las esferas posibles: sea Civil, Penal, Constitucional, logrando así efectivamente, proteger el Derecho a la propiedad, de manera integral frente a cualquier ataque relacionado con las nuevas tecnologías de la información y comunicación.

En la actualidad nuestro Código Penal no contiene todas las modalidades existentes relacionadas con los Delitos informáticos, se justifica el tratar de modificar el Código Penal para que este más actualizado o establecer una ley general relativa a los delitos informáticos.

Se justifica lograr estos cambios en nuestra legislación a fin de poder tener los controles necesarios para enfrentar estas nuevas formas de criminalidad y así el Estado proveer al ciudadano protección a sus derechos y la apropiada ayuda al usuario cuando necesite respuestas frente un ataque de esta naturaleza a su propiedad.

CAPÍTULO 2

MARCO DE REFERENCIA

2.1 Marco teórico

2.1.1 Consideraciones fundamentales sobre la delincuencia informática y concepto de la Delincuencia Informática

2.1.1.1. Antecedentes de la delincuencia informática

El desarrollo tecnológico experimentado a finales de este siglo en lo referente a las tecnologías de la información y comunicación ha significado un avance en el desarrollo de la sociedad, pues la informática proporciona muchos beneficios, pero, al mismo tiempo, origina numerosos riesgos, no solo para el patrimonio de otras personas, sino también, al generar abundante información en poco tiempo y en un espacio muy reducido para la esfera privada del individuo, no en vano JAEN VALLEJO menciona que, "cada vez es más frecuente el pirateo y sabotaje de programas, especialmente en Internet, quizás porque a través del ordenador es mucho menor la conciencia del riesgo de la acción y de la crítica social que en los supuestos tradicionales (atraco a un banco por ejemplo)". (Jaén Vallejo, 2004:76)

En los últimos 30 años el Derecho Penal ha debatido acerca de establecer medidas para contrarrestar esta criminalidad informática, y las legislaciones se han enfrentado a problemas dogmáticos y de política criminal, al momento de incorporar estos delitos en

sus legislaciones penales como conductas nuevas de manera autonoma en leyes especiales o en tratados internacionales

Durante los inicios de la decada de 1990 se hacia mencion de manipulaciones informáticas las cuales representaban una amenaza seria a la moderna economia y se mencionaba en las estafas y falsificaciones de documentos manipulaciones de inputs y de programas como tambien la manipulacion de outputs el espionaje y sabotaje de datos temas y conductas que a futuro serian tema diario de discusion del derecho penal en general (Cfr Tiedemann 1993 51)

La aparicion y desarrollo de la criminalidad informática se ha descrito de diferentes maneras asi por ejemplo HOLLINGER divide esta evolución en cuatro periodos distintos un primer periodo del descubrimiento que circunscribe de 1946 a 1976 donde el abuso sobre computadoras o sobre sistemas de comunicacion o información como lo fue el phreaking son identificados y destacados en la literatura especializada (Cfr Hollinger 1997 En Walden 2007 25)

Posteriormente se concibe que durante 1977 a 1988 se da el segundo periodo llamado el de la racionalizacion ya que surgen los primeros intentos del Derecho Penal para corregir o actualizar las legislaciones a fin de hacer frente a este tipo de criminalidad

Durante 1988 a 1993 se presenta el tercer periodo denominado el periodo de denominacion del hacker donde las agencias policiales y de investigacion trataron

usualmente de manera poco efectiva de perseguir a quienes actuaran de cualquier manera que atentara contra la revolución de las llamadas tecnologías de la comunicación e información, en específico los "hackers y phreakers".

Finalmente, en la actualidad estamos en el período de la censura, donde el interés dejó de ser aquellas conductas que pongan en peligro la integridad de la computadora, para centrarse en aquellas conductas que suponen poner en Internet contenido ilegal, al que cualquiera pueda acceder, como lo es la pornografía infantil, etc.

Otros autores han presentado la evolución de la criminalidad informática partiendo de las etapas legislativas, en las cuales el Derecho Penal ha elaborado algún ordenamiento que regule el informático para así enfrentar la creciente criminalidad relacionada con las computadoras, la cual posteriormente se identificara como delito informático. Por ejemplo SIEBER mencionaba seis distintos momentos en el tratamiento legal de los delitos informáticos por parte de las naciones. (Cfr. Sieber 1998 en Walden 2007:26)

Así partiendo de un análisis a los intentos de legislar en materia penal sobre los delitos informáticos, se considera que entre 1970 y 1980, en una primera etapa, aparecen leyes sobre protección de datos, relacionadas con el bien jurídico de la intimidad, para dar respuesta a la capacidad de las computadoras para tratar datos de carácter personal.

La segunda etapa, inicia desde mediados de 1980, donde se actualizaron legislaciones a fin de tratar conductas de criminalidad informática, pero lastimosamente

no lograban ser una adecuada tutela para estas conductas.

Posteriormente durante la década de 1980 y hasta mediados de la década de 1990, se actualizan las leyes en materia de propiedad intelectual, para lograr tutelar las nuevas formas de propiedad relacionadas con las tecnologías de la información y comunicación, como lo son el "software" y la manera en que se tratarían frente estas nuevas tecnologías, aquellas obras ya reguladas previamente de manera tradicional.

En este periodo se resalta la aparición de la red global o Internet durante los mediados de la década de 1990, donde se centró la atención por crear y actualizar la legislación dirigida a tutelar los contenidos de carácter ofensivo o ilegal (antisemitismo, pornografía infantil, etc.) y se armoniza a la vez la legislación procesal.

Finalmente menciona SIEBER, una última etapa donde se elaboran normas relacionadas con la regulación de protocolos y medidas de seguridad informática, como lo son la criptografía y las firmas digitales en general, lo cual se ubica durante los finales de la década de 1990.

Dentro de los diversos criterios para lograr la determinación de los orígenes y desarrollo de los delitos informáticos: se considera que la aparición y motivación del delincuente informático al momento de realizar estas actividades, es decir, desde la perspectiva del "hacker" y de quien crea un virus informático, ya que se puede establecer que los primeros hackers, ante todo estaban en conductas impulsadas por curiosidad y experimentación, no por la intención de apropiarse de algo ajeno, así se habla que

proporcionalmente al desarrollo y propagación de estas tecnologías, estos delitos informáticos evolucionaron de tal manera que en la actualidad son conductas criminales comunes en nuestra sociedad tecnológica, las cuales conllevan resultados y efectos a mucha mayor escala, no solo con perjuicios de carácter personal, sino de carácter económico a gran escala. (Cfr. Walden, 2007:26).

En la actualidad los problemas que enfrenta el Derecho Penal frente a la criminalidad informática son numerosos, la naturaleza y cambio constante de la tecnología enfrentándose al tiempo que demora modificar la legislación penal supone grandes limites al momento de actualizar la legislación.

Así problemas como el robo o violación de la confidencialidad de la información, los fraudes financieros cometidos por vía electrónica y los fraudes de telecomunicaciones causan grandes pérdidas o gastos a sus victimas, no obstante nuevas conductas están apareciendo con el pasar del tiempo como lo es el tratar de acceder ilegalmente a la información contenida en teléfonos móviles de tercera generación.

Otras nuevas conductas que resultan problemáticas para descifrar y detener son el lavado de dinero a través de fraudes en línea en sitios de contratación o búsqueda de empleo donde criminales tratan de captar usuarios a los cuales les pagan o tratan con dinero sucio a fin de poco a poco lograr estafarles alguna cantidad de dinero y a su vez poner su dinero sucio a circular.

Gran problema resulta ser que cada vez más el criminal informático encuentra

nuevas maneras de incrementar el grado de impunidad de sus delitos o por lo menos cada vez más utilizan medios que hacen difícil la persecución de estos por las autoridades, sea con el manejo ilegal de las claves de un proveedor de servicio de Internet o el uso de códigos clave; por no decir que el trabajo en contra de estos criminales cada vez resulta ser más difícil y tedioso.

Así en la actualidad entre todas las otras discusiones que pueden encontrarse frente a la criminalidad informática se está tratando de crear legislación a fin de legitimar mayores controles sobre el Internet y en especifico sobre los sitios de Internet malignos, con propuestas que buscan legalizar el cerrar un sitio de Internet, frente lo que se hace en la actualidad que es poner controles sobre el proveedor de servicio de Internet quien brinda el servicio al titular del sitio de Internet malicioso.

Para terminar, en nuestro país el antecedente previo al delito de sabotaje informático lo encontramos en el Anteproyecto de Código Penal de 2006, en el Titulo II, Capítulo VI De los Daños, artículo 242, establecía como agravante para el delito de daños, cuando se ocasionara utilizando instrumento o medios informáticos a computadora, dato, red o programa de esa naturaleza. El texto del artículo 242 del anteproyecto de Código Penal de 2006 decía lo siguiente:

> *"Artículo 242. Quien destruya, inutilice, rompa o dañe cosa mueble o inmueble que pertenezca a otro será sancionado con pena de uno (1) a dos (2) años de prisión*

o su equivalente en dias multa o arresto de fines de semana La sancion se aumentara de una cuarta parte a la mitad de la pena si el delito se comete

1 En perjuicio de un servidor publico a causa del ejercicio de sus funciones

2 Mediante intimidacion o violencia contra tercero

3 Con destruccion o grave daño en residencia oficina particular edificio o bien publico bien destinado al servicio publico edificio privado o destinado al ejercicio de algun culto en un vehiculo monumento publico cementerio cosa de valor cientifico cultural historico o artistico

4 En una plantacion sementera o en las cercas protectoras de fundos agricolas o pecuarios

5 Mediante la utilizacion de sustancia venenosa o corrosiva

6 Si el dano total ocasionado supera la suma de dos mil balboas (B/ 2 000 00) independientemente del valor del bien que se haya afectado directamente con la accion

Cuando se ocasione utilizando instrumento o medios

informaticos a computadora dato red o programa

de esa naturaleza la pena sera de dos (2) a cuatro (4)

años de prision

Cabe indicar que varios fueron los intentos legislativos para incorporar algunos de los delitos informaticos en la legislacion penal panameña los cuales desarrollaremos a continuacion

2 1 1 2 Orígenes y actualidad de la Delincuencia informática en la Legislación Panameña

2 1 1 2 1 Situación previa al Código Penal de 2007

Las legislaciones penales previas al Codigo Penal de 2007 no contemplaron la regulacion de los delitos informaticos sin embargo hay que señalar que hubo una propuesta legislativa en el año 2001 y que también por su parte los Anteproyectos de Codigo Penal de 1998 y revisado de 1999 hacian referencia al sabotaje informático respectivamente los artículos 173 y 225

Asi es necesario mencionar la propuesta legislativa que presento el Honorable Legislador Nodier Miranda a consideracion de la Comision de Gobierno Justicia y

Asuntos Constitucionales, en el año 2001. Tal propuesta de modificación del Código Penal de 1982, contenía normas relativas a los delitos informáticos.

Por razones que desconocemos tal propuesta de reforma, no fue aprobada aunque existe constancia de que el Presidente de la Comisión de Gobierno Jerry Wilson Navarro, comunicó el primero de octubre de 1982, al Presidente de la Asamblea Honorable Legislador, Rubén Arosemena Valdés, que la comisión había analizado el Anteproyecto de Ley No. 34 por medio del cual se añadían los artículos 241-a, 241-b, 241-c, 241-d y 241-e al Capítulo II, del Título VII del Código Penal tipificando el delito informático y se toman otras disposiciones, con el objeto de darle el trámite correspondiente, en primer debate.

El Anteproyecto de Ley no. 34, en sus cinco artículos decía lo siguiente:

> *Artículo 1. Se añade el artículo 241-A al Código Penal, el cual rezará así:*
>
> *Artículo 241-A: El que por cualquier medio, destruya, altere, inutilice, dañe, impida u obstaculice el funcionamiento de sistemas de tratamiento de datos o información, sus partes o componentes, así como programas y documentos electrónicos ajenos que se encuentren en redes, soportes, sistemas de tratamientos de datos o información, sus partes o componentes será*

condenado a pena de prisión de uno (1) a cuatro (4) años.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2. Se añade el artículo 241-B al Código Penal, el cual rezará así:

Artículo 241-B: El que con el ánimo de apoderarse, copiar, usar o conocer indebidamente información contenida o en tránsito en un sistema de tratamiento de datos o información, interfiera o acceda a él, será condenado a pena de prisión de dos (2) a cuatro (4) años.

Artículo 3. Se añade el artículo 241-C al Código Penal, el cual rezará así:

Artículo 241-C: El que con dolo altere, dañe o destruya los datos contenidos o en tránsito en un sistema de tratamiento de datos o información, será condenado a pena de prisión de dos (2) a seis (6) años.

Artículo 4. Se añade el artículo 241-D al Código Penal, el cual rezará así:

Artículo 241-D: El que con culpa revele o difunda los

datos sensibles contenidos en un sistema de datos o información o aquellos cuya difusión esté prohibida por mandato legal, será condenado a pena de prisión de uno (1) a tres (3) años. Si en la revelación o difusión de datos, media el dolo, la pena será de dos (2) a seis (6) años de prisión.

Artículo 5. Se añade el artículo 241-E al Código Penal, el cual rezará así:

Artículo 241-E: Cuando el agente que incurra en las conductas tipificadas artículos 241-A, 241-B, 241-C, 241-D, es el responsable del sistema de tratamiento de datos, información o red de informática o la realizó utilizando información privilegiada, la pena aplicable será la máxima establecida para cada caso.

De las disposiciones anteriores del Anteproyecto No. 34 de 2001, se aprecia que el artículo 241-A, hacía referencia a la incriminación del delito de sabotaje informático, ya que establece como conductas punibles "destruir, inutilizar o dañar" el funcionamiento de sistemas de tratamiento de datos o información, sus partes o componentes, así como programas y documentos electrónicos ajenos que se encontrasen en redes, soportes, sistemas de tratamientos de datos o información, sus partes o componentes", sin embargo

es lamentable que el legislador no hubiera mostrado interés en la aprobación final de esta propuesta legislativa, ya que su inclusión no solo tipificaba el delito de sabotaje informático sino también tutelaba la intimidad frente el acceso no autorizado a una base de datos con el fin de revelar secretos y de manera acertada aumentaba la pena para casos específicos, pero especialmente frente al caso de quien fuera el que hacia alguna conducta establecida en el anteproyecto era el encargado o responsable se le aumentaba la pena considerablemente.

Ahora bien el Código Penal de 1982, no contempló los delitos relacionados con la informática, sin embargo, posteriormente, se adicionaron algunos delitos, tales como por ejemplo, los relativos a la pornografía infantil cuya existencia se debe a la proliferación de este contenido ilegal en Internet.

En lo que respecta a los Anteproyectos de Código Penal de 1998, los comisionados Ana Belfon, José Juan Ceballos y Luis Carlos Cabezas incluyeron en los Delitos contra el patrimonio en el artículo 173 una forma agravada del delito de daños que en parte se asemeja al sabotaje informático, la norma reza de la siguiente manera:

> *"Artículo 173: Se sancionará con pena de seis (6) meses a tres (3) años de prisión o su equivalente en días –multa o arresto de fines de semana, si el delito se comete:*
>
> *Contra un servidor público, a causa del ejercicio de sus funciones;*

Con Destruccion o grave dano en residencia oficina particular edificio publico o destinado a uso publico o al ejercicio de algun culto en una nave o aeronave del estado monumento publico cementerio cosa de valor cientifico cultural historico o artistico

En una plantacion sementera o en las cercas protectoras de fundos agricolas o pecuarios

Mediante utilizacion de sustancia venenosa o corrosiva

Mediante destruccion alteracion o inutilizacion de datos programas electronicos o informacion contenida en red soporte o sistema informatico

El Anteproyecto de Código Penal revisado de 1999 incluyo tal como lo hiciera en su momento el Anteproyecto de Codigo Penal de 1998 una norma agravante para el delito de daños la cual era similar al sabotaje informatico

Esa agravante al delito de daños estaba contenida en el articulo 225 del Anteproyecto de Código Penal Revisado de 1999

El texto del articulo 225 del Código Penal revisado de 1999 lo establece de la siguiente manera

Articulo 225 El que destruya inutilice rompa o dañe cosas muebles o inmuebles que pertenezcan a otro se

sancionará con pena de dos (2) a cuatro (4) años de prisión si el delito se comete:

a. En perjuicio de un servidor público, a causa del ejercicio de sus funciones;

b. Mediante amenaza o violencia contra tercero;

c. Con destrucción o grave daño en residencia, oficina particular, edificio público o privado, o destinado al ejercicio de algún culto; en vehículos; en una nave o aeronave, monumento público, cementerio, cosa de valor científico, cultural, histórico o artístico;

d. En una plantación, sementera, o en las cercas protectoras de fundos agrícolas o pecuarios;

e. Mediante la utilización de sustancia venenosa o corrosiva;

f. Mediante la destrucción, alteración, o inutilización de datos, programas electrónicos o información contenida en red, soporte o sistema informático."

2 1 1 2 2 La delincuencia informática en el Código Penal de 2007

Al partir del Codigo de 2007 es cuando efectivamente el legislador panameno demuestra preocupacion por esta nueva forma de criminalidad al ser actualizado el Codigo para que incluyese diversas normas relacionadas con las tecnologias de la información y la comunicacion Esto causo que el Codigo Penal de 2007 tuviese normas relativas a una diversidad de delitos por medios informáticos como también la tipificación especifica de los delitos que atentan contra la seguridad informática

El Codigo Penal de 2007 no obstante no contempla de manera estricta ni individualizada el sabotaje informático y en el caso de los Delitos contra la Seguridad Informática ni siquiera se hace alusion al mismo pues esas normas de seguridad informática, lo que persiguen castigar es el acceso no autorizado tutelando asi el derecho a la intimidad frente a las conductas de intruismo o hacking mas que tutelar el patrimonio frente a las numerosas conductas que lo afectan como por ejemplo el fraude electrónico o el sabotaje informático

A continuación citamos las disposiciones referentes a los delitos contra la Seguridad Informática en el titulo VIII Delitos contra la seguridad juridica de los medios electrónicos capitulo I Delitos contra la seguridad informatica

Articulo 285 Quien indebidamente ingrese o utilice una base de datos red o sistema informatico sera sancionada

con dos a cuatro años de prisión.

Artículo 286. Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión.

Artículo 287. Las conductas descritas en los artículos 285 y 286 se agravarán de un tercio a una sexta parte

de la pena si se cometen contra datos contenidos en bases de datos o sistema informático de:

1. Oficinas públicas o bajo su tutela.

2. Instituciones públicas, privadas o mixtas que presten servicio público.

3. Bancos, aseguradoras y demás instituciones financieras y bursátiles.

También se agravará la pena en la forma prevista en este artículo cuando los hechos sean cometidos con fines lucrativos.

Estas sanciones se aplicarán sin perjuicio de las sanciones aplicables si los datos de que trata el presente

capítulo consiste en información confidencial de acceso restringido, referente a la seguridad del Estado, según lo dispuesto en el Capítulo I, Título XIV, del libro segundo de este Código.

Artículo 288. Si las conductas descritas en el presente capítulo las comete la persona encargada o responsable de la base o del sistema informático o la persona autorizada para acceder a este, o las cometió utilizando información privilegiada, la sanción se agravará entre una sexta y una tercera parte.

2.1.2 Nociones sobre delincuencia informática

2.1.2.1 Concepto de Delincuencia Informática

Es necesario como punto de partida en este punto destacar que la denominación "delito informático" o "delitos informáticos" apenas aportan en la actualidad una mínima precisión unificadora desde el punto de vista criminológico, dogmático, política criminal y de política legislativa, toda vez que esta noción abarca una variedad de conductas delictivas que atentan contra una pluralidad y diversidad de bienes jurídico como bien

anota ROMEO CASABONA (Romeo Casabona 2006 8)

Se ha indicado que el concepto de delito informatico es un concepto de naturaleza doctrinal asi lo establece GALAN MUNOZ al decir que el concepto de delito informático es un concepto de naturaleza claramente doctrinal y no legal habiendose desarrollado definiciones del mismo de una enorme amplitud con la unica pretension de dar cabida en su seno a todas las posibles figuras delictivas que tuviesen o pudiesen tener una conexion con el uso de sistemas de tratamiento electronico de datos (Galan Muñoz 2005 30)

Para la doctrina el establecer una definición para delito informatico ha variado en la creacion de esta, algunas corrientes las hacen amplias y otros en cambio prefieren una definicion mas restrictiva frente al contenido de lo que seria el delito informatico

Serian amplias aquellas que dentro de su concepto incluyan cualquier acto que este relacionado con un proceso electronico de datos necesariamente incluyendo no solo los actos que involucren una computadora sino aquellas donde el objeto de la accion es del tipo informático

Asi por ejemplo la definición aportada por VILLALOBOS en su diccionario de Derecho Informático es del fundamento amplio al decir que serian delitos informáticos Todas aquellas conductas ilicitas susceptibles de ser sancionada por el derecho penal que hacen uso indebido de cualquier medio informatico Se pueden definir como todos aquellos actos ilicitos que en perjuicio de terceros son realizados con empleo de un

equipo informático". (Villalobos, 2002:57)

En palabras similares MORANT VIDAL, lo define como, "aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico o que afectan al funcionamiento de los sistemas informáticos". (Morant Vidal, 2003:42)

GUERRA DE VILLALAZ, ha señalado sobre esta materia que, se trata de hechos realizados por personas que se encuentran vinculados al manejo de la informática que hacen mal uso o se aprovechan de estos nuevos inventos o adelantos tecnológicos, para afectar bienes jurídicos tutelados. (Cfr. Guerra de Villalaz, 1993:175)

Por su parte LUZ CLARA, define delito informático, siguiendo lo establecido por el Departamento de Justicia de los Estados Unidos, estableciendo que, "es cualquier acto ilegal en relación con el cual, el conocimiento de la tecnología informática sea esencial para su comisión, investigación y persecución" (Luz Clara 2001:118), en la misma idea ESTRADA y SOMELLERA, lo definen como, "el acto en el cual interviene un sistema de cómputo como utensilio en la producción de un hecho criminológico, en donde se atenta contra los derechos y libertades de los ciudadanos". (Estrada y Somellera, 1998:42)

Las definiciones señaladas difieren muy poco de la principal definición del delito relacionado con ordenadores (o computer related crime en inglés), por ser que en 1983 la Organización para la Cooperación y Desarrollo Económico (OCDE), en París reúne a diferentes expertos los cuales lo definen como cualquier comportamiento antijurídico, no

etico o no autorizado relacionado con el procesado automatico de datos y/o transmisiones de datos

Sobre la definición de delito relacionado con ordenadores segun la OCDE estima SIEBER que la amplitud de este concepto es ventajosa puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales criminologicos económicos preventivos o legales donde concluye que la definicion permite a cada rama y disciplina ligada a este tema tomar para asi lo hechos que causen problemas especificos para su disciplina (Sieber 1986 en Mir Puig 1992 66)

Igual postura a la de SIEBER sobre la definicion de la OCDE sigue PALAZZI al decir que las ventajas de la amplitud de esta definicion de la OCDE que nosotros adoptamos son evidentes Permiten abarcar un interesante campo de estudio que no sólo se limita al delito informatico sino a toda la delincuencia relacionada con la informatica y las nuevas tecnologias (Palazzi 2000 39)

En cambio una definicion restrictiva, como supone el nombre busca reducir la amplitud del concepto de delito informático estas evitan introducir dentro del concepto mención de aquellas conductas donde su unico elemento informatico sea la naturaleza del objeto de la acción

En defensa de una postura restrictiva se puede observar la postura de CAMACHO LOSA que al definir delito informatico expresa no considero que deban incluirse dentro de este concepto aquellos hechos en los que los dispositivos informaticos son

objeto de un delito de los tipificados en el Código Penal, como es el caso de la sustracción de material hardware, ya que en mi opinión este tipo de hechos no reúnen las características diferenciadoras del delito informático, y su relación con la informática es un mero accidente". (Camacho Losa, 1987:25)

Por su parte CRUZ DE PABLO define el delito informático como "aquellas conductas típicas, antijurídicas, culpables y debidamente sancionadas por el ordenamiento jurídico penal para cuya ejecución se valen de ordenadores, computadoras o cualquier otro mecanismo electrónico o informático, bien como medio, bien como fin, o mediante el uso indebido de los mismos". (Cruz de Pablo, 2006:20)

MORALES GARCIA considera que por ser un sector no definido de la sociedad, es provechoso utilizar como definición términos que resulten generales, poco estrictos para enmarcar todo riesgo a la sociedad, así entonces utilizando la definición propuesta por SIEBER definiendo la delincuencia informática como "cualquier comportamiento ilegal, al margen de la ética o realizando sin autorización en el marco del proceso de transmisión de datos". (Morales García, 2005:395)

A juicio de DAVARA RODRIGUEZ, la definición de delito informático debe darse como, "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software". (Davará Rodríguez, 2003:350)

ROMEO CASABONA al analizar la materia que nos ocupa, considera que el Derecho Penal se enfrenta a una criminalidad progresivamente más poderosa y peligrosa desde muchos puntos de vista a la que aquél no debe renunciar a darle la respuesta que sea necesaria Al mismo tiempo se acrecienta la complejidad tecnica y juridica con el efecto subsiguiente de que las construcciones juridico penales elaboradas a lo largo de las ultimas décadas no siempre pueden adaptarse a las caracteristicas de estas tecnologias ni a las manifestaciones criminales que propicia (Romeo Casabona op cit 4)

Por lo que respecta al llamado cibercrimen o ciberdelito y su relación con el delito informatico es necesario lograr distinguir entre ambos asi se necesita establecer que estos nacen de las distintas posibilidades juridicas que nacen por razón de los nuevos recursos técnicos que supone el Internet en si

Así es posible la ilimitada transferencia, flujo y comunicacion de la informacion como tambien el ofrecimiento de cualquier servicio sin importar el espacio donde se efectua, ni mucho menos el lugar donde se percibira el beneficio del servicio causado esa libertad de acceso y de puesta de información su trato y manipulación lo que supone entonces nuevas conductas criminales relacionadas al Internet

En opinion de ROMEO CASABONA sobre aquellas nuevas conductas relacionadas en si con el desarrollo de la Internet considera que la posibilidad de difundir contenidos ilicitos de dispar significación y la reproduccion e intercambio de obras musicales y cinematográficas etc documentos confidenciales situados en

cualquier lugar del planeta permiten calificar las Tecnologias de la informacion y comunicacion como instrumentos muy potentes para la comisión de delitos de muy diversa naturaleza y considerar a estos como una de las consecuencias de la globalizacion (Romeo Casabona op cit 8)

Frente a estas nuevas conductas que aunque en principio pudiesen ser clasificadas dentro de los delitos informaticos se prefiere hablar de esta nueva generación de delincuencia informática vinculada con las tecnologias de la información y comunicación en especifico de la combinación de los sistemas informaticos y telemáticos como cibercrimen o ciberdelito termino aceptado internacionalmente

Para ROMEO CASABONA el cibercrimen se debe entender como el conjunto de conductas relativas al acceso apropiacion intercambio y puesta a disposicion de informacion en redes telematicas las cuales constituyen su entorno comisivo perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilicito pudiendo afectar a bienes juridicos diversos de naturaleza individual o supraindividual (Romeo Casabona op cit 9)

La importancia o no de la construcción del termino cibercrimen frente a los delitos informaticos en si desde el punto penal resulta interesante aunque por su parte ROMEO CASABONA le resta importancia considerando que desde un punto de vista tecnico juridico tampoco parece sin embargo que el término cibercrimen pueda llegar a satisfacer plenamente una función dogmatica de integracion de estos delitos de nueva

generación sin perjuicio de que desde planteamientos criminologicos pueda ser adecuado para cumplir una funcion descriptiva o de identificacion de un fenomeno criminal singular y el espacio virtual en el que se manifiesta pues presenta unos perfiles diferentes respecto a lo que se venia entendiendo por delito o delitos informáticos y desde luego a cualesquiera otros delitos (Romeo Casabona su cit 9)

Asi entonces aunque no exista uniformidad de como nombrar o distinguir entre estas conductas en la practica la falta de un concepto dogmatico de delito o delitos informáticos o de cibercrimen o ciberdelito no afecta en nada para poder hacer distinción entre innumerables conductas criminales relacionadas con la informatica, asi las conductas caracterizadas por ser perpetradas en torno a sistemas informaticos en los que la red de ser utilizada, resulta tener importancia limitada o secundaria para las características de la conducta delictiva, serian consideradas dentro de la categoría de los delitos informaticos en cambio si la conducta ocurre frente redes telematicas (abiertas cerradas o de acceso restringido) siendo en estos casos los sistemas informáticos más instrumentales o secundarios para el delito estariamos en presencia de un cibercrimen o ciberdelito (Cfr Jiménez Villarejo 2009 16)

Igual de importante a la distincion que se da entre el cibercrimen y el ciberdelito es necesario considerar lo postulado por WALDEN quien es de la opinión que indistintamente de como se quiera distinguir estas conductas todo Estado que desee tratar este tema, debe correctamente identificar las diferentes formas de conductas criminales

relacionadas con las tecnologias de la información y comunicacion no solo por lo que respecta al derecho sustantivo (Derecho Penal principalmente) sino también facilitar la investigacion y el posterior enjuiciamiento de aquellas conductas lo que resulta ser un problema del procedimiento penal en si por lo que fallar en la construccion de la fase procesal afecte el sentido de la norma penal (Cfr Walden 2007 42)

2 1 2.2 Clasificación de la Delincuencia Informática.

La doctrina penal ha utilizado diferentes criterios al momento de tratar de clasificar este tipo de criminalidad y se puede a observar que los autores siguen diversos criterios unos lo hacen de manera amplia y otros con un criterio restringido hay algunos que presentan la clasificacion en atencion a como sea utilizada la computadora, entre otros

A continuacion pasaremos a abordar las diversas clasificaciones sobre delitos informáticos que nos permitirian reconocer que estamos ante una compleja criminalidad que esta en constante transformacion no sin antes señalar que en el caso de nuestro pais legislativamente el Código Penal del 2007 en su gran mayoria los ubica como delitos cometidos por medio del sistema informático y en menor medida se destina una proteccion a los delitos contra el sistema informático los llamados Delitos contra la seguridad informática, los cuales se refieren mas que nada al intruismo o hacking en

general

1 Clasificacion de SIEBER y SALT

Los delitos informaticos se pueden agrupar en delitos de caracter economico y delitos informáticos contra la privacidad entendiendo como los primeros los fraudes contenidos a traves de la manipulación de sistemas informáticos la copia ilegal de software y espionaje informático el sabotaje informatico el robo de uso de sistema informático y el acceso sin autorizacion a sistemas mientras que los delitos contra la privacidad son aquellas que a través de los medios informáticos pueden afectar la privacidad del ciudadano

Partidarios de seguir la postura de SIEBER como veremos más adelante son ABOSO y ZAPATA como también GUTIERREZ FRANCES y CHOCLAN MONTALVO (Cfr Choclan Montalvo 2001 314)

a Fraudes informaticos o manipulaciones al ordenador

Los fraudes informaticos es una forma de criminalidad muy frecuente en la que se realizan modificaciones se crean o cambian los datos contenidos en sistemas informaticos realizados por empleados de las empresas con fines de enriquecimiento personal o de obtener ganancias indebidas (Cfr Sieber 1982 en Mir Puig 1992 15 y SALT 1997 51)

Así se puede mencionar el caso de un empleado de banco que tenía acceso a las terminales de computadoras del mismo, y que en varias ocasiones transfirió a través del sistema informático fondos de distintas cuenta a su cuenta personal, y posteriormente retiro el dinero, o casos como manipular el pago de sueldos y facturas, pagos injustificados de subsidios infantiles y de rentas, manipulación de la existencia de mercancía o la elaboración del balance.

En opinión de GUTIERREZ FRANCES, lo informático del fraude esta en el aprovechamiento, utilización o abuso de las características funcionales de los sistemas informáticos como instrumento para realizar una conducta astuta, engañosa, artera, subrepticia "con animus decipiendi, de un modo de obrar intencional...", estableciendo que la defraudación informática (fraude informático) sería la causación de un perjuicio económico no necesariamente individual en sentido microsocial individualista irrogado mediante un comportamiento astuto, supersticioso o engañoso, es decir un medio fraudulento, que en este caso sería la propia manipulación informática. (Gutiérrez Frances, 1991:111)

Con toda razón, ABOSO y ZAPATA, establecen que en la actualidad, "esta clase de delincuencia informática registra la participación de grupos criminales dedicados a la explotación ilícita de de este tipo de modalidad delictiva que incluye la duplicación de tarjetas magnéticas y la manipulación de la información original para su posterior uso ilegitimo", haciendo la aclaración también que este abuso no solo se refiere a la

duplicación de tarjetas magnéticas de bancos, sino que igualmente abarcan con igual fuerza las tarjetas telefónicas y el uso indebido de las redes de telecomunicación. (Aboso y Zapata, 2006:48)

La manipulación del ordenador se puede manifestar de diferentes formas, según SIEBER, "el autor puede en principio introducir datos falsos en el ordenador (manipulaciones del input), puede alterar el orden del proceso (manipulaciones del programa y de la consola), o bien puede posteriormente falsear el resultado, inicialmente correcto, obtenido del ordenador (manipulaciones del output)". (Sieber, op. cit.:16)

a.2 Formas de Fraude Informático

Se conciben diferentes maneras de realizar el fraude, así mencionamos, alterar, omitir, ingresar datos verdaderos o introducir datos falsos en un ordenador, acto conocido como manipulación de Input o en interferir en el procesamiento de la información alterando el programa o secuela lógica con el que trabaja el ordenador, modalidad que exige conocimientos especiales en informática. (Cfr. SALT, op. cit. 58)

SIEBER a manera de ejemplo menciona el caso de un empleado de banco, de la sección de proceso de datos, que consiguió manipular el tráfico informatizado de transferencias internacionales de uno de los bancos más importantes de Suiza. El empleado, que trabajaba en el centro de calculo del banco como operador y controlador de datos, interceptó varias ordenes de transferencias dadas por sus coautores y multiplico por mil cada una de las cantidades transferidas, lo cual dio como consecuencia que

recibieran al momento de recoger el dinero una suma mayor de la que les correspondía. Solo después de averiguaciones que resultaron ser extremadamente difíciles, fue posible apresar y juzgar a los sujetos que participaron en estas manipulaciones. (Sieber, op. cit.: 17)

El mismo SIEBER, sostiene que a través de manipulaciones del programa, el agente puede modificar los programas de la empresa o cambiar, con la ayuda de los programas que el ha hecho, los datos almacenados en el banco de datos, y para ello cita el caso de un individuo que laboraba como programador en una sociedad anónima alemana y con la ayuda de un programa elaborado por el, intercaló datos, que contenía los datos de los saldos de los sueldos de la empresa, los datos del sueldo de personas ficticias, e indico su propia cuenta para que le transfiriesen los sueldos de dichas personas. (Sieber, op. cit.: 18)

Así mismo, existen las denominadas manipulaciones de consola, las que no tienen como objeto manipular el programa, sino más bien los elementos del servicio mecánico de la instalación del proceso de datos, se señala como ejemplo de el caso ocurrido en un banco, en virtud del cual los autores con el fin de encubrir determinados negocios de especulación de divisas, consiguieron oprimir la tecla de interrupción, situada en la consola del mini ordenador, evitando así que se registrará en el ordenador principal las pérdidas, dejando de contabilizar o bien no contabilizando correctamente, cantidades de millones de dólares.

Otras formas de manipulacion informatica constituyen las manipulaciones del output (cfr Sieber op cit 21) que consisten en producir cambios en los datos anteriormente procesados es decir falsear el resultado inicialmente correcto obtenido por un ordenador (cfr Salt op cit 52) asi como los abusos especiales en tiempo compartido Time Sharing y teleproceso en el cual las manipulaciones en este ultimo caso son efectuadas solo por los empleados sino tambien por otros usuarios que utilizan los ordenadores conjuntamente o de personas que acceden al mismo teleproceso

Asi por ejemplo esta la manipulacion efectuada por un joven norteamericano en los años sesenta que se introdujo mediante la red publica de telefonos en el ordenador central de la Pacific Telephone Corporation e indujo a esta al envio de mercancia de forma gratuita por valor de aproximadamente un millón de dólares

a 3 Problemas penales del Fraude Informatico y Tendencias legislativas

Ahora bien los problemas que se presentan en el ambito juridico penal ante la ausencia de una disposición especial referida a esta clase de actos ha contribuido a que la doctrina haya insistido en la creacion de tipos penales destinados a proteger de manera especial a la sociedad contra estos hechos ilicitos

En este contexto en la legislación estadounidense tanto a nivel federal como estatal se han adoptado disposiciones para enfrentar esta criminalidad castigando entre otros los delitos financieros ocasionados por delincuencia informatica la sustracción de información acceso a sistema de informacion con finalidad de conocer copiar o

apropiarse de la informacion ajena los delitos de acceso y uso no autorizado los delitos relativos a los sistemas electronicos de transferencia de fondos entre otros (Gutiérrez Frances op cit 350)

De igual forma a nivel europeo existen legislaciones penales especiales para afrontar esta delincuencia electronica castigando en Alemania por ejemplo el delito de Estafa Informatica o a traves de ordenador el delito de falsificacion de datos susceptibles de servir de prueba en Suecia el acceso a un registro de procesamiento automatico de datos o que altere o destruya ilegalmente introduzca un registro semejante en su archivo entre otros

A manera de conclusión es importante destacar la necesidad de adoptar una legislacion que se adecue a la criminalidad informatica tomando en consideración por los bienes juridicos que quedan afectados por su realizacion ilicita bienes juridicos de caracter patrimonial (Cfr Romeo Casabona, 1987 114)

b Copia ilegal de software y espionaje informático

Segun ABOSO y ZAPATA en este grupo se incluyen las conductas dirigidas a obtener datos en forma ilegitima, de un sistema de informacion agregan que es comun el apoderamiento de datos de investigaciones listas de clientes balances etc En muchos casos el objeto de apoderamiento es el mismo programa de computacion (software) que suele tener un importante valor economico (Aboso y Zapata, op cit 49)

b 1 Copia Ilegal de Software

Sobre la copia ilegal de software tenemos que consiste en reproducir o copiar un programa de ordenador sin autorizacion generalmente por los propios usuarios y constituye a su vez una de las formas de espionaje informatico de mayor importancia que provoca graves daños a los autores y productores de los mismos

La copia ilegal de software es tambien denominada como pirateria de software y esta protegida en leyes especiales sobre Derecho de Autor o en códigos penales a traves de la Propiedad Intelectual asimilando estos como obras cientificas que exigen una protección penal para proteger los derechos de explotacion de los autores aunque como haya indicado ROMEO CASABONA tal garantia se efectua primando los intereses de los cesionarios de esos derechos por ejemplo las empresas de explotación y comercialización del software en detrimento del autor aunque trabaje para una empresa y de los usuarios de los programas (Cfr Romeo Casabona 1987 152)

b 2 Espionaje Informatico o copia de ficheros o bases de datos

Por lo que respecta al espionaje informático o espionaje de datos se trata de conductas encaminadas a la obtencion de datos de manera ilegitima de un sistema de información tales como listas de clientes balances datos de investigaciones etc infracciones cometidas en ocasiones con fines de extorsionar cometer sabotaje industrial militar o politico o simplemente espionaje industrial

En estos casos el agente puede copiar el fichero sin destruirlo ni alterar la información original, ya sea de disquette a disquette, ya la visión de la pantalla o accediendo ilícitamente al sistema en la que se duplica o copia información lesionando el derecho de exclusividad del propietario, que será posible su castigo a través de la estafa cuando persiga animo de lucro, se engañe al propietario o al encargado del sistema para que proporcione una copia o permita el acceso al elemento lógico pretendido, o en su defecto la revelación de secretos, o también cuando se copie destruyendo o no la información general, que en este último caso puede sancionarse como delito de hurto, robo o apropiación indebida, aunque doctrinalmente sea discutible el alcance penal de estas figuras en otras formas, tomando el criterio de la corporalidad, tangibilidad y apreciabilidad aunque en la actualidad en algunos países tienen su protección especial. (cfr. González Rus, 1999:120)

A manera de conclusión el espionaje informático o la copia de ficheros o bases de datos, constituye en ocasiones hechos ya contemplados legislativamente, tal como se ha indicado, pero por ser este delito tan específico es necesario establecer claramente una delimitación a fin de no confundirlo con una mera revelación de secretos (cfr. Romeo Casabona op. cit.: 171 y 172). Por lo que nos sumamos a las propuestas de reforma legislativa entorno a esta materia.

c. Sabotaje Informático

Se entiende por sabotaje informático aquellos ilícitos que consisten en la destrucción o el daño que se produce al sistema informático, ya sea el hardware o el software.

En este sentido, se mencionan los incendios intencionales o bombazos que se dirigen contra centros computacionales, las bombas lógicas, que provocan destrucción de archivos, el sabotaje encubierto, los daños maliciosos, destrucción con martillo, armas de fuego etc.

Según ABOSO y ZAPATA, "el sabotaje informático (Computersabotage) se ha transformado en una de las actividades ilícitas más extendidas en el marco de la delincuencia informática"; estableciendo que, "para ello acude al recurso del llamado "programa gusano" o "virus informático", que afecta el uso correcto del sistema o lo ralentiza.", es necesario tener en cuenta que debido a que en la actualidad el mundo cada vez más es dependiente de sistemas informáticos, el sabotaje informático resulta ser una conducta que con muy poco esfuerzo puede causar innumerables perjuicios, no en vano consideran que "la pérdida de información almacenada y la afectación de los procesos de comunicación de datos constituyen el talón de Aquiles de nuestra moderna sociedad". (Aboso y Zapata, op. cit.:49)

d. robo de servicios o de uso de sistema informáticos

En cuanto al robo de uso debe señalarse que no integra ningún comportamiento

delictivo ya que hay ausencia de apropiarse la cosa salvo que el sujeto tenga como intención no solamente el uso sino el apoderamiento

El individuo utiliza los ordenadores y los programas informaticos sin autorizacion vgr los empleados utilizan los ordenadores como tambien los sistemas de proceso de datos y los programas para lograr un fin privado produciendo asi un perjuicio economico (SALT op cit 52)

En opinion de SIEBER el hurto de tiempo no implica una peligrosidad especial más bien se trata de dañar a la empresa por abuso y el costo que tiene que pagar por el alquiler del ordenador o en los casos que el autor atrae el cliente a su empresa

Esto dentro de las agresiones al soporte material informatico se encuentra el hurto de tiempo este no implica la traslación del aparato sino mas bien utilizar sus servicios sin autorizacion valiendose gratuitamente y sin autorizacion hecho que no tiene la consideración de un ilicito penal pero si civil

Tambien se ha denominado hurto de uso porque el individuo utiliza el ordenador para tareas extrañas simple diversion etc actividad reparable que consiste en el uso distinto al autorizado pero que es impune por la ausencia del animo de apoderarse de la cosa (Cfr Gonzalez Rus (op cit 119)

e Acceso sin autorización a sistemas

A diferencia de las anteriores el sujeto accede a un sistema de datos a traves de un proceso de datos a distancia sin fines fraudulentos ni de espionaje o sabotaje

informático vgr los denominados piratas juveniles que se introducen en los sistemas informaticos solo por el reto de vencer el sistema de seguridad o de curiosidad o como formar de adquirir notoriedad en la prensa

Segun ABOSO y ZAPATA el denominado Computerhacking significa el ingresar en el sistema informatico de otro sin el proposito de manipularlo sabotearlo o espiarlo sino de pasear o interiorizarse sobre las medidas tecnicas de seguridad del sistema (Aboso y Zapata op cit 50)

2 Clasificación de GONZALES RUS

Para GONZALEZ RUS los ilicitos patrimoniales relacionados con medios o procedimientos informáticos son los siguientes

a delitos contra el sistema informaticos

Dentro de esta categoria se ubican aquellos ilicitos donde el sistema o sus elementos son el objeto directo de ataque el eventual objeto material en la cual las actividades ilicitas recae sobre hechos punibles previstos en la ley (hurto apropiacion indebida, daños descubrimiento y revelacion de secretos) y otros que tienen un caracter netamente informático como son el hurto de tiempo hurto de software apropiación o destruccion de datos

La anterior clasificación permite agrupar los delitos en dos vertientes asi seran aquello hechos punibles referidos a los elementos fisicos del sistema informático (hardware monitores dispositivos de almacenamiento soportes de almacenamiento

disquetes cintas discos de comunicacion etc y a elementos lógicos (ficheros de datos y no programas) del sistema informatico

Asi cabe mencionar que JIJENA LEIVA señala que los delitos contra el sistema informatico o delitos contra los medios informáticos son aquellos que afectan la información almacenada son en esencia delito especificamente informático en donde el legislador lo que busca es tutelar el contenido de la informacion de un sistema de tratamiento automatizado de la misma y no el hardware o soporte tecnológico en que aquel almacena (Cfr Jijena Leiva, 1992 83)

b delitos cometidos por medio del sistema informático

El sistema informático es en muchas ocasiones el instrumento o medio que se vale el agente para realizar su comportamiento punible

Los delitos en este ultimo caso de dividen en delitos para cuya realizacion se utiliza el sistema informatico a traves de diversas manipulaciones del soporte logico o mediante la utilizacion delictiva de los datos y programas del sistema que revisten una particularidad al emplear estos medios y que pueden concretar estafas falsificaciones etc

c Delitos posibles solo con los medios informáticos

En el cual el agente utiliza el banco de datos para atentar contra la intimidad personal el acceso a la informacion informática y libertades publicas (fr González Rus op cit 117)

3) Clasificación de ESTRADA y SOMELLERA.

La postura de ESTRADA y SOMELLERA, frente a la clasificación de los delitos informáticos, merece ser detallada no solo por lo extensa que es, sino por ser muestra clara de los peligros que supone para el legislador ser muy taxativo al tratar de tipificar conductas que puedan ser calificadas como delito informático, como también por el hecho de que nos decantamos por una distinción de los delitos informáticos siguiendo las ideas de SIEBER. (Cfr. Estrada y Somellera, 1998: 425 a 431)

Aun así el gran valor Doctrinal de ESTRADA y SOMELLERA, no descansa en sí en la clasificación sino en el contenido de esta, donde presentan muy detenidamente aquellas conductas que pueden ser clasificadas como delito informático, conductas como :

a. la Infiltración en las redes Computacionales

> La conducta del hacker, aquel que utiliza las herramientas de software instaladas en una computadora, con el fin de introducirse dentro de cualquier computadora del mundo, actuando sin la autorización del titular de esta, roban información, plantan algún virus informático o sino conductas poco perjudiciales, como cambiar las claves de los usuarios de la computadora, como también sus nombres.
>
> Para ESTRADA y SOMELLERA, es importante tener claro

que respecto a este delito se puede clasifica o castigar de acuerdo a la magnitud del dano ocasionado si hablamos de algo como cambiar el password de algun usuario no se le puede castigar de la misma manera que aquel que roba información confidencial o planta algun virus que daña todo un sistema por lo que el castigo debe ser proporcional a la conducta y perjuicio realizado por esta (Estrada y Somellera su cit 426)

b La infraccion de los derechos de autor

Debido a que no hay clara interpretacion de los conceptos de copia, distribución cesion y comunicacion publica de los programas de la computadora utilizando la internet el problema de la responsabilidad o no del propietario de un servicio en linea o de un operador se observa la practica de advertir y reservarse una cláusula extracontractual que exonera al propietario de la responsabilidad frente a quien suba o de upload de un programa o fichero que infrinja los derechos de autor de un tercero

c La infracción del copyright de bases de datos

Esto se refiere a la falta de uniformidad de proteccion de las

bases de datos en países con acceso al internet, lo que hace que se tenga que tener controles de protección como el de tipo contractual donde el propietario de la base de datos, solo permite a los usuarios descargar archivos o selecciones específicas, mientras que se reserva para sí la base de datos y prohíbe su copia, como también la copia masiva de su información.

d. La interceptación de e-mail

Para estos casos se debe entender que el objeto material en los delitos que tutelan la inviolabilidad de la correspondencia, este no solo se referirá a las cartas o despachos telegráficos, también los correos electrónicos, hasta el punto de ser considerado el hecho de simplemente observar a través del soporte físico el contenido de un correo, así es tutelada la violación de la correspondencia no solo en los casos comunes sino también en un correo electrónico.

e. Las estafas electrónicas

El problema del comercio electrónico, y específicamente las compras por internet, permite la proliferación de diversas conductas que se configuran en un delito de estafa, pero en la mayoría de los

casos resulta necesario darle un enfoque nuevo la legislacion a fin de correctamente tipificar la estafa donde se utilice una computadora para facilitar su comision

f Piratería Informática o Hackers

Segun ESTRADA y SOMELLERA este tipo de delincuente aprovecha 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 Especialmente se trata de introducir en aquellos sistemas que necesitan un nombre de usuario y algun tipo de contraseña como tambien de alguna contraseña establecida dentro del mismo sistema para su mantenimiento a fin de que estando a distancia de aquella computadora en la que se introduce pueda lograr su cometido utilizando diversos metodos como la bomba lógica los gusanos y virus etc (Estrada y Somellera, op cit 427)

g La bomba lógica o cronologica

Este delito supone un grado de especializacion en el criminal ya que este deberá programar la destrucción o modificación de datos del sistema en el momento futuro que este desee Mientras que los

virus se pueden detectar, las bombas lógicas presentan una mayor dificultad para ubicar antes de que exploten.

No en vano ESTRADA y SOMELLERA, establecen que, "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. Así l figura de 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". (Estrada y Somellera, op. cit.:427)

h. Espionaje

El acceso no autorizado a sistemas informáticos gubernamentales, las interceptaciones de correos electrónicos de agencias de inteligencia Estatales, son los principales actos de Espionaje que se pueden lograr a través del uso de una computadora, especialmente si el que se beneficia de esta actuación es un gobierno u organización extranjera.

ı Espionaje Industrial

Si el espionaje entre estados se puede tener como una posibilidad entre empresas y grandes corporaciones la posibilidad de contratar un hacker a fin de que logre obtener información de nuevos productos estrategias de mercadeo balances y estados de cuentas de alguna corporación que sea competencia No en vano uno de los principales rubros de seguridad en que invierten las corporaciones es el de seguridad de internet debido a lo sensitivo que seria ser victima de espionaje industrial mediante computadora

ȷ Gusanos

Son aquellos programas que como un virus son preparados para ser introducidos dentro algun programa legitimo de procesamiento de datos o para modificar o destruir los datos pero difieren por el hecho de que estos no se regeneran Aunque en escala el daño de un gusano no es equiparable al de un virus es posible que un gusano cause grandes perjuicios especialmente cuando se trata de aquellos gusanos aplicados al sector bancario donde puede obligar al sistema a transferir grandes fondos al final del programa

k. Virus

Son una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada.

l. Fraude efectuado por manipulación informática

ESTRADA y SOMELLERA, sobre esta clase de actuar son de la consideración de que este "delito que aprovecha las repeticiones automáticas de los procesos de un 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". (Estrada y Somellera, op. cit.:428)

m. manipulación de datos de salida

Este delito se efectua fijando un objetivo al funcionamiento del sistema informático, como aquellos delitos relacionados a tarjetas de créditos donde se alteran el contenido de la cinta magnética de una tarjeta, como también los datos de alguna tarjeta de crédito, a fin de poder aprovecharse de los datos introducidos.

n manipulacion de programas

La conducta aqui se desarrolla al modificar un programa existente en un sistema informatico o en insertar nuevos programas o rutinas Asi por ejemplo el famoso metodo del caballo de troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informatico para que pueda realizar una funcion no autorizada al mismo tiempo que su función normal Por su naturaleza se entiende que es necesario tener conocimientos especializados en informatica para lograr crear y manipular las instrucciones introducidas en un programa

o manipulación de datos de entrada

Este fraude tambien conocido como la sustraccion de datos representa el delito informatico mas comun por lo facil de cometer y descubrir Delito que no necesita que el autor tenga conocimientos especiales en informática, sino simplemente acceso al procesamiento de datos en la fase de adquisicion de los mismos

p pirateria de software

La pirateria de software representa como delito informatico

uno de los que más perjuicio causa, ya que debido a la copia de un programa y su posterior venta, se logra vender muy fácilmente a menor precio las copias del programa, este delito supone usualmente que solo se persigue al gran pirata no al pequeño, estas conductas no solo perjudican al titular del programa, sino también al usuario que no tiene verdadera garantía del funcionamiento del programa, y los beneficios adicionales que tendría si fuese original.

q. pornografía infantil

Indistintamente a que este en el Internet o no, la pornografía infantil es ilegal, pero por más que se intente detener aquellos delincuentes que posean este material, siempre aparecen diversos medios, sitios o personas que facilitan el obtener imágenes de niños con poca ropa o en diferentes actos sexuales. La pornografía infantil y su relación con el Internet, ha sido fuerza impulsadora de diversas políticas de cooperación internacional a fin de lograr llevar a juicio a cualquiera que posea intercambie o facilite pornografía infantil.

r. bombardeo de Correo Electrónico (e-mail bombing)

El programar una computadora para que envié correos

electrónicos a una direccion especifica puede lograr inundar el correo del usuario potencialmente apagar sistemas completos igualmente introducirle a un correo electronico algun tipo de virus para que al momento de que se observa este se logre hacerse con alguna informacion no autorizada o simplemente borrar todo el sistema Estas conductas son relacionas con actos de Terrorismo por su potencial capacidad para deshabilitar sistemas completos (Cfr Estrada y Somellera, op cit 428)

s password sniffers

Son programas que rastrean el nombre y clave de los usuarios de la red en el momento en que ellos ingresan poniendo en juego la seguridad El que instale un programa de este tipo puede tomar la identidad de un usuario y conectarse logrando tener accesos a documentos restringidos Asi atacando gravemente la intimidad de la persona estas conductas en algunos paises son relacionados con los robos de identidad debido a que a través de el acceso no autorizado a la identidad de un usuario el delincuente puede hacerse con los suficientes datos del usuario para causarle graves perjuicios por ser que actuara bajo el nombre del usuario especialmente afectarle

patrimonialmente haciendo compras en su nombre

t spoofing

Es el acto de disfrazar una computadora para que parezca otra desde el punto de vista electronico con el objeto de obtener acceso a un sistema que por lo regular esta restringido Delito tratado de igual manera al Password Sniffer

u el fraude con tarjeta de crédito

La utilización fraudulenta de tarjetas de crédito y la utilizacion para llamadas de tarjetas robadas a bases de datos en linea suponen grandes perjuicios mundialmente por lo que cada vez más se tratan de instaurar mayores controles para evitar la utilizacion fraudulenta de una tarjeta de crédito dentro del internet como tambien del aprovechamiento de una tarjeta de llamadas o de teléfono de manera fraudulenta, conductas ampliamente abusadas por el delincuente informatico

A su vez tambien se trata cada vez más lograr brindarle mayor proteccion a las bases de datos que contienen la informacion relativa a las tarjetas de credito y a las tarjetas de llamadas a fin de que estas

sean más seguras y se prevengan cada vez más cualquier intento de cometer un delito informático de este tipo.

4. La Clasificación de DAVARA RODRIGUEZ

Una clasificación que toma en cuenta la manipulación informática, es la que presenta DAVARA RODRIGUEZ, ya que para este el delito informático se clasifica atendiendo al fin perseguido por su autor, fin que podrá ser dos vertientes distintas, aquellas conductas que se refieren al acceso y manipulación de los datos o sino aquellas que se refieran a la manipulación de los programas, haciendo la salvedad que de acuerdo al fin que persigan las acciones, el delito informático se divide en seis categorías distintas (cfr. Davara Rodríguez op. cit.:358 y 359), a saber:

a. Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos;

Estas manipulaciones sin distinguir la manera en que se hagan, tienen como presupuesto haber sido efectuadas por alguien no autorizado para ello y suponer un beneficio para la persona que la realiza o para quien lo realiza o en perjuicio de otro.

Asi DAVARA RODRIGUEZ, establece que para este fin la manipulación puede ser cometida en cuatro fases diferentes:

1. Almacenamiento de los datos.

2. Procesamiento de los datos.

3. Retroalimentación (feedback) con resultados intermedios de los datos y.

4. Transmisión de los resultados del proceso, ya sea en el mismo ordenador a ficheros destino, ya sea por medio de comunicaciones o acceso a periféricos en los que se depositan. (Cfr. Davara Rodríguez, op. cit.:355)

b. Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello.

El acceso, malintencionado o no de una persona no autorizada para ello, que se de contra los datos almacenados en una base o soporte informático, es una realidad muy común en esta sociedad tecnológicamente avanzada, donde se aprovechan todos los medios de comunicación posibles.

DAVARA RODRIGUEZ presenta ejemplos de acceso malintencionado, conductas que traen como resultado, el obtener la lista de clientes o resultados de un competidor, el conocer la información que un tercero procesa o envía a través de medios telemáticos, el conocer la información que un tercero almacena en su computadora, o el caso de introducir programas en un ordenador a fin de que realicen una copia del contenido de este, copia de otros programas o de resultados de procesos de investigación. (Davara Rodríguez, op. cit.: 356 y 357)

Sobre este tipo de conducta establece DAVARA RODRIGUEZ que este tipo de delito podría estar clasificado en lo que denominariamos «espionaje industrial» si lo que se logra con el acceso por medios informaticos es el conocimiento de secretos industriales o actuaciones de la competencia con los que conseguir un beneficio para el delincuente y en perjuicio de otro (Davara Rodriguez op cit 357)

c Introducción de programas o rutinas en otros ordenadores para destruir información datos o programas

Sobre esta conducta establece DAVARA RODRIGUEZ que en ocasiones se realiza esta accion sin que se pueda determinar ni su origen ni su autora ni lo que es más triste su finalidad La introducción de programas o partes de programas e incluso solamente de algunas instrucciones que al ser ejecutadas producen un efecto perjudicial para el titular de los datos e informacion almacenada, puede traer consecuencias de difícil estimacion y perjuicios irreparables para el titular de los datos de los programas o del sistema Es sin duda una intromision ilegitima en un derecho basico del titular agregando sobre los virus informaticos que estos son consistentes en rutinas instrucciones o partes de programas que se introducen a traves de un soporte fisico que los contiene o a traves de la red de comunicaciones actuando en el

momento o con efecto retardado y destruyendo datos información o programas y en ocasiones toda la información contenida en el ordenador Davara Rodríguez (op cit 357)

d Utilización del ordenador y/o los programas de otra persona si autorización con el fin de obtener beneficios propios y en perjuicio de otro

Este es el caso del llamado hurto de tiempo donde se utiliza los programas o la misma computadora sin autorización con el fin de obtener beneficio propio y en perjuicio de otro ya sea en el espacio físico donde se encuentra ubicada la computadora o a traves de la red

Sobre este tipo de ilícito DAVARA RODRIGUEZ aclara que este es el caso de determinados empleados de instalaciones informáticas que utilizan los programas y el ordenador de su empresa para realizar trabajos de servicios a terceros con un evidente lucro para ambos y en perjuicio de la empresa titular de los ordenadores y programas (Davara Rodríguez op cit 358)

e Utilización del ordenador con fines fraudulentos y

Sobre esta categoría establece DAVARA RODRIGUEZ

"las posibilidades de tratamiento de la información por medios mecanizados, así como la potencia y velocidad de los cálculos que en los ordenadores se pueden realizar, permiten disponer de un elemento óptimo para la manipulación fraudulenta de datos, con la realización de complejos cálculos e, incluso, la posibilidad de enmascaramiento de información". (Davara Rodríguez, su. cit.:358)

La utilización de una computadora permite realizar cantidad innumerable de conductas fraudulentas, como el enmascaramiento de datos, cálculos complejos para eludir obligaciones fiscales, esconder información, conductas muy comunes y realizadas muy frecuentemente que usualmente no son detectadas.

f. Agresión a la privacidad mediante la utilización y procesamiento de datos personales con fin distinto al autorizado.

La intimidad y la propia imagen, bienes jurídicos relacionados con la privacidad son fácilmente afectados frente a un ataque a los datos personales de su titular, en sí el bien jurídico intimidad, el derecho a tener control sobre que partes de su vida una persona decide compartir o mantener para sí, supone a parte del patrimonio uno de los bienes jurídicos más afectados comúnmente por un delito informático.

No en vano DAVARA RODRIGUEZ establece que la potencial agresividad a la intimidad de la persona y a su propia imagen o a la denominada privacidad mediante la utilizacion y procesamiento de datos personales que se tienen legalmente para un fin determinado utilizandolos para un fin distinto de aquel para el que se esta autorizado asi como la utilizacion del resultado del proceso y nuevo tratamiento automatizado de esos datos personales con fines y para actividades distintas de las que justificaron su obtencion y almacenamiento son cuestiones que han sido objeto de estudio y desarrollo legislativo en numerosos paises de nuestro entorno (Davara Rodriguez op cit 358)

5 Otras Clasificaciones

Es necesario resaltar que frente a la categorización o clasificacion de los delitos informaticos en el derecho comparado se puede revisar lo postulado existe por el convenio sobre cibercriminalidad del Consejo Europeo de 2001 el cual divide en cuatro categorias aquellas conductas criminales que pueden ser consideradas como delito informático o como cibercrimen las cuales son

1 Infracciones contra la confidencialidad la integridad y la disponibilidad de los datos y sistemas informáticos

2 Infracciones informaticas

3 Infracciones relativas al contenido y

4. Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

TÉLLEZ VALDÉS, hablando del llamado Delito Cibernético, a finales de la década del noventa, clasifica extensamente el delito, configurándolo en dos categorías, delitos en que la computadora es el instrumento y aquellos en la que esta es el fin u objetivo, así entonces desarrolla el autor:

1. Como Instrumento o Medio, categoría donde incluye las conductas que utilizan la computadora como método, medio o símbolo:

a. falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera.)

b. variación de los activos y pasivos en la situación contable de las empresas;

c. planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera.).

d. robo de tiempo de computadora.

e. lectura, sustracción o copiado de información confidencial.

f. modificación de datos tanto en la entrada como en la salida.

h. aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto es lo que se conoce en el medio como el método del

"caballo de troya"

i. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la técnica del salami".

j. uso no autorizado de programas de cómputo

k. introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios.

l. alteración en el funcionamiento de los sistemas.

m. obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

n. acceso a áreas informatizadas en forma no autorizada.

o. intervención en las líneas de comunicación de datos o teleproceso. (Cfr. Tellez Valdés, 1998:113 a 116)

2. Como fin u objetivo, donde al categorizar conductas dirigidas contra la computadora en sí, se las divide en:

a. programación de instrucciones que producen un bloqueo total al sistema.

b. destrucción de programas por cualquier método

c. daño a la memoria

d. atentado físico contra la máquina o sus accesorios (discos, cintas,

terminales, etcétera).

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

f. Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etcétera).

Por su parte LUZ CLARA, presenta su clasificación de los delitos informáticos, atendiendo a como sea utilizada la computadora:

a. Delitos contra el sistema, donde la computadora es el objeto del delito, aquel ataque se puede dar contra el hardware (soporte físico, la computadora en sí) o el software (el soporte lógico, constituido por os programas que permiten a la computadora cumplir sus funciones.)

b. Delitos mediante el sistema, donde la computadora es el instrumento para cometer el delito, considerando que aquellos ataques pueden darse contra el patrimonio, la privacidad o la seguridad supraindividual. (Cfr. Luz Clara, op.cit.:118)

SAINZ CAPEL presenta un punto de vista diferente al desarrollar la clasificación de estos delitos, así habla de

1. La entrada, alteración, borrado o supresión de datos y/o programas informáticos efectuados de manera consciente e intencional con la

finalidad de llevar a cabo una transferencia ilegal de fondos o de otra cosa de valor o simplemente realizar o dificultar el funcionamiento de un sistema informatico o telecomunicaciones si se hace ilegalmente

2 La vulneracion del derecho exclusivo del titular de su programa informatico protegido por la ley con el fin de explotarlo comercialmente entendia esta ultima palabra en sentido muy amplio Y en igual sentido la violacion de dibujos signos o diseños protegidos de un circuito creado para su explotacion comercializacion

3 El acceso o la interceptacion de un ordenador o de un sistema de telecomunicaciones hecho dolosamente incluyendo el supuesto de obtencion por medios ilegitimos de los datos personales (por ejemplo en un establecimiento sanitario o de prisiones) o de un secreto comercial o industrial Sainz Capel (2001 37)

RIQUERT al presentar su clasificación de estos delitos los distingue en

a) Fraudes cometidos mediante manipulación de computadoras

b) falsificaciones informaticas y

c) daños o modificaciones de programas o datos computarizados (Cfr Riquert 1999 40)

PALAZZI en cambio clasifica estos delitos de acuerdo a las distintas modalidades delictivas relacionadas a la informatica con los distintos bienes juridicos que

se pudieran ver afectados, por lo cual este previo a tratar de hacer una clasificación de los delitos informáticos, prefiere hacer una distinción de aquellos bienes jurídicos afectados, así distingue:

a. Delitos contra el patrimonio, donde establece que en su momento el principal ataque se perpetraba contra maquinas de cajeros automáticos, posteriormente considera PALAZZI, que la información en sí, es uno de los principales bienes jurídicos atacados relacionados al patrimonio, agregando también la amenaza que representa para la información los virus informáticos y aquellos programas dirigidos para un fin determinado, fin que debe ser ilícito.

b. Delitos contra la intimidad, con motivo del comercio que se da con datos de carácter personal, se invade la intimidad de aquellas personas que desconocen aquel comercio de sus datos personales, establece PALAZZI, "con una simple conexión a Internet cualquiera puede saber si su vecino fue inhabilitado por el Banco Central para operar en cuenta corriente bancaria, o mediante un satélite es posible fotografiar cualquier superficie de la tierra o por medio de un scanner térmico podemos detectar que sucede en un hogar", lo que supone ampliar el concepto tradicional intimidad y su ámbito de protección. (Palazzi, op.cit.:45)

c. Delitos contra la seguridad pública y las comunicaciones, el autor

considerando la rápida integración de la informática en todos los aspectos de la vida, al momento de que una computadora o sistema informático se emplee para servicios de comunicaciones o de transporte, el ataque a este bien de carácter colectivo, se podrá efectuar de manera que el ataque se configure a través de un delito informático. Igualmente considera que estos ataques también se relacionan a temas de defensa nacional y seguridad militar, donde los Estados en el futuro deberán tener planes de contingencia frente a posibles atentados a los sistemas informáticos del país.

d. Falsificaciones informáticas mediante la alteración de documentos electrónicos, considerando que la Fe Pública como bien jurídico se debe rediseñar frente a las nuevas tecnologías, ya que con la simple alteración de un dato dentro de un proceso o programa se puede causar grandes daños al patrimonio, no esta demás la opinión de PALAZZI, que considera que, "el problema aquí es mucho más grave que los delitos tradicionales porque estas falsedades cibernéticas rara vez dejan huellas, y si lo hacen, es posible programar al ordenador para que los elimine y dificulte la detención del delito. (Palazzi, op. cit.:47)

e. Contenidos ilegales en internet. PALAZZI, establece que "el paso de un ámbito académico a uno comercial de internet, hizo que la red fuera

invadida por una gran cantidad de material ilícito", así el autor describen aquellos contenidos como propaganda discriminatoria o antisemita, los contenidos pornográficos y pedofílicos entre otros. (Palazzi, op.cit.:47)

RUIZ VADILLO (Ruiz Vadillo En Rovira del Canto 2002: 121-122), estableció los siguientes supuestos de delincuencia informática:

1. Entrada, alteración, borrado y/o supresión de datos y/o programas informáticos efectuados de manera consciente o intencional con la finalidad de llegar a cabo una transferencia ilegal de fondos o de otra cosa de valor o simplemente de realizar una falsedad, cualquiera que sea su finalidad o de obstaculizar o dificultar el funcionamiento de un sistema informático o de telecomunicaciones si se hace ilegalmente.

2. La vulneración del derecho exclusivo del titular de su programa informático protegido por la Ley con el fin de explotarlo comercialmente, entendida esta última palabra en sentido muy amplio. Y en igual sentido la violación de dibujos, signos o diseños protegidos de un círculo creado para su explotación comercial.

3. El acceso o la interceptación de un ordenador o de un sistema de telecomunicaciones hecho dolosamente, incluyendo el supuesto de obtención por medios ilegítimos de los datos de un ordenador y su divulgación, bien si trate de datos personales o de un secreto comercial o industrial.

Consideración interesante de la materia hace ROMEO CASABONA (Romeo

Casabona 2006:7), quien desarrolla su clasificación partiendo desde la base de que debido a la incorporación de distintas Tecnologías de la información y comunicación al mundo económico, empresarial y financiero, se observaron una nueva expresión más profunda de delincuencia patrimonial y socioeconómica, las cuales son capaces de causar grandes perjuicios a las distintas esferas ya mencionadas, por lo que este hace una relación de las conductas más significativas desde su perspectiva partiendo de la idea de distinguir el delito informático del cibercrimen, así presentan cinco modalidades principales, las cuales son a saber:

a. Manipulaciones de datos y/o programas, o 'fraude informático';

b. copia ilegal de programas, 'piratería informática';

c. Obtención y utilización ilícita de datos, o 'espionaje informático';

d. Destrucción o inutilización de datos y/o sistemas informáticos, o daños o 'sabotaje informático';

e. Agresiones en el hardware o soporte material informático, principalmente 'hurto de tiempo de un sistema informático '.

Es necesario destacar que frente al tema del 'espionaje informático', siguiendo los criterios de su clasificación, ROMEO CASABONA, establece que, "en este contexto económico quiere aludir a la afectación de la capacidad competitiva de la empresa (espionaje industrial, de mercado o financiero". (Romeo Casabona, op. cit.:7)

La postura de WALDEN (cfr. Walden op. cit.:23), al categorizar el delito

informático, como también el cibercrimen, es la de seguir principalmente lo establecido por el convenio sobre cibercriminalidad del Consejo Europeo de 2001, pero prefiriendo utilizar una clasificación tripartita de los delitos en vez de la versión del Convenio, la cual contiene cuatro conductas distintas, así este prefiere tener:

a. Crimen relacionado con computadoras, conductas típicas de los delitos informáticos donde la computadora será utilizada para cometer un delito.

b. Crimen relacionado al Contenido, en esta categoría condiciona aquellos cibercrimenes, que contienen actos relacionados a pornografía infantil o sobre la propiedad intelectual, esta categoría se refiere al uso de la computadora y las tecnologías de la información y comunicación para facilitar la distribución de contenido o datos ilegales por internet, estas conductas se diferencian de los delitos informáticos comunes, donde la computadora y los procesos y datos son todos parte de un proceso o herramienta para lograr cometer un delito, mientras que en estos casos, en estos delitos relacionados al contenido, los datos o la información procesada son la conducta delictual en sí, no una herramienta.

c. ataques a la integridad de la computadoras, categoría donde trata aquellas conductas que atacan la integridad de una computadora o de un

sistema de comunicación en sí, como por ejemplo la distribución de un virus, o la intrusión no autorizada de un sistema informático (crackin), en general estas conductas suponen ataques a la información en sí, independientemente de que tipo de información sea, sea información de carácter personal, información crediticia, sea información reservada de carácter comercial, etc.

ROVIRA DEL CANTO previo a presentar su propia visión de como se debe clasificar los delitos informáticos, hace mención de la gran relación que tiene el trabajo de SIEBER con el de LAMPE, que respondiendo a un sistema vinculado a las características del procesamiento automático de datos y a una separación de los diversos tipos criminológicos de conducta y que agrupa las conductas mas significativas, estableciendo las siguientes distinciones:

1. Manipulaciones de datos y/o programas, o fraude informáticos
2. Copia ilegal de programas
3. Obtención y utilización ilícita de datos o "espionaje informático"
4. destrucción o inutilización de datos y/o programas o "sabotaje informático"
5. Agresiones en el hardware o soporte material informático principalmente el "hurto de tiempo del ordenador" (cfr. Rovira del Canto 2002:120)

El mismo ROVIRA DEL CANTO (cfr. Rovira del Canto op. cit.:128), presenta su clasificación de los ilícitos informáticos atendiendo criterios de áreas de incidencia de la delincuencia informática en relación al bien o interés jurídico tradicional atacado, por lo que define cuatro grupos criminológicos:

1. Infracciones a la intimidad;
2. Ilícitos económicos;
3. Ilícitos de comunicación por la emisión y difusión de contenidos ilegales y peligrosos; y
4. Otros ilícitos informáticos.

Tal cual se observa, la doctrina muestra de numerosas maneras la clasificación de los delitos informáticos, unas restrictivas otras tan amplias que hasta parecen más bien una lista taxativa de todos los posibles actos que constituyen delito informático, estas posturas tienen un gran valor referencial para el legislador, toda vez que este deberá decidir a que sistema adherirse y como plasmar la doctrina en el Código Penal de manera especifica.

2. El Delito de Daños y su relación con el Sabotaje Informático

Hemos considerado necesario referirnos previamente a algunos aspectos del delito de daños y su relación con el delito de sabotaje informático, desde la perspectiva de la legislación anterior y del Código Penal del 2007, tomando en consideración que, en el

sabotaje informático, se provoca un deterioro o destrucción al hardware y al software, es decir, una destrucción de datos, a los sistemas informáticos, que provocan una destrucción, o inutilización a través de un virus, por ejemplo de datos.

2.1.3. El delito de daños en el Código Penal de 1982

El delito de daños, se contemplaba en el Código Penal de 1982, en el Capítulo VII "Daños" del Título IV "Delitos contra el Patrimonio", en los artículos 200 y 201.

El delito de daños "damnum injuria datum" presenta el tipo básico en el artículo 200, que comprende las conductas de destruir, inutilizar , romper; o de cualquier otro modo dañar cosas muebles o inmuebles, incluyendo en la última fórmula el legislador, la posibilidad de incorporar, cualquiera otra conducta que cause iguales resultados nocivos a la propiedad. Cfr. Febres Cordero (1993:593)

En ese sentido, el Código Penal de 1982, configuraba el delito de daños de la siguiente manera:

> *ARTICULO 200. El que destruya, inutilice, rompa o de cualquier modo dañe cosas muebles o inmuebles que pertenezcan a otro, será sancionado con 10 a 50 días-multa. Cuando el hecho fuere ejecutado por 2 o más personas la sanción se aumentará hasta la mitad del*

máximo.

De lo anterior, resulta en principio que se tutelaba cualquier ataque en contra de bienes muebles o inmuebles ajenos, lo que permitia tutelar de manera abierta cualquier conducta dolosa de daño contra la propiedad ajena.

En sentido estricto tratándose de la comisión de delitos informáticos o cibernéticos, se presentaban algunos problemas pues en la doctrina nadie discutía la posibilidad de hacer daños al hardware y al software, una discusión sobre la naturaleza corpórea del objeto material de este delito, no hacía posible que se extendiera su interpretación para incluir objetos inmateriales como la información contenida en un programa informático o de ordenador. Cfr. Guerra de Villalaz (2002:130)

La pena para la figura básica del delito de daños, es de 10 a 50 días multa, y se agrava la pena cuando el hecho fuere ejecutado por dos o mas personas, aumentándose hasta la mitad del máximo.

En cuanto, al artículo 201, contenía el tipo derivado del delito de daños de la siguiente manera:

ARTICULO 201. Se sancionará con 6 meses a 2 años de prisión y de 50 a 100 días-multa si el delito de daño se comete:

1. Por venganza contra un servidor público, a causa del ejercicio de sus funciones;

2. Por medio de violencia contra personas;

3. Con destrucción o grave daño en las residencias u oficinas particulares, en los edificios públicos o destinados a uso público o al ejercicio de algún culto, en los edificios u obras militares, naves o aeronaves del Estado, en los monumentos públicos o cementerios o en cosas de valor científico, cultural, histórico o artístico,

4. En las plantaciones o sementeras o en las cercas protectoras de fundos agrícolas o pecuarios.

De la lectura del artículo 201, se observa el interés del legislador de tutelar el daño que se provoca en un servidor público por razón del ejercicio de sus funciones, el que se comete por medio de violencia contra las personas, el daño cometido en edificios públicos o privados o de otra naturaleza, y en plantaciones o sementeras o en las cercas protectoras de fundos agrícolas o pecuarios, todas estas agravantes típicas en el delito de daños.

En conclusión, luego de este breve análisis del Código Penal de 1982, resaltamos que es notorio que de manera textual no se hace mención a los daños que pudieran provocarse a través de medios electrónicos, sea una computadora o un sistema de red, de manera que el sabotaje electrónico no estaba tipificado de manera específica en nuestra legislación, limitándose su protección, aunque por ser que el Delito de daño del Código

Penal de 1982 estaba dirigido a tutelar la propiedad ajena de cualquier acto que suponiera la destrucción, inutilización o el simple romper la cosa mueble o inmueble ajena, no hay duda que la Legislación Panameña de manera amplia aceptaba la posibilidad de castigar el acto dañar, inutilizar o romper la cosa ajena, la cual pudiera serlo una computadora o los datos contenidos en esta.

2.1.3.1 El Delito de Daños en el Código Penal de 2007

El Código Penal del 2007, se aprobó el 18 de mayo de 2007 por la Asamblea Nacional de Panamá, mediante la Ley 14 de 18 de mayo de 2007, y se estableció una "vacatio legis", por lo que empezó a regir este año.

El Delito de daños, está insertado en el artículo 226 correspondiente al capítulo VI "Daños", del Título VI denominado "Delitos contra el Patrimonio Económico", que expresa lo siguiente.

> *Artículo 226. Quien destruya, inutilice, rompa o dañe cosa mueble o inmueble que pertenezca a otro será sancionado con pena de uno a dos años de prisión o su equivalente en días-multa o arresto de fines de semana.*
>
> *La sanción se aumentará de una cuarta parte a la mitad de la pena si el delito se comete:*
>
> *1. En perjuicio de un servidor público, a causa del*

ejercicio de sus funciones.

2. Mediante intimidación o violencia contra tercero.

3. Con destrucción o grave daño en residencia, oficina particular, edificio o bien público, bien destinado al servicio público, edificio privado o destinado al ejercicio de algún culto, vehículo oficial, monumento público, cementerio o cosa de valor científico, cultural, histórico o artístico.

4. En una plantación, sementera o en las cercas protectoras de fundos agrícolas o pecuarios.

5. Mediante la utilización de sustancia venenosa o corrosiva.

6. Si el daño total ocasionado supera la suma de dos mil balboas (B/.2,000.00), independientemente del valor del bien que se haya afectado directamente con la acción.

Cuando el daño se ocasione utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza, la pena será de dos a cuatro años de prisión.

El tipo penal del delito de daños, no difiere mucho del código anterior, ya que se

mantienen como verbos rectores "destruir, inutilizar, romper o dañar", cosas muebles o inmuebles que pertenecen a otros.

Por lo que respecta a la punibilidad el Código Penal de 2007 no solo ha aumentado las penas para este delito, sino también consagra penas de carácter alternativo, a la pena prevista de uno a dos años de prisión, que son la pena de días multa o arresto de fines de semana, a diferencia del código anterior.

De igual forma se observa, que se mantienen las mismas agravantes previstas en el Código de 1982, referentes a daños cometidos un servidor público a causa del ejercicio de sus funciones, por medio de violencia contra las personas, destrucción grave daño en las residencias u oficinas particulares en edificios públicos o destinados a uso público, al ejercicio de algún culto, en edificios, en los monumentos públicos o cementerios o en cosas de valor científico cultural histórico o artístico, también se contempla de manera similar las agravantes de daño ocasionado en plantaciones o sementeras o en las cercas protectoras de fundos agrícolas o pecuarios

Por otro lado, no contempla como agravante del delito de daño los daños ocasionados a los apiarios, equipos e instalaciones utilizados en la apicultura e igualmente se elimina la agravación de la pena cuando varias personas realizan el delito de daños.

Por otro lado se incorporan como agravantes situaciones específicas al tipo delito de daños, como son los daños que sean provocados utilizando sustancias venenosas o

corrosivas por el riesgo que las mismas implican en las personas.

A diferencia de la legislación anterior se aumenta la pena en atención a la cuantía del daño ocasionado cuando el mismo supere la suma de dos mil balboas (B/. 2,000,00), independientemente del valor del bien afectado que se haya afectado directamente con la acción.

Para terminar, en materia de informática consta que el párrafo tercero del artículo 226 incrimina el delito de daños por medios informáticos de la siguiente manera, cuando el daño se ocasione utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza, la pena será de dos a cuatro años de prisión".

De lo anterior se observa que no se incrimina de manera directa el delito de sabotaje informático, porque en el sabotaje informático el daño esta dirigido de manera directa al hardware o al software, o a los datos contenidos en el sistema informático.

En este caso el legislador lo que pretende es proteger el patrimonio del sujeto contra cualquier clase de daño, aunque con ello no pueda obviarse que queden comprendidos los daños al sistema informático, que es lo que a nuestro modo de ver fue la ratio legis.

Al igual que nuestra legislación, países como Alemania, España, Francia y Honduras, contienen de alguna manera u otra dentro del mismo Delito de daños, la tutela en casos relacionados al uso de medios informáticos para cometer el delito, algunos lo configuran como un delito distinto al daño genérico (Alemania), mientras que otros lo

desarrollan dentro de las agravantes del delito de daño genérico (España), tal cual como se hace en Panamá.

Las nuevas formas de criminalidad relacionada con la informática y si bien no contempla de manera estricta la figura del sabotaje informático, si hace referencia a daños ocasionados utilizando medios informáticos, los cuales pueden en ocasiones destruir, inutilizar o dañar la información contenida en los sistemas.

A diferencia de nuestra legislación algunos países como Bolivia, Chile o Guatemala prefieren hacer de este tema tutela especifica de leyes especiales relacionadas a los delitos informáticos y cualquier otro tema relacionado con los medios informáticos y la tecnología.

2.1.3.2 El Bien Jurídico Protegido en el Delito de Sabotaje Informático.

2.1.3.2.1 Consideraciones previas entorno al bien Jurídico Protegido en el Delito de Daños

Antes de examinar el bien jurídico en el delito de sabotaje informático es necesario precisar, en que consiste la tutela penal del delito de daños, desde la perspectiva de la legislación nacional y del Derecho comparado.

En primer término, hay que señalar que siguiendo la ubicación del delito de daños

en nuestra legislación "Delitos contra el Patrimonio Económico", la tutela penal recae sobre el patrimonio económico, denominación que a juicio de ACEVEDO, constituye una limitante innecesaria, porque hay patrimonio abstracto, no económico. El concepto debe ser correctamente entendido, si la finalidad es diferenciarla con otros bienes económicos, como la propiedad intelectual. (Acevedo, 2008:331)

A nuestro modo de ver, la expresión "patrimonio económico", contiene dos conceptos que son necesarios explicar para poder determinar sobre que recae la tutela jurídica en el delito de daños.

Por patrimonio siguiendo los diccionarios jurídicos, se refiere al conjunto de bienes, derechos y obligaciones susceptibles de estimación económica pertenecientes a una persona física o jurídica, pero también en su significado gramatical, se alude al conjunto de bienes materiales y morales que posee una persona física.

Por su parte el término económico de acuerdo al Diccionario de la Real Academia Española se define como "perteneciente o relativo a la economía".

Desde el punto de vista jurídico, patrimonio se entiende por el conjunto de derechos patrimoniales pertenecientes a una persona, dicho conjunto forma una universalidad de la cual hace parte la propiedad y los derechos derivados de ella, los créditos y los derechos que recaen sobre objetos inmateriales. (Cfr. Romero Soto, 1990:13), expresión que es más extensa que el término económico.

BAJO FERNANDEZ y PEREZ MANZANO, manifiestan que hay una

concepción jurídica y económica de patrimonio en la doctrina, entendiendo por la primera "el conjunto de derechos y deberes patrimoniales de una persona" y en la segunda "forma parte del patrimonio los bienes que se encuentran a disposición de una persona con independencia de que ese poder de disposición no se halle protegido jurídicamente por las normas de derecho privado" y finalmente una concepción mixta o jurídica económica, que la limita a afirmar que patrimonio son "todas aquellas posiciones de poder sobre una cosa valorable económicamente". (Bajo Fernández y Pérez Manzano, op. cit.:400-441)

PABÓN PARRA, es de la opinión que frente el tema de la estructura del bien jurídico de los delitos contra el patrimonio, se debe tener como tal una concepción jurídico-económica del patrimonio, estableciendo que "lo que caracteriza el concepto penal de patrimonio es tanto el valor económico de la cosa como la protección jurídica que se brinda a la relación de una persona con esa cosa", así entendiendo que se tutelaran los bienes materiales e inmateriales; así entonces considera establecer algunas características relacionadas a esta postura, al establecer:

> a. objeto material de un delito patrimonial solo pueden serlo aquellos bienes dotados de valor económico.
>
> b. para ser un sujeto pasivo de u delito patrimonial no basta con que el sujeto tenga una relación meramente fáctica con la cosa, es preciso que esté relacionado con ella en virtud de una relación protegida por el

ordenamiento jurídico.

c. por perjuicio patrimonial hay que entender toda disminución, económicamente evaluable, del acervo patrimonial que, jurídicamente, corresponda a una persona". (Pabón Parra, 2002:16)

Para LAMARCA Y OTROS, los Delitos contra el patrimonio, "pretenden proteger el conjunto de bienes y derechos, de contenido económico, sobre el que cada ciudadano puede ejercer legítimamente derechos de aprovechamiento o disposición": agregando que este concepto de patrimonio, supera el uso del término propiedad, el cual resultaba algo limitado desde la perspectiva de la política criminal, la cual se reserva el derecho de posteriormente retocar la noción de propiedad o patrimonio a fin de ajustarse a los designios de la realidad económica de un país. (Lamarca y Otros, 2001:202)

ANDRÉS DOMINGUEZ tomando postura sobre el concepto de patrimonio en el Código Penal español y su relación al delito de daños establece que, "en nuestra opinión el concepto de patrimonio que se desprende del Código Penal es un concepto económico jurídico. La teoria económica constituye la base para la concreción del concepto de patrimonio pero se encuentra limitada por apreciaciones jurídicas: son bienes patrimoniales aquellos que están dotados del valor económico y se encuentran bajo el poder fáctico del sujeto sin que medie desaprobación por parte del ordenamiento jurídico". (Andrés Domínguez, 1999:83)

De lo anterior se desprende que por la expresión patrimonio económico se alude a todos aquellos conjuntos de bienes o derechos de la persona que tienen un valor económico apreciable.

En este sentido en el delito de daño cuando se realizan la conducta de destruir, deteriorar o inutilizar la cosa mueble ajena se produce una afectación sobre la cosa, que representa un daño económico para el patrimonio económico de su propietario. (Cfr. Mata y Martín. 2003:93)

Desde el punto de vista del derecho comparado el delito de daño es ubicado como un Delito contra la propiedad, en otras legislaciones Contra el patrimonio, Delitos contra el patrimonio económico o Delitos contra el patrimonio y el orden socioeconómico.

La doctrina históricamente consideraba como bien jurídico protegido la propiedad, tal como sucedía con el Código Penal de 1922, expresión que posteriormente fue reemplazada en el Código Penal de 1982, por el término patrimonio, mismo término que posteriormente ha sido reemplazado por patrimonio y por otras concepciones,

GUERRA DE VILLALAZ, considera como el delito de daños supone la destrucción de una cosa, sea esta mueble o no causada con el interés de perjudicar al sujeto pasivo, se debe tener al patrimonio como bien jurídico tutelado, "el delito de daños no supone un perjuicio patrimonial en sí mismo, sino el menoscabo de la cosa atendiendo a su valor y a la lesión producida en su esencia o sustancia". (Guerra de Villalaz, op. cit.:128)

En tal sentido hay que señalar que BUOMPADRE afirma que el termino propiedad se toma en un sentido amplio lo que supone que abarca al patrimonio en toda su totalidad es comprensiva de los derechos reales y personales bienes materiales e inmateriales y en general todos los intereses apreciables que un hombre pueda poseer fuera de si mismo de su vida y de su libertad (Buompadre 1998 21)

En opinión de VIVES ANTON la protección a la propiedad ajena sea publica o privada sera el objeto tutelado por el delito de daños aunque considera que igualmente por el delito de daños se tutelan bienes como la vida o integridad de las personas por razon del ulterior peligro que supone la comision de este delito para tales personas (Cfr Vives Antón 1996 1313 1314)

Para ZUGALDIA el delito de daños resulta ser una infracción que atenta contra el derecho de propiedad asi establece que la doctrina entiende de forma pacifica que es el derecho de propiedad entendido en su sentido estricto juridico privado el bien jurídicamente protegido a traves de su tipificación pues el derecho de uso y disfrute del propietario sobre la cosa objeto material de la infraccion se vera en todo caso menoscabado como consecuencia de la misma (Zugaldia 1988 29)

Para BRAMONT ARIAS el bien juridico protegido que es la propiedad desde la perspectiva que se protege la propiedad ante actos que tienden a la destrucción o inutilización tanto de bienes muebles como inmuebles (Bramont Arias 1994 382) mientras que por parte SERRANO GOMEZ señala que es el patrimonio ajeno y su

integridad (Serrano Gómez 2003 456)

Otro aspecto que merece destacarse en cuanto al delito de daños es que si bien se tutela el patrimonio economico al igual que sucede con los restantes delitos de este titulo la distinta naturaleza del delito de dano con los restantes delitos supone también que existen diferencias sobre el modo en que es afectada la propiedad

En este sentido SUAREZ SANCHEZ sostiene que la propiedad puede verse desde una doble óptica desde su perspectiva social y como derecho fundamental De modo que no es la propiedad una institucion solo económica pues esta en el epicentro de los agudos problemas humanos fue el caracter formal de los derechos de libertad e igualdad el que condujo a la introduccion de los derechos económicos y sociales (Suarez Sanchez 2000 70)

De igual forma FEBRES CORDERO es de la opinion que el bien jurídico protegido es la incolumidad de las cosas muebles o inmuebles pertenecientes a otro contra las acciones que supriman o disminuyan la integridad la utilidad o el valor de dichas cosas asi hay que tener claro que este tipo de delito sera distinto de los otros delitos contra la propiedad en general por ser que en el delito de daños el sujeto carece de un animus lucrandi indispensable en los otros delitos contra el patrimonio (Febres Cordero op cit 595)

Por su parte coinciden BAJO FERNANDEZ y PEREZ MANZANO que desde el punto de vista subjetivo en el delito de daños no se requiere el animo de lucro sino

simplemente destruir inutilizar o deteriorar la cosa por lo que el bien juridico recae sobre la cosa mueble o inmueble ajena que tiene gran valor económico susceptible de afectar el patrimonio (Cfr Bajo Fernández y Perez Manzano 1993 507)

En la misma linea el delito de daño se diferencia de los demas delitos contra el patrimonio segun CALDERON Y CHOCLAN por la intención despojada de lucro que guía al sujeto activo que no pretende beneficiarse sino solo perjudicar al sujeto pasivo sin obtener un correlativo enriquecimiento No es el móvil egoista el que impulsa su conducta, sino el odio o la voluntad de venganza proyectada sobre la destrucción o deterioro de los bienes ajenos (Calderón y Choclan 1999 849)

Para DAMIANOVICH el caso del delito de daño como bien juridico se debe tener en el contexto de que el patrimonio aparece elocuente y unicamente protegido en la sancion penal a esta conducta atentatoria de bienes concretos que lo componen sea mediante la destruccion sea mediante el deterioro En este ultimo caso debe destacarse que lo que aparece penalmente protegido es la disminucion del valor venal (Damianovich 2000 54)

En opinión de DONNA respecto al bien juridico en el delito de daño se da, básicamente un atentado contra una cosa Dicho atentado disminuye o elimina el valor de la cosa contra la que se atenta, pero quien sufre es la cosa en si misma no un derecho o poder sobre ella agrega que no se da un desplazamiento de derechos referentes a una cosa como segun el autor se encuentran en el resto de los delitos contra el patrimonio

sino un degradamiento de la cosa en sí (Donna 2001 759 760)

Para terminar CACERES señala que la posibilidad de encontrar dentro del bien jurídico del delito de daños diferentes bienes jurídicos a tutelar por lo cual este considera que se pueden vulnerar la existencia de diversos objetos de proteccion la propiedad en general la salud publica el ejercicio legitimo de la autoridad y la correcta aplicación de la ley la propiedad publica o demanial la capacidad económica del perjudicado el patrimonio informático el patrimonio o infraestructura de las fuerzas y cuerpos de seguridad la vida e integridad de las personas resumiendo que la tutela se refiere al derecho de propiedad (Cfr Caceres 2006 200)

2 1.3 2.2 El Bien Jurídico Protegido en el Delito de Sabotaje Informático

En nuestra legislación el delito de sabotaje informatico esta ubicado como un delito contra el patrimonio económico sin embargo hemos podido apreciar que la doctrina considera que hay otros intereses afectados razón por la cual pasaremos ha hacer una referencia sobre ellos aunque para ello nuestra labor en este aspecto haya sido dificultoso pues la doctrina no ha desarrollado lo suficiente

1 El patrimonio como bien jurídico protegidos

La figura delictiva del sabotaje informatico ha sido considerada como un delito de

daño cuando se producen alteraciones u obstrucciones graves en el funcionamiento de un ordenador o cuando se afectan los datos o programas informáticos (Cfr Saez Capel 2001 34)

En el caso del Codigo Penal del 2007 el legislador patrio ha seguido el criterio de considerar su tutela penal sobre el patrimonio económico que en otras legislaciones recae sobre el patrimonio en si pero debe señalarse que su ubicacion ha sido cuestionada, porque no puede identificarse con el patrimonio stricto sensu (Cfr Moron Lerma, 2002 67)

En la doctrina se ha sostenido sin embargo que en el delito de sabotaje informático se provocan perjuicios de caracter económico por la manipulacion de los datos (Romeo Casabona op cit 72) o por su destruccion pero lo que si es cierto que no estamos ante un enriquecimiento por parte del agente del delito a diferencia de los delitos contra el patrimonio sino en todo caso un empobrecimiento (Queralt op cit 483)

Desde la perspectiva especifica del delito de Sabotaje Informatico aunque el bien juridico protegido sigue siendo el patrimonio este concepto de patrimonio deja de ser el clásico concepto de patrimonio donde solo se aceptaba la noción de tutelar aquellas cosas materiales sino debido a la misma naturaleza del objeto de estos delitos aquellos datos programas o redes o soportes informáticos contenidos dentro o no de una computadora o sistema informatico es necesario tener una nocion de patrimonio que acepte la nueva inmaterialidad del patrimonio

Con toda razon el Estado ha tomado en cuenta la necesidad de evitar que se causen daños a estos sistemas como también a la informacion en si que se almacena en estos en atencion a los perjuicios economicos o financieros tomando en cuanta los estragos que pueden ser causados cuando un acto de sabotaje recaiga sobre una planta eléctrica o sobre el sistema de comunicacion de un pais entre otros

No en vano se refiere MARCHENA GOMEZ a la capacidad destructiva al alcance de cualquier cracker puede llegar a resultar ilimitada La inoculacion de virus informaticos en sistemas interconectados y el empleo de tecnicas de bombardeo de datos valiéndose de ordenadores esclavizados permiten multiplicar hasta el infinito el potencial numero de afectados El riesgo de unos daños a gran escala, asociados al simple envió de un programa destructivo se cierne sobre los numerosos usuarios de internet (Marchena Gómez 2001 356 357)

El fin de la tutela del sabotaje es evitar no solo el daño a los datos archivos o programas de una computadora, sistema informatico o red sino también evitar los otros problemas que suponen estos ataques sea el tiempo que demore restaurar los programas a sus estados originales esa perdida del acceso a la informacion resulta ser igual perjuicio al patrimonio del sujeto especialmente si este esta en una situacion de dependencia de algun sistema informatico que es inhabilitado por aquel acto de sabotaje (Cfr Palazzi op cit 161)

Igualmente se discuten algunos autores como MORALES PRATS (CFR Morales

Prats en ROMEO CASABONA el cibercrimen p 276) si la seguridad de los sistemas de información pueda ser o no un nuevo bien jurídico a tutelar frente a la nueva concepcion del ciberterrorismo o tal vez como MARCHENA GOMEZ (Marchena Gomez op cit 363 365) que considera mas bien que se debe relacionar mas el delito de sabotaje informatico a la tutela de la seguridad colectiva frente a la figura en si de los desordenes publico

Para MORÓN LERMA considerando el desarrollo y relación del bien jurídico del delito de daños y el sabotaje informatico enuncia que entendemos que la protección se dispensa respecto de intereses de contenido economico que atendiendo a los perfiles diferenciables que presentan los delitos de danos no pueden identificarse con el patrimonio stricto sensu es de la opinión de la autora que aunque el legislador considere que estos atentados afectan al patrimonio y son un delito de daños en la mayoria de los casos estos pocas veces toman un matiz patrimonial relacionado al delito de daños en si sino mas bien funcionan como parte de un metodo a fin de lograr un cometido ulterior (Moron Lerma, op cit 59 60)

En general la doctrina frente al bien jurídico tutelado del delito de sabotaje informático como bien establece BIDASOLO se haya dividida, asi establece que para lo que se protege es la propiedad para otros la utilidad o aplicabilidad de la información contenida en los datos y finalmente otros autores entienden que lo que se protege son situaciones análogas a la propiedad de modo que se protegen los datos en cuanto un

sujeto tiene un interes inmediato en su integridad esto se hace a fin de poder distinguir estas conductas del delito simple de daños como tambien poder delimitar quienes son el sujeto activo y pasivo de estos delitos (Corcoy Bidasolo en Mir Puig op cit 164)

Para terminar siguiendo nuestra legislacion vigente debe quedar claro independiente de las opiniones de la doctrina que él bien juridico protegido es el patrimonio cuando se producen los daños informaticos

2 La información como bien jurídico protegido

La información se considera como un bien juridico en los delitos informaticos no solo desde el punto de vista de los intereses económicos del propietario sino tambien desde la perspectiva de los sujetos interesados en dicha información siendo obvio el establecimiento de reglas con respecto al acceso de la misma (Cfr Rovira del Canto op cit 41)

Y es que los avances tecnológicos exigen ahora como indica ABOSO Y ZAPATA (Aboso y Zapata 2006 16) un nuevo interes social con un nuevo valor autónomo que al mismo tiempo se resalta la vulnerabilidad de los datos por la actual sociedad de la informacion por lo que hace que los Estados deban adoptar medidas para protegerla (Romeo Casabona 2006 350)

En esa linea se proyecta en la criminalidad informática la informacion como un bien juridico genérico proyectable y que dentro de los bienes juridicos que de ella se

desprenden a no dudar el mas importante es la información, por ser un bien jurídico esencial para la sociedad, y por los eventuales daños que se pueden realizar por los lícitos informático, y en la que se señala que son múltiples bienes jurídicos afectados por la tutela de la información: si la información es nominativa o relacionada con las personas se atenta contra la intimidad, de ser económica o representar valores, se atenta contra la propiedad o el patrimonio y de ser estratégica contra la seguridad social. (Jijena Leiva, op. cit.:45)

A propósito de ello, ROMEO CASABONA, hace mención a los datos de carácter personal en una computadora o sistema informático, en la cual la victima del delito de sabotaje informático se le causa daño por la destrucción de los datos. (CFR. Romeo Casabona op.cit.:167-190)

Y si bien observamos que en el sabotaje informático, la titularidad de estos delitos recae generalmente sobre el patrimonio, al causarse daños en elementos electrónicos, como lo denominan algunas legislaciones, no cabe duda, que la finalidad de la norma eventualmente tiende a proteger la integridad de los datos almacenados, los programas o documentos electrónicos. (Suárez-Mira Rodríguez, 2003:258)

Con toda razón se justifica la incriminación del sabotaje informático pues además de ocasionar un daño patrimonial, es evidente que los daños causados al software y al hardware primordialmente afectan gravemente la información intangible contenida en esos programas. (Cfr. Aboso y Zapata, op. cit. 49)

En sintesis el sabotaje informatico desde la perspectiva actual tiene como finalidad tutelar a los sujetos y a la sociedad en general contra los daños la inutilizacion o la destrucción de datos programas o información (Rovira del Canto op cit 226)

3 Otros Bienes juridicos

Sostiene MARCHENA GOMEZ que el sabotaje informatico no solo puede visualizarse como un problema de carácter individual del afectado (patrimonio) sino como una situacion que tiene un numero potencial de afectados por los daños provocados en gran escala a los usuarios de la red (Marchena Gómez op cit 360)

Y en ese sentido las estadisticas mundiales advierten de los riesgos y daños provocados provocado por los saboteadores en las que se proyectan negativas consecuencias en las comunicaciones estamos hablando en si del entorpecimiento temporal o definitivo de las comunicaciones vgr mediante correo electrónico o de mayor escala del riesgo potencial de deterioro de otro tipo de comunicación con base telemática, en la que se alude que se trataria en ocasiones de desordenes publicos

En efecto si la Legislacion española, la acusación de daños en telecomunicaciones no solo se trata de un delito de desordenes publicos sino también de daño en la que se destaca la particularidad de los objetos afectados y existe la posibilidad de que se pueda provocar algun tipo de desorden en la vida colectiva

2 1.3.3 1 El Objeto Material en el Delito de Daños

En principio el delito de daños y el sabotaje informático pueden tener muchas similitudes basicas por lo que es necesario previamente hacer algunas consideraciones sobre el objeto material en el delito de daños

En opinion de BUOMPADRE la discusion sobre el objeto material en el delito de daños resulta muy simple ya que considera que el objeto del delito puede ser una cosa mueble un inmueble o un animal total o parcialmente ajenos (Buompadre 1998 343)

Por su parte también señala AMUCHATEGUI que el objeto material del delito de daños sera la cosa mueble o inmueble (Amuchategui 1993 410)

La expresion **cosa,** extraída del derecho civil plasmada en nuestra legislacion civil distingue entre cosas muebles e inmuebles entendiéndose como cosa mueble aquella cosa que puede trasladarse de un lugar a otro sin llegar a perder su esencia o naturaleza, mientras que cosas inmuebles son las que perderian su esencia o naturaleza al ser trasladadas

Estas **cosas muebles o inmuebles** deben ser objetos capaces de ser valorizados debe poder cuantificarse economicamente su valor no podemos aceptar la nocion de tratar de considerar material descartado como objeto material de este delito o tal vez algun bien sin valor economico

Asi en este sentido CALDERON Y CHOCLAN consideran que el objeto

material dentro del delito de daños esta representado por cosas corporales sean estas muebles o inmuebles evaluables economicamente y susceptibles de destrucción o deterioro considerando especialmente el caso de las energias como tambien los daños causados en datos programas o documentos como tambien los daños causados en datos programas o documentos electrónicos ajenos contenidos en redes soportes o sistemas informáticos (Cfr Calderon y Choclan op cit 851)

La corporeidad o no de la cosa como objeto material en los delitos contra el patrimonio ha sido objeto de una gran discusión en el pasado asi algunos autores sostenian que las cosas materiales las cosas corpóreas y otras sin importar el estado de la materia (agua y gas) podian ser objeto material del delito de hurto y se presentaba igual discusión frente a la consideracion o no de la de la electricidad como objeto material en los delitos contra el patrimonio por esa razon sostenian otros que debia tomarse en consideración la descripción legislativa

En efecto muchos autores frente a la de corporeidad o no del objeto material en el delito de daños en concreto GONZALEZ RUS manifiesta que ni la letra de los preceptos ni el bien juridico protegido ni la conducta tipica, ni el resultado preciso para el delito ni ningun elemento expreso o implicito de la figura de delito imponen efectivamente que sólo las cosas corporales puedan ser objeto material del delito de daños Ha sido por el contrario una mala inteligencia del delito que ha trasladado aquí exigencias de corporeidad o materialidad que solo son necesarias en los delitos de

apoderamiento las que han conducido a tan cuestionable criterio limitativo del ámbito de aplicacion de la figura delictiva (González Rus 2002 1472)

Con toda razón insiste el citado autor que que esa concepcion clasica del objeto material del delito de daños a la cosa mueble o inmueble material y económicamente valorable susceptible de deterioro o destrucción y de ejercicio de la propiedad debe considerar los daños causados en bienes inmateriales no especificamente tipificados se deben tomar como si fueran dentro de los objetos materiales de fin informático como datos o programas por ser que la dinámica del delito de daños se construye en torno a la posibilidad de destruccion o deterioro de la cosa por lo que la materialidad o corporalidad del objeto resulta ser una condición legalmente no requerida en este delito estableciendo por consecuencia que el objeto material del delito de daños 'todo aquello que material o inmaterial tenga valor economico sea capaz de fundamentar un derecho de propiedad y pueda ser dañado (González Rus 1996 755)

De igual forma siguiendo la doctrina mayoritaria SUAREZ MIRA es de la opinión que el objeto material en el delito de daños será aquella cosa mueble o inmueble sea material o inmaterial que aunque la mayoria de los delitos de daños recaigan sobre cosas de carácter corporal estos también se produciran sobre cosas incorpóreas dentro de alguna corpórea como lo son los datos los programas o los documentos ajenos contenidos en redes soportes electronicos o sistemas informaticos (Suarez Mira, op cit 257)

Por otro lado el objeto material del delito de daños recae sobre la propiedad ajena, pero esta al ser un bien abstracto supone la necesidad de materializarse por lo que recaera sobre cosas muebles o inmuebles con valor economico en si mismos como tambien ser susceptibles de destruccion inutilizacion o deterioren lo que hace suponer que se refiera cosas fisicamente dañables por lo que se rechaza la idea de tener en cuenta el daño moral al ser que este no es economicamente evaluable ni mucho menos vulnerable a medios fisicos (Cfr Cáceres op cit 202)

En ese sentido el daño de la cosa propia o de aquellas que no tienen dueño no configura el delito parecida opinión resulta ser la de WASHINGTON y GALLETA quienes agregan luego de hacer inclusion de los bienes muebles e inmuebles que es requisito esencial que se trata de bienes ajenos pero es indiferente quien ejerce la tenencia al momento del hecho y en que caracter (Cfr Washington y Galleta, 2001 op cit 111)

Otro aspecto que merece señalar es que a juicio de DONNA el daño al objeto material debe causarle un perjuicio al sujeto pasivo este daño sea o no capaz de destruir totalmente o inutilice un objeto debe por lo menos ser capaz de lograr perjuicio que exija al sujeto pasivo al momento de tratar de restituir a su estado original el objeto algun tipo de gasto trabajo o esfuerzo (Cfr Donna, op cit 760)

Considerando que este perjuicio causado en detrimento del sujeto pasivo de este delito sea de caracter patrimonial o económico aunque resalta el autor que la doctrina no

esta de acuerdo en este punto

Sobre el objeto material en el delito de danos ANDRES DOMINGUEZ opina que la constituyen una proteccion que se brinda a la propiedad sobre la existencia incolume de una cosa amenazando con una sancion penal su destruccion o deterioro La interrelación entre objeto juridico y objeto material impone la exigencia de que éste ultimo sea susceptible de daño en su integridad material requisito que concurre en las cosas corporales o materiales se destaca tambien el hecho de que frente al tratar de legislar el daño en datos programas o documentos electronicos esta autora considera que aunque estos ataques necesiten una debida tutela penal estos no deben ser ubicados dentro del delito de daños ya que en muchos casos aquellos daños que recaigan sobre datos programas o documentos no seran objetos corporeos en si sino mas bien objetos intangibles requisito de vial importancia para la autora (Cfr Andres Dominguez op cit 111 112)

Desde un sentido más especifico al Objeto material desde la perspectiva del delito de daños es necesario tomar en cuenta que no solo sera aquel dato archivo o programa en una computadora, tambien se toma en funcion de una red o soporte informatico que aunque resulte ser problemático ubicar fisicamente este al igual que el dato en si ya que la perdida o ataque de estos usualmente son causantes de grandes perjuicios economicos (Cfr Davara, op cit 378)

En lo que respecta a la legislacion panameña con anterioridad al Codigo Penal de

1982 el delito de daños recae sobre una cosa mueble o inmueble y esa consideración ha arribado GUERRA DE VILLALAZ cuando manifiesta que el delito de daños es una ofensa a la propiedad que tiene como objetivo perjudicar la cosa sin que medie un apoderamiento ni desplazamiento del ámbito de dominio o vigilancia del dueño o poseedor por lo que puede recaer tanto en bienes muebles como inmuebles (Guerra de Villalaz 1989 91)

En conclusión el objeto material en el delito de daño puede recaer sobre una cosa mueble o inmueble al tenor de la disposicion legal sin embargo luego de haber revisado los planteamientos de la doctrina moderna no solamente tiene un alcance sobre las cosas corporales como tradicionalmente señalaban algunos autores sino también incluye los objetos inmateriales o intangibles y a manera de ejemplo podemos señalar que en nuestra legislación la cosa hurtada puede recaer sobre energia eléctrica agua telefonia y television abierta o cerrada (articulo 211 numeral 14)

Por otro lado segun veremos más adelante el objeto material de conformidad con el ultimo parrafo del articulo 226 plantea la posibilidad de que no se trate unicamente de una cosa corporal mueble o inmueble

2 1.3.3.2 El objeto material en el delito de sabotaje informático

El sabotaje informatico en estricto sentido como hemos indicado previamente se

refiere a un ataque perpetrado por medios informaticos contra un sistema red dato o en si a la informacion contenida en un sistema afectado

En el caso de nuestra legislación el parrafo tercero del articulo 226 se refiere a los daños ocasionados utilizando instrumentos o medios informaticos que podriamos decir que tiene cierta relacion con el sabotaje informático porque este ultimo se contempla como una figura autonoma y no como una forma agravada del mismo

En lo que respecta a la doctrina cabe señalar que no se ha estudiado con profundidad la problemática del delito de sabotaje informático y por ende su objeto material

Sin embargo hemos apreciado que un numero reducido de autores han planteado algunas tesis al respecto lo que nos permitira llegar a una conclusión

En este sentido en cuanto al objeto material del delito de sabotaje informatico se encuentra dividida la doctrina, sobre si este recae sobre los elementos fisicos (la cosa mueble) el hardware o si por el contrario recae sobre los elementos logicos (la cosa incorporal o intangible) como son los datos o la informacion en general

No en vano GONZALEZ RUS habla de la existencia de elementos físicos y lógicos en un computador siendo elementos lógicos aquellos relacionados al software en general y a los ficheros o archivos informáticos en los que se recogen datos informacion o documentos electronicos cualquiera que sea su contenido concreto (Gonzáles Rus 2002 1281)

Así para este daño informático se referirá únicamente a aquellos actos de destruir o inutilizar elementos lógicos sin importar que la inutilización se logre con una daño a un elemento físico: por lo que a su juicio no constituye sabotaje informático la destrucción de elementos físicos de un equipo informático en los que no contienen datos (monitor, impresora, disco duro vació), ni tampoco en rigor, la simple alteración del funcionamiento del sistema informático que afecta al procesamiento de la información, pero que produce afectando únicamente a los elementos físicos del equipo y con el fin de impedirla o dificultarla (inutilización de un microprocesador, que imposibilita o ralentiza el tratamiento de la información, deterioro de la memoria RAM, etc.

Sostiene CORCOY BIDASOLO que en el delito de sabotaje informático, el objeto material son los datos, sin importar de que estos sean datos protegidos o no, siempre que se encuentren registrados en forma no directamente perceptible para el hombre o que, de esta forma sean transmitidos, esto por ser que si fuese el caso de que su transmisión fuese perceptible al ser humano, sería mas bien delito de daños simple. (Corcoy Bidasolo en Mir Puig, op. cit.165)

Para ROVIRA DEL CANTO, el objeto material del delito de sabotaje informático recae sobre elementos como son las instalaciones informáticas tangibles como también los datos intangibles contenidos en programas informáticos y cualesquiera otra información valiosa, pero aclara que una nueva perspectiva considera que sabotaje informático en sí debe quedar limitado a aquellos elementos intangibles de la

computadora, los datos o información en sí. (Rovira del Canto, op. cit.:225)

En opinión de FERNANDEZ TERUELO (p.114), el objeto material se constituye por los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos...estableciendo que la diferencia entre dato y documento electrónico se encuentra en que el segundo es la configuración ordenada de los primeros en un medio o soporte informático. Resaltando que en el caso de los daños informáticos el daño no tiene porque recaer sobre la sustancia o materia en al que se alojan los datos soporte interno o externo: HD, CD, DVD, memoria USB, etc.), sino que basta con que se manifieste sobre su contenido. "De este modo será suficiente el borrado o alteración significativa de datos, aunque su soporte quede intacto (vgr. Formatear un disco duro de un PC); considerando este que frente la cuantificación económica de este daño se considere más bien un criterio de coste de recuperación o restablecimiento de la información o del sistema, por ser que en algunos casos, especificamente los relacionados con los datos afectados en ataques que tengan lugar en el ámbito del Internet son con frecuencia elementos que no están en el mercado (vgr. Lista de clientes)." (Fernández Teruelo, 2007:115);

A juicio de GONZALEZ RUS, es de la consideración de que aunque presenta elementos parecidos en lo que se refiere al objeto material del delito de sabotaje informático, establece que, "el objeto de ataque de los daños producidos a través de Internet es un fichero o archivo que en el momento del delito puede estar situado tanto en

un soporte físico (disco duro, CD, DVD, tarjeta, etc.) como en la memoria del ordenador o sistema o siendo transmitido a través de una red de transmisión de datos.", resaltando el autor que "lo significativo es que los elementos lógicos del sistema informático, esos ficheros o archivos donde se contienen los datos, los programas o los documentos electrónicos, resultan ser una especia de -flujo electromagnético-, incorpóreo, inmaterial e inaprensible en cuanto tal. Además, la característica común a todos ellos es que los datos que contienen no pueden ser leídos o percibidos directamente por el hombre, precisándose para ello la ayuda de máquinas capaces de interpretar señales digitales que los integran". (González Rus, 2005:1413)

Igualmente este hace mención a la definición de ROMEO CASABONA, la cual a su juicio comprende los casos en que se destruyen elementos lógicos tanto si ello se hace mediante la destrucción de sistemas informáticos completos como mediante la especifica de equipos y datos, programas y documentos electrónicos.

A consideración de GONZALEZ RUS, es necesario destacar, "de que más que la incidencia directa o indirecta en elementos lógicos, o que la conducta pueda afectar o no únicamente a elementos físicos, lo que caracteriza al sabotaje o a los daños informáticos, como prefiera decirse, es que se van comprometidas las funciones de almacenamiento o procesamiento de la información, incluyendo dentro de este ultimo concepto la transmisión de datos. (González Rus, 2002:1282)

En opinión de CACERES, al tratar el objeto material del delito de este delito que,

"el objeto material pueden ser datos, documentos, programas de naturaleza electrónica mantenidos en redes, soportes o sistemas informáticos" (Cáceres, op.cit.:203)

De conformidad con lo anterior no cabe duda que el objeto material en el delito de sabotaje informático en aquellas legislaciones que lo contemplan de manera autónoma recae exclusivamente sobre el dato, archivo, programa, sistema o red que resulte afectado por este delito, y no sobre otra clase de objetos, como por ejemplo la computadora, ya que esto no es la finalidad del legislador.

Sin embargo en aquellas legislaciones en las cuales se contemplan los daños por medios informáticos, dentro de la figura del delito de daño, se puede pensar que el objeto material recae sobre una cosa corporal, cuando en realidad es una cosa intangible.

Lo anterior tiene relación con nuestra legislación ya que el delito de daño recae sobre cosa corporal, mueble o inmueble según el párrafo primero del artículo 226, sin embargo el tercer párrafo ni si quiera menciona la cosa sobre recae el delito de daño. Más bien se refiere a los medios que se utilizan para ocasionar los daños.

Esto no quiere decir que el tipo agravado de daño relacionado con el sabotaje informático no tenga objeto material porque el objeto material va recaer sobre la cosa intangible (datos, archivos, programas, redes o soportes) que son dañados por la utilización de instrumentos o medios informáticos.

Y es que cuando una persona utiliza instrumentos o medios informáticos para causar daños directamente será afectada la información (dato, archivo, programa o redes

o soporte) contenida en el sistema afectado y no en si la computadora o hardware ni mucho menos el lugar donde se encuentre tal equipo

Desde el punto de vista de la informatica la informacion afectada a la que no es estamos refiriendo comprende términos como dato programas redes sistema informático y soportes

Por lo que respecta a los elementos comunes del objeto material del delito de sabotaje informático GONZALEZ RUS desarrolla los términos Datos Documento Electrónico Programas Redes Sistema informático y Soportes (González Rus en Romeo Casabona 2006 256)

Se entiende por Dato aquella unidad basica de información cualquiera que sea su contenido (un numero una palabra, un sonido una imagen) y que al ser procesadas dan lugar a la informacion que resulta de la conexion entre dos o más datos

Programas son el cuerpo sistematico de instrucciones legibles por la computadora y que le permiten realizar una tarea concreta son ese conjunto de codificaciones que interpretan la informacion que se introduce mediante un teclado u otro dispositivo de entrada y luego hace que la computadora ejecute una tarea

El termino Redes se refiere a un conjunto de tecnicas conexiones fisicas y programas informaticos que sirven para conectar dos o mas ordenadores permitiendoles compartir ficheros o equipos comunicarse entre si intercambiar información enviar mensajes electrónicos transmitir datos ejecutar programa conjuntamente etc Se integra

los elementos físicos (el hardware de red) y lógicos (el software de aplicaciones y el software de red), que pueden ser objeto de destrucción autónoma pudiendo dar lugar, por tanto a la modalidad de daños que corresponda en atención a su naturaleza física o lógica del elemento afectado.

Por lo que respecta al termino sistema informático, este en sentido estricto se refiere al conjunto de elementos dotados de un grado de estructuración y complejidad superior al de un ordenador personal; aunque es necesario entender el termino desde una perspectiva legal, por lo que se referirá a cualquier conjunto de dispositivos físicos y de ficheros y aplicaciones lógicas que permiten el procesamiento informático de datos, programas y documentos electrónicos, incluso si sirve para el uso aislado y particular de un solo usuario.

Soportes, serán aquellos dispositivos físicos en donde se almacenan los ficheros, programas o documentos electrónicos cualquiera que sea su naturaleza y funcionamiento (electromagnético, óptico, memoria RAM, etc.)

2.1.4. Análisis dogmático Jurídico del delito de Sabotaje Informático

2.1.4.1 Tipo Objetivo

2.1.4.1.1 Sujeto Activo

En la dogmática jurídico-penal se señala que la persona que realiza la conducta descrita en el tipo, es el sujeto activo. (Cfr. Righi, 1996:154), del cual solo puede ser considerada una persona natural. (Cfr. Bustos Ramírez, 2004:808)

Para MARTINEZ-PEREDA y ROMA VALDEZ en cambio es "el realizador de la acción determinante del resultado dañoso o creadora del peligro". (Martínez-Pereda y Roma Valdés, 1999:37)

El sujeto activo, también llamado sujeto de la acción, identifica a la persona física que comete el delito castigado en la legislación penal, que en el caso de nuestra legislación viene definido por regla general con la expresión "quien", "quienes" o tratándose de delitos especiales con otras formulas, por ejemplo "el servidor público, la mujer, el testigo" entre otros.

En lo que respecta al tipo agravado de daños previsto en el artículo 226 párrafo tercero, que estamos analizando relacionado con el sabotaje informático, dice lo siguiente "*cuando el daño se ocasione utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza, la pena será de dos a cuatro años*

de prisión", mientras que el tipo simple del delito de daños dice, "*quien destruya, inutilice, rompa o dañe cosa mueble o inmueble que pertenezca a otro será sancionado con pena de uno a dos años de prisión o su equivalente en días-multa o arresto de fines de semana.*"

En cuanto al delito de sabotaje informático, la doctrina ha señalado que es una conducta que puede ser realizada por cualquier persona, un poseedor o cualquiera que tenga derecho sobre la cosa, menos el propietario, que tiene el derecho de propiedad, pues el daño debe recaer sobre una cosa ajena.

También ha establecido que, es un delito común, monosubjetivo, en la que el sujeto activo es quien daña, inutiliza, o destruye datos, programas o información, es decir, es un delito que puede ser realizado por cualquier persona (Carmona Salgado, op.cit:141; Queralt, op.cit.:326), aunque se haya relacionado a los programadores (Villalobos, op.cit.:155) y a otros sujetos que tienen conocimientos especiales, entre los que se destacan rasgos como, la edad entre 8 y 45 años, con conocimientos en informática, y sin antecedentes penales. (Cfr. Villalobos, op.cit.:157)

De esta manera se ha determinado que existe un perfil del delincuente informático, que es un sujeto que tiene conocimientos especiales en el manejo de la tecnología informática, un sujeto calificado con niveles de inteligencia y conocimientos superiores, (Jijeiva Leiva, op.cit.:110) aunque para otros solo se requiera que el sujeto tenga mínimamente un conocimiento sobre el manejo de ordenadores (González, Rus, op.

Cit.:111), el cual puede ser personas que laboran en empresas, usuarios, o por el contrario intrusos, o como señala GUTIÉRREZ FRANCÉS (Gutiérrez Francés, op.cit.:74), simplemente un sujeto que trabaja en el mundo de la informática, de edad superior al prototipo y la mitad de inteligente.

Sobre esto último indica SÁEZ CAPEL que es muy frecuente que los daños sean cometidos por empleados de empresas, que tienen conflictos laborales o sociales. (Sáez Capel, op. Cit.:125)

En opinión de PALAZZI dependiendo de la clase de delito ejecutado, existe un perfil del delincuente informático, así por ejemplo en los delitos patrimoniales contra bancos y entidades financieras, son cometidos por empleados en especial cajeros, los delitos de acceso ilegitimo o delitos de daños menores, por hackers, phreakes, usuarios descontentos, los daños o sabotajes informáticos, por empleados de la empresa, profesionales o industriales,, las violaciones a la privacidad, tratamiento ilícito de datos personales, por investigadores privados, empresarios de marketing, agencias de informes crediticios y de solvencia patrimonial, y las violaciones a la propiedad intelectual de software y bancos de datos, con informes o compilaciones de datos, por piratas informáticos o también usuarios (la copia amigable) empresas que realizan competencia "parasitaria". (Palazzi, op. Cit.68).

En la terminología informática usualmente quien realiza estas conductas se le llama por diversos nombres, de Hacking, Craking, Cyberpunk y del Sniffer,

comportamientos que suponen GONZÁLEZ RUS "o un acceso ilícito, en el sentido de no autorizado, a sistemas o equipos informáticos, o a la producción de daños en equipos y sistemas informáticos introduciendo programas o rutinas nocivas en los mismos", lo que para el autor son conductas de sabotaje informático o acceso informático no autorizado (o intrusionismo). (González Rus en Romeo Casabona 2006:242)

De esta manera, el Hacker, realiza un acceso no autorizado a ordenadores y sistemas informáticos ajenos, utilizando las redes públicas de telefonía o transmisión de datos y con propósitos distintos al de la causación de daños; lo más comunes que se haga para violar la intimidad del titular del equipo o para la utilización de los mismos sin autorización o más allá de lo autorizado.

Por su parte Crakers, "son quienes se dedican al craking, término que se utiliza aquí para referirse específicamente a los daños informáticos que se producen accediendo o infectado sistemas informáticos ajenos a través de internet o redes de transmisión de datos."; agregando el autor que el vandalismo electrónico o cyberpunk igualmente hace referencia a los daños informáticos, y finalmente se refiere el autor a los sniffers (o rastreadores), programas que permiten introducirse en el disco duro de los ordenadores conectados a la red, buscando algún tipo de información.

En ese sentido, se entiende por algunos sectores de la sociedad que las personas que cometen los delitos informáticos son aquellas que poseen 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 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, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Por lo que respecta al tipo agravado de daños del artículo 226, que se refiere al agente que ocasiona daños por medios informáticos se observa que esta conducta puede ser realizada por cualquier persona, es por tanto un delito común y no puede ser calificado de delito especial.

Las razones por las cuales llegamos a esta consideración tienen su fundamento en que el legislador no lo califica delito especial, pero también porque se ha determinado doctrinalmente según hemos señalado previamente que cualquier sujeto lo puede realizar.

En síntesis, el sujeto activo de este delito no puede ser calificado de delito especial, pues si bien se identifica con un sujeto que tiene ciertos conocimientos, la doctrina lo ha descartado aunque lo usual se trate de sujetos que tienen un conocimiento en el manejo de computadoras. (Jijena Leiva, op.cit.:180)

2.1.4.1.2 Sujeto Pasivo

El sujeto pasivo es el titular del bien jurídico protegido, que resulta afectado por la

acción realizada por el sujeto activo. (Cfr. Muñoz Conde op. Cit. 186).

En lo que respecta al sabotaje informático. podemos encontrarnos ante un sujeto pasivo variable, el de carácter privado. el empresario de un negocio. de una industria. el titular de una institución bancaria. y de naturaleza publica, como un centro de enseñanza.

Por tanto. puede ser sujeto pasivo. la sociedad (sujeto pasivo mediato). y el inmediato. el titular del bien jurídico lesionado o atacado por el hecho punible. los propietarios de un sistema. los clientes del servicio. (Jijena Leiva. op.cit:180)

Pero lo cierto es que estos delitos informáticos ocasionan numerosos perjuicios patrimoniales y de otra naturaleza, por lo que se confirma que son numerosas las victimas que pueden presentarse, individuos. instituciones crediticias. gobiernos. etc.. que usan sistemas automatizados de información. generalmente conectados a otros".

En nuestra legislación el tipo agravado del artículo 226 del delito de daños. determina como sujeto pasivo a la persona que se le ocasiona el daño por medios informáticos a su patrimonio.

Por otro lado en aquellas legislaciones que contemplan los daños sobre programas o documentos electrónicos ajenos manifiesta CACERES. que el sujeto pasivo será aquel titular del derecho de propiedad afectado por la acción del sujeto activo, así entonces será el propietario de la cosa dañada el sujeto pasivo de este delito. (Cfr. Cáceres, op. cit.:202)

En conclusión el sujeto pasivo cuando se ocasionan daños por medios informáticos o en sí daños informáticos. el sujeto pasivo no solamente es la persona

afectada en su patrimonio sino también puede haber innumerables victimas como la sociedad por la alteración o destrucción de la información guardada.

2.1.4.1.3 La Conducta Punible

Como hemos señalado el sabotaje informático es una figura delictiva que aparece contemplada de manera autónoma en el derecho comparado y se ha entendido por regla general, como el acto de destruir, alterar, inutilizar o de cualquier otro modo dañar los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos, mientras que para un sector minoritario como por ejemplo Venezuela el alcance del sabotaje informático incluye también los componentes de un sistema que utilice tecnologías de información.

En el sabotaje informático, los daños informáticos se concretan, cuando el sujeto destruye o inutiliza los datos, programas ajenos contenidos en sistemas informáticos, es decir, son los realizados con métodos que causan destrozos lógicos, que afectan normalmente al software. (Cfr. Sáez Capel, op.cit:125)

En nuestra legislación no tenemos propiamente un delito de sabotaje informático, pero el artículo 226 del tipo agravado del delito de daños dice lo siguiente, "*Cuando el daños se ocasione utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza*".

De lo anterior se desprende que el artículo 226 del tipo agravado, del delito de daños contempla los daños por medios informáticos, que están relacionados con el sabotaje informático.

En lo que respecta al sabotaje informático en el derecho comparado las acciones punibles son variadas, así tenemos por ejemplo, "el suprimir, inutilizar o cambiar datos"; "destruir, eliminar o modificar un equipo de procesamiento de datos"; inutilizar datos, sistema de tratamiento de información ,inutilizar datos en computadora, inutilizar registros informáticos; el poner en circulación programas o instrucciones destructivas que puedan causar perjuicio a los registros, programas o equipos de computación, el modificar, destruir o provocar perdida de información contenida en sistemas o equipos de informática, entre otros.

Por su parte en nuestra legislación siguiendo el tipo agravado del artículo 226, la conducta consiste en **ocasionar** un daño mediante medios informáticos o de otra naturaleza, es decir causar, provocar, daños informáticos.

Por "ocasionar un daño" debe entenderse que el sujeto destruye, es decir, estropea la cosa o la reduce a nada, la inutiliza, es decir la aniquila o la reduce a la nada, la rompe, y finalmente, la daña, es decir le causa un detrimento o menoscabo.

El legislador refiriéndose al delito de daño utiliza varios verbos rectores, "destruir, inutilizar, romper o dañar", que desde el punto de vista gramatical son todas expresiones sinónimas, por lo que cuando se habla de ocasionar daño quedan comprendidas todas las

acciones antes señaladas.

En lo que respecta a los medios de comisión del delito el artículo 226 determina que los daños se ocasionan utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza.

En tal sentido cuando se habla de medios informáticos el legislador se esta refiriendo a nuestro modo de ver al uso de cualquier tecnología de la comunicación e información, que cuales quiera métodos, procedimientos o recursos que involucren estas tecnologías con el fin de cometer un delito.

También puede realizarse el hecho por el uso de la computadora, dato que en este caso será aquella unidad básica de información, cualquiera que sea su contenido (un número, una palabra, un sonido, una imagen) y que al ser procesadas dan lugar a la información, la cual resulta de la conexión entre dos o más datos.

Cuando el daño se ocasiona por medio de red, el término Redes, se refiere a un conjunto de técnicas, conexiones físicas y programas informáticos que sirven para conectar dos o más ordenadores, permitiéndoles compartir ficheros o equipos, comunicarse entre sí, intercambiar información, enviar mensajes electrónicos, transmitir datos, ejecutar programa conjuntamente etc. Se integra los elementos físicos (el hardware de red) y lógicos (el software de aplicaciones y el software de red).

Por programa se entiende, aquel cuerpo sistemático de instrucciones legibles por la computadora y que le permiten realizar una tarea concreta, son ese conjunto de

codificaciones que interpretan la información que se introduce mediante un teclado u otro dispositivo de entrada y luego hace que la computadora ejecute una tarea

Por otro lado existen diversos métodos posibles de efectuar el delito de sabotaje informatico

1 Uso de programas destructores en este caso el daño lógico producido a la computadora se logra borrando grandes cantidades de datos o de informacion daño que se logra en un periodo corto de tiempo asi se habla del empleo de programas como la bomba lógica utilidades auto reproducibles o rutinas establecidas en un programa de aplicación o sistema, llamados comunmente caballo de troya o simplemente los llamados bugs programas que se aprovechan de la existencia de defectos de hardware y software

Aunque el método mas comun en estos casos resulta ser el uso de un virus informático o programas especificos llamados gusanos o worms programas que se distinguen entre si por ser que los virus a diferencia de los gusanos se propagan a través de un programa anfitrion de un sistema informatico concreto mientras que el gusano ataca y se extiende en sistemas informático independientes

Asi ROVIRA DEL CANTO establece que debido a la diferencia en el diseño tecnico de un virus se pueda distinguir entre

a El virus informático clasico él cual se extiende en un programa anfitrion y

se activan cuando se carga un archivo.

b. El virus de sector de arranque, él cual luego de ser copiado a un medio de almacenamiento, este destruye toda la tabla de asignación de archivos. Estos logran su cometido con solo lograr ser insertados en el medio de almacenamiento.

c. El Macro virus, estos se basan en aprovechar el desarrollo de programas relacionados al procesamiento de un texto y hojas de calculo, donde se le pueden agregar códigos los cuales permitan acceso a distintas tareas, lo que permite transformar un simple archivo de texto en un programa capaz de borrar, grabar o transferir algún tipo de información o sino borrar el contenido de algún programa.

2. Sobre el abuso de hardware defectuoso o la terminación de software, donde a través de un bug es posible construir una aplicación capaz de destruir programas o sistemas informáticos, lo que hace posible crear por ejemplo un programa que ataque a todos los procesadores de computadora de alguna marca especifico o de algún modelo especifico.
3. La utilización de programa ping (programa usado para determinar si un anfitrión Internet es accesible en un momento y saber durante cuanto tiempo viajan los datos por internet), el llamado ping de la muerte o ping of death, el cual hace que un programa basado en la utilidad del ping envié datos especificos a sistemas de

windows 95 y haga que estos paren debido a un error de concepcion en el desarrollo del software TCP/IP de Windows En si estos ataques no representan gran peligro para la informacion almacenada en la computadora pero en el caso de que esta no sea salvada previo al ataque al momento que se reinicie el programa afectado esta sera perdida Haciendo entonces muy comun la existencia de programas que evitan estos ataques los llamados bug fixes o workaraounds con el fin de evitar futuros ataques empleando algun programa de la computadora

4 El sabotaje fisico dirigido a lineas de telefono u otras lineas de datos o telematicas suponen otro atentado de sabotaje donde mediante medios fisicos logran grandes perjuicios como lo son el destruir el cableado de red de una compañia telefónica o de alguna empresa o institucion especifica (Cfr Rovira del Canto op cit 230)

5 Otro tipo de ataque lógico a un sistema de comunicacion telematica e Internet es el remarcar las acciones de denegación de servicio (denial of service o DOS) culminadas en la más compleja denegación distribuida de servicios (DdoS) esta acción tradicionalmente consiste en enviar mucha informacion a un ordenador o terminal informatica a traves de la red en forma de cartas electronicas (sistema denominado mailbombing en cuanto supera la mera actividad de spamnming) o de paquetes de datos hasta que el equipo atacado no lo soporta se bloquea y deja de funcionar lo cual naturalmente depende de que el atacante disponga de

más ancho de banda que el atacado

A juicio de FERNANDEZ TERUELO el sabotaje informatico presenta dos conductas esenciales a saber en primer lugar el bloqueo (inutilizacion) parcial o total temporal o definitivo de paginas web u otros servicios de Internet y en segundo lugar la destrucción o alteración total o parcial de contenidos información o datos ajenos

Considerando que la produccion de tales resultados se puede conseguir mediante ataques o accesos no autorizados a espacios virtuales ajenos utilizando principalmente dos vias

a el mero aprovechamiento de la falta de cuidado del titular o encargado del control del servicio o pagina web o

b el recurso a formular tecnicas especificas como lo son

1 la difusion de virus secuencia de codigo que se inserta en un fichero ejecutable denominado host de forma que al ejecutar el programa tambien se ejecuta el virus generalmente esta ejecución implica la copia del código viral o una modificación del mismo en otros programas

2 Troyanos programas que simulan ejecutar una función mientras que realmente ejecuta otra Normalmente la tarea secundaria del troyano consiste en dar un control sobre el ordenador victima al atacante bloquear el mismo etc

3 Bombas lógicas o de tiempo programas que se activan al producirse

un acontecimiento determinado La condicion suele ser una fecha (bomba de tiempo) una combinacion de teclas o ciertas condiciones tecnicas (bombas logicas) Si no se produce la condicion permanece oculta al usuario

4 Gusanos programas capaces de ejecutarse y propagarse por si mismos a traves de redes en ocasiones portando virus o aprovechando bugs (fallos de seguridad) de los sistemas a los que se conecta causarles daños

5 Applets hostiles estos al ser descargados intentan explorar los recursos del sistema de una forma inapropiada esto incluye desde ataques clasicos como negaciones de servicio o ejecucion remota de programas en la maquina clienta, hasta amenazas mucho mas elaboradas como difusión de virus ruptura lógica de cortafuegos o utilizacion de recursos remotos para grandes cálculos científicos

6 Bacterias los conejos o bacterias son programas que no dañan al sistema de forma directa sino que se limitan a reproducirse generalmente de forma exponencial hasta que la cantidad de recursos consumidos termina por bloquearlo

7 Denegacion de servicio la llamada denegación de servicio (dDOS) persigue hacer caer a la maquina contra la que se realiza el ataque mediante el envió de cantidades ingentes de informacion

8 Canales ocultos un canal oculto es un cauce de comunicacion que permite a un proceso receptor y a otro emisor intercambiar información violando la politica de seguridad del sistema no es parte del diseño original del sistema pero puede utilizarse para transferir informacion a un proceso o usuario que a priori no estaria autorizado a acceder a la misma

9 Puertas traseras son códigos insertos en un programa que permiten a quien conoce su funcionamiento saltarse los métodos usuales de autenticación para realizar determinadas tareas Habitualmente son introducidos por los programadores para agilizar las pruebas del codigo durante la fase de desarrollo del mismo y se eliminan en el producto final pero en ciertas situaciones el programador puede mantener estas puertas traseras en el programa funcional ya sea deliberada o involuntariamente

10 xploits son programas que se aprovecha de algun tipo de vulnerabilidad en el sistema donde se usan y mayoritariamente sirven para ganar privilegios en el equipo

11 practicas de sniffing consiste en filtrar todos los paquetes que pasan por una red abriendo cada uno de ellos para examinar el interior en busca de contraseñas o informacion util

Estos instrumentos permiten el acceso directo y/o a distancia del sistema esto es la introducción virtual del autor en la máquina donde se encuentran los datos o la

difusion de algun elemento que termina por dañar los elementos logicos del sistema ajeno

2 1 4.2 Tipo Subjetivo

2 1 4.2 1 El Dolo

El articulo 27 del Código Penal vigente establece que actua con dolo quien quiere el resultado del hecho legalmente descrito y quien lo acepta en el caso de representárselo como posible mientras que la culpa es definida por el articulo 28 al establecer que actua con culpa quien realiza el hecho legalmente descrito por inobservancia del deber objetivo de cuidado que le incumbe de acuerdo con las circunstancias y las condiciones personales o en el caso de representarselo como posible actua confiado en poder evitarlo

El tipo simple del delito de daño es un delito doloso al igual que sucede con el tipo agravado de daño ocasionado utilizando instrumentos o medios informáticos computadora dato red o programa de esa naturaleza

En la doctrina el delito de daño se ha sostenido que no requiere ninguna particularidad subjetiva por parte del agente aunque es necesario que el sujeto tenga conocimiento de que se trata de una cosa ajena y que la accion es dañosa, por lo que

puede darse el "damnum injuria datum". (Cfr. Soler, 1970:472)

Al tenor del artículo 226 se manifiesta un comportamiento doloso, que consiste en "dañar"una cosa mueble o inmueble que pertenece a otro, de manera que no sea punible el daño culposo.

Se requiere un dolo directo y el ánimo en el agente de querer dañar la cosa, no son necesarios móviles o fines especiales en el agente, ni siquiera el móvil de perjudicar al propietario de la cosa, que constituye por sí un dolo directo. (Cfr. Donna, op cit p.762).

No hay pues una exigencia de un determinado ánimo "animus damnandi o nocendi" según afirman algunos autores, descartándose como un elemento subjetivo del injusto. (Isabel Valldecabres Ortiz, p.1314, en Comentarios al Código Penal de 1995)

En relación al sabotaje informático se sostiene que la tipicidad subjetiva se ve colmada a juicio de MORON LERMA, con la presencia del dolo, no requiriéndose, en este caso la concurrencia de una especia tendencia subjetiva, trascendente al propio dolo.", agregando que "el delito analizado tampoco admite la subsunción de las conductas de mero intruismo informático, desprovistas de un ulterior propósito al mero acceso y en consecuencia desnudas de un hipotético animo de dañar los datos contenidos en dichos sistemas. (Cfr. Morón Lerma, op.cit.:60)

Así GONZALEZ RUS, es de la opinión de que es "preciso que la conducta del delito de daños suponga algo más que la exclusiva afectación del valor de uso de la cosa", es necesario un daño y que en caso de la inutilización, "se precisa al menos una

afectación de la sustancia que determina, aun de forma mínima, un menoscabo de la cosa con incidencia de su estructura material y que suponga una pérdida de valor real independiente de los perjuicios derivados de la imposibilidad de uso, comprendiendo, en todo caso los supuestos de perdida, corrupción o degradación del objeto. (González Rus.:262)

El dolo en este delito, debe comprender la conciencia y voluntad de que se destruye un elemento lógico o un elemento físico en el que se contienen datos, programas o documentos electrónicos. No es preciso que concurra elemento subjetivo particular alguno. Este agrega que, "la existencia del dolo no debe verse dificultada por la dilación temporal entre el tiempo en el que se produce la conducta y aquél en el que se causa el daño, como ocurre en los casos de bombas lógicas, caballos de troya (troyanos) y supuestos semejantes. El dolo de dañar existe desde el momento en que se realiza la conducta, puesto que el sujeto conoce y quiere el proceso causal, incluidas las condiciones que deban cumplirse o las circunstancias que hayan de concurrir, que conducirá a la producción del resultado dañoso". (González Rus.:268)

Por lo que respecta a la necesidad de necesitar perjuicio para que se configure el delito de daños, el autor al igual de la mayoría de la doctrina española considera que no es preciso el perjuicio ajeno como consecuencia de la destrucción, deterioro o inutilización de la cosa al momento de configurar una acción como delito de daños.

Así también es posible observar dentro de un acto doloso la concurrencia de un

dolo eventual, al ser que el resultado de su conducta pueda producir perjuicios muchos mayores a aquellos queridos directamente por el sujeto.

Autores como CACERES, son de la opinión que la exigencia de un elemento subjetivo del injusto, ese llamado animus damnadi es descartado por la mayoría de los autores aunque siempre será mencionado por la jurisprudencia. (Cáceres, op.cit.:204)

Tratándose del sabotaje informático la acción del sujeto se manifiesta a juicio de Villalobos con la destrucción, limitación o alteración de la capacidad de los elementos informáticos debido a virus, rutinas, cáncer, programas borradores, etc. (Cfr. Villalobos, op.cit.:127)

Finalmente reiteramos que se excluye el comportamiento culposo en los delitos de daños, pues el sujeto actúa con intención de dañar la cosa por regla general. (Bramont-Arias Torres/ García Cantizano, Manual de Derecho Penal, Parte General; Cfr. Soler, op. cit.:473)

2.1.4.2.2 El error de tipo

Según ZUGALDÍA por error de tipo, "se alude a casos en que el sujeto realiza los elementos objetivos de un tipo penal pero sin saberlo, es decir, obra con desconocimiento de todos o de alguno de los elementos del tipo objetivo". (Zugaldía, op. cit.:513)

Esto es porque el autor debe conocer los elementos objetivos integrantes del tipo de injusto. Cualquier desconocimiento o error sobre la existencia de algunos de estos

elementos excluye, por tanto el dolo y todo lo más, si el error fuera vencible, deja subsiguiente el tipo de injusto de un delito imprudente.

Hay dos clases de error de tipo, un error de tipo vencible que para ARANGO DURLING, no es más que aquel en donde el "agente pudo haber salido del error en el que se encontraba y pudo evitar el resultado observando el cuidado debido que las circunstancias exigen para poder evitar cualquier tipo de resultado y el efecto del mismo, es que no hay ausencia de responsabilidad penal, porque si bien se elimina el dolo, subsiste la imprudencia si hay un tipo penal". (Arango Durling, 2008:22).

Igualmente se considera la existencia del error de tipo invencible como el nombre supone ocurrir en aquellos casos en que el sujeto "ha actuado con la mayor cautela y diligencia, y no ha podido obviar el conocimiento equivocado, de manera que su conducta sea atípica y se elimine el dolo y la culpa" (Arango Durling, op. cit. :22)

2.1.4.2.3 Admisibilidad del error de tipo

En lo que respecta al error de tipo en el delito de daños hemos encontrado muy poca información sobre este tema salvo el estudio realizado por SANTA CECILIA GARCIA en el trabajo monográfico sobre el delito de daños.

El citado autor analiza las distintas posibilidades en que puede manifestarse el error de tipo, el error directo, el error inverso y los diferentes errores accidentales.

En cuanto al error directo, (elimina el dolo y hace al comportamiento impune)

sostiene el autor que puede presentarse sobre la acción, por ejemplo cuando el sujeto aprieta el disparador de un arma que creía descargada que causa daños sobre la propiedad ajena, sobre el objeto material, cuando hay confusiones sobre el objeto material por su gran parecido el agente daña algo pensando que es suyo cuando en realidad es de un tercero y por cuanto al resultado, como cuando el sujeto creyendo disparar a una pieza de casa mata al perro de su compañero. (Cfr. Santa Cecilia García, op. cit.:351)

En relación a los errores accidentales, debe tenerse presente que subsiste la responsabilidad penal y en primer término podemos mencionar el casos de la *aberratio* o error en la ejecución, que es cuando el sujeto quiere un resultado delictivo pero por error produce un resultado distinto. A manera de ejemplo podemos mencionar el caso del dañador confunde un objeto con otro y dirige su acción contra un objeto distinto del que se había representado.

En cuanto al error inverso (error putativo), SANTA CECILIA GARCIA, sostiene que no tiene consecuencias penales, tomando en consideración la naturaleza del mismo.

Por lo que respecta al sabotaje informático indudablemente nuestra labor investigativa en este caso ha sido infructuosa y consideramos que todo lo anterior consecuentemente es aplicable a este delito.

2.1.4.2.4 Antijuridicidad y causas de justificación

Las causas de justificación en el Código Penal del 2007 lo constituyen el legitimo

ejercicio de un derecho o el cumplimiento de un deber legal, legitima defensa y, el estado de necesidad, encontradas en el capítulo IV del Titulo II Hechos Punibles y Personas Penalmente responsables del libro I del Código Penal. (arts. 31 y ss.)

El artículo 31 del Código Penal de 2007, establece como causa de justificación el ejercicio legítimo de un derecho o el cumplimiento de un deber expresamente, como se puede observar de la norma:

> ***"Artículo 31.*** *No comete delito quien actúe en el legítimo ejercicio de un derecho o en cumplimiento de un deber legal."*

En lo que se refiere al artículo 32 del Código Penal de 2007, justifica el actuar en legítima defensa de la persona, de los derechos o de un tercero o de sus bienes, siempre que las circunstancias así lo requieran, así entonces el texto del articulo 32 del Código Penal de 2007, establece:

> ***"Artículo 32.*** *No comete delito quien actúe en legítima defensa de su persona, de sus derechos o de un tercero o sus bienes, siempre que las circunstancias así lo requieran.*
>
> *La defensa es legítima cuando concurran las siguientes condiciones:*
>
> *1. Existencia de una agresión injusta, actual o inminente*

de la que resulte o pudiera resultar afectado por el hecho;

2. Utilización de un medio racional para impedir o repeler la agresión; y

3. Falta de provocación suficiente por parte de quien se defiende o es defendido.

Se presume que actúa en legítima defensa quien razonablemente repele al que, sin su consentimiento, ha ingresado a su residencia, morada, casa o habitación."

Finalmente el artículo *33* del Código Penal de 2007, consagra en su texto el estado de necesidad como causa de justificación, para la persona que ante una situación de peligro para evitar un mal a sí mismo o a un tercero, lesione un bien jurídico de otro, estableciendo las condiciones necesarias para tal justificación, tal como lo establece el texto del Código al decir:

"Artículo 33. *Actúa en estado de necesidad la persona que, ante una situación de peligro, para evitar un mal a sí misma o a un tercero, lesiona el bien jurídico de otro, siempre que concurran las siguientes condiciones:*

1. Que el peligro sea grave, actual o inminente;

2. Que no sea evitable de otra manera;

3. Que el peligro no haya sido ocasionado

voluntariamente por el agente o por la persona a quien se protege;

4. Que el agente no tenga el deber jurídico de afrontar el riesgo; y

5. Que el mal producido sea menos grave que el evitado."

De manera concreta no hemos encontrado en la doctrina, referencia especial sobre este delito en esta materia, y se ha señalado que debe ser enfocada desde la perspectiva general del delito de daños, la cual acepta la legítima defensa, el estado de necesidad y el ejercicio de un derecho o cumplimiento legal con tal que sea en total acorde con los requisitos inherentes de cada una de estas causas de justificación.

Sobre este tema es necesario agregar que según SANTA CECILIA GARCIA, se hará una distinción entre dos grupos de causas que excluyen la antijuricidad, siguiendo los principios de ausencia de interés y el del interés preponderante. Así menciona que "el primer principio origina como causa de exclusión el consentimiento expreso o presunto del ofendido. En efecto, el consentimiento del propietario de la cosa dañada, de acuerdo con la vieja máxima *violenti non fit injuria*, elimina el injusto, por tratarse de un bien jurídico, que como la propiedad es disponible". (Santa Cecilia García, op. Cit.: 302)

En cuanto a las causas referentes al interés preponderante, entendemos que las causas de justificación encontradas en nuestro Código Penal se basan en esta perspectiva por lo cual haremos mención específica de algunos casos relacionados con alguna de

estas.

Para que esta exención de responsabilidad penal se configure es requisito necesario de que se cumplan con las exigencias cada una de ellas.

A propósito la legitima defensa se ha aceptado en la defensa de los bienes porque se produce una agresión ilegitima a los mismos, donde el ataque debe poner a los bienes en grave peligro de deterioro o pérdida inminente.

El supuesto de cumplimiento de un deber legal del servidor público que labora en una sección de informática de la policía o del Ministerio Público, el cual que lesiona la intimidad y la inviolabilidad del secreto por el acceder sin la autorización del titular a su correo electrónico o en sus sistema informático solo seria aceptable si fuese autorizado por una autoridad competente, así de esa misma manera en el sabotaje informático, un servidor público introduzca algún programa que altere los datos de una computadora, para conseguir información para la investigación del delito, si actuó al margen de una autorización legal estaría cometiendo un simple delito en vez de actuar legítimamente durante el cumplimiento de sus funciones..

En cuanto al ejercicio de un derecho, no puede descartarse esta posibilidad ya que los medios informáticos están al alcance de los profesionales, en concreto de los ingenieros en sistemas de la banca, que encuentre información no autorizada o confidencial del banco en Internet, y procede a dañar, inutilizar o alterar el lugar donde se encuentra dicha información.

2.1.4.3 La Culpabilidad

Para que una conducta sea culpable se requiere que sea realizada por un sujeto con capacidad de culpabilidad, teniendo conocimiento de antijuridicidad del hecho y que se de su comportamiento concurra exigibilidad por su actuar.

Desde la perspectiva del Código Penal de 2007, se consagra mediante el artículo 35 del código la presunción de imputabilidad del sujeto, esta presunción se desecha cuando el sujeto se encuentra amparado bajo alguno de los casos de inimputabilidad contemplados en el Código Penal.

El artículo 36 del Código Penal de 2007, sobre la inimputabilidad establece que, no es imputable quien, al momento de cometer el hecho punible, no tenga la capacidad de comprender su ilicitud o, en caso de comprenderla, de autodeterminarse de acuerdo con esa comprensión.

Un sujeto imputable responderá penalmente por su actuar según lo tipificado por Código Penal, salvo en aquellos casos donde el sujeto se encuentre bajo algún caso de inimputabilidad, la cual será cuando este bajo estado de enajenación mental, dejando el código condiciones especificas en caso de que esta enajenación mental sea producto del alcohol o de drogas

No esta demás mencionar sobre la minoría de edad como causa de inimputabilidad actualmente se mantiene que menor de catorce años no delinque y que

frente aquellos menores infractores que tengan una edad entre los catorce y dieciocho, su responsabilidad se rige por la Ley 40 de 1999 sobre Responsabilidad Penal de Adolescentes.

Se pueden dar casos en los cuales el autor crea que su actuar es conforme a derecho, cuando en realidad no lo sea, este llamado error de prohibición. El error de Prohibición en la doctrina ha sido tema de innumerables discusiones, podemos mencionar que este se divide en error de prohibición directo y en indirecto, siendo el directo aquel que supone un desconocimiento de la norma, mientras que el indirecto supone un el suponer la existencia de una causa de justificación, la cual no es aplicable o inexistente.

Sobre el Delito de Daños y el error de prohibición, SANTA CECILIA GARCIA, es de la opinión, que frente al error de prohibición directo, salvo en casos de índole cultural o de condición psicológica del infractor, no es aceptable, ya que en toda la sociedad el respeto a la cosa ajena y la no destrucción de esta es algo generalizado. (Cfr. Santa Cecilia García, op. Cit.:350-351)

La clásica imagen de un adolescente que desafía los límites y parámetros de seguridad de un sistema informático del cual no tiene autorización, por querer demostrarle a sus amigos su capacidad en el manejo de las computadoras, accesando con una finalidad distinta a causar daños en el sistema o realizar daños a un sistema informático, desconociendo los alcances de la normativa legal de un país, son actos que pueden encajar un posible error de prohibición.

En general aceptamos la posibilidad que dependiendo del caso el error de prohibición es valido frente a caso de Sabotaje Informático no esta demas mencionar que ROXIN al establecer las formas de manifestacion de la conciencia de la antijuridicidad establece que todos los errores de prohibicion son iguales en que el sujeto se equivoca sobre la prohibicion especifica del tipo Pero las razones en las que se basan los errores de prohibición pueden ser diversas y permiten hablar de formas especificas de manifestación del error de prohibición (Roxin 2003 870 873)

Igualmente establece las manifestaciones más importantes del error de prohibición a saber

1) El error sobre la existencia de la prohibicion
2) El error sobre la existencia o los limites de una causa de justificacion
3) El error de subsuncion
4) El error de validez

Dependera de la realidad social y cultural de la sujeto el estudiar la posibilidad o no de que un actuar tipico y antijurídico relacionado con el sabotaje informatico no sea culpable la naturaleza cambiante y constante de las tecnologías de la información y comunicación pone numerosas posibilidades de error de prohibicion

En el Código del 2007 el error de prohibición no es determinado en si como error de prohibición sino que de su lectura se entiende que el legislador contempla que unicamente el error de prohibicion invencible será aquel que suponga eximente de

responsabilidad penal, lo cual es normal en el tratamiento del error. Así entonces el artículo 39 del Código Penal de 2007, establece que:

> *Artículo 39. No es culpable quien, conociendo las condiciones o las circunstancias del hecho que integran la conducta, por error invencible ignora su ilicitud.*

Se concibe lo expuesto en el artículo 39 del Código Penal de 2007, por ser que en el error de prohibición, en un caso específico tiene distintas consecuencias, ya que si el error es invencible, no habrá reproche alguno, dando entonces la absolución por falta de culpabilidad. En cambio si el error es vencible se atenúa el reproche, el cual será menor con respecto a que este hubiese obrado conociendo la antijuridicidad, así el sujeto será penado, pero esta será de responsabilidad menor, lo que conlleva a la pena atenuada.

Dentro del tratamiento de la culpabilidad es necesario mencionar también la no exigibilidad de un comportamiento distinto como eximente de responsabilidad penal.

En su momento MUÑOZ RUBIO y GUERRA DE VILLALAZ al referirse de la no exigibilidad establecen que la situación se produce cuando, "el agente, por las circunstancias en que ha realizado el hecho típico, no hubiera podido actuar en forma distinta a como lo hizo, es decir, no le fue posible conducirse motivado de acuerdo con su deber, su comportamiento típico y antijurídico no será reprochable y en consecuencia del mismo no se deduce responsabilidad penal alguna". (Muñoz Rubio y Guerra de Villalaz, 1980:297)

Al trabajar el tema de la no exigibilidad ARANGO DURLING establece que para la doctrina moderna, existen tres supuestos en los cuales puede darse la no exigibilidad de otra conducta distinta, las cuales son el encubrimiento entre parientes el miedo insuperable y el estado de necesidad inculpante si bien no hay referencias en doctrina nacional y derecho comparado con respecto al sabotaje informático no podemos descartar que sea admisible en concreto en el encubrimiento entre parientes (Arango Durling 1998 146)

En cuanto a las eximentes de culpabilidad el Código Penal de 2007 maneja diferentes eximentes el articulo 40 desarrolla la obediencia debida, contemplando una salvedad para los miembros de la fuerza publica que cuando estén en servicio la responsabilidad solo recaerá sobre el superior jerarquico que imparta la orden salvo que sea frente aun delito contra la Humanidad o de desaparición forzosa de personas

> ***Articulo 40*** *No es culpable quien actua en virtud de orden emanada de una autoridad competente para expedirla revestida de las formalidades legales correspondientes que el agente este obligado a cumplirla y que no tenga caracter de una evidente infraccion punible*
>
> *Se exceptuan los miembros de la Fuerza Publica cuando*

estén en servicio, en cuyo caso la responsabilidad recae únicamente sobre el superior jerárquico que imparta la orden. Esta excepción no es aplicable cuando se trate de delitos contra la Humanidad o del delito de desaparición forzada de personas.

El artículo 41 del Código Penal de 2007, menciona el estado de necesidad disculpante, al establecer que:

"Artículo 41. *No es culpable quien realiza un hecho punible no provocado por el agente, para impedir un mal actual e inminente de un bien jurídico propio o ajeno, no evitable de otro modo, siempre que este sea igual o superior al bien jurídico lesionado."*

El artículo 42 del Código Penal de 2007, recopila en un solo enunciado diferentes eximentes de responsabilidad penal, como lo son la coacción, el miedo insuperable y el error de prohibición en la justificación, cosa que no es necesaria porque de la sola inclusión del error de prohibición en el código se entiende que también se admitiría cuando sea frente a una causa de justificación.

"Artículo 42. *No es culpable quien actúa bajo una de las siguientes circunstancias:*

1. Por coacción o amenaza grave, insuperable, actual o

inminente ejercida por un tercero.

2. Impulsado por miedo insuperable, serio, real e inminente de un mal mayor o igual al causado.

3. Convencido erróneamente de que está amparado por una causa de justificación."

Aunque no encontramos tácitamente mención sobre el tratamiento del sabotaje informático frente las eximentes de responsabilidad penal somos de la opinión que dependiendo de las circunstancias de cada caso es posible la aplicación de estas.

2.1.4.4 Formas de Aparición del Delito

2.1.4.4.1 Consumación

El delito de daño según lo ha indicado la doctrina es un delito de resultado, por la destrucción, inutilización o menoscabo que se produce sobre la cosa que constituye un perjuicio económico para su titular, de ahí que la consumación se completa con la realización de la conducta típica prevista. (Cfr. Donna, op. cit.:762).

Sostiene SOLER que la acción en el delito de daño, se entiende que la cosa ha sido destruida cuando por efecto de la acción no existe mas en la sustancia y forma que la especificaban y le daban valor, ni siquiera dice el autor que es necesario que se produzca la destrucción total de la cosa, basta solo dañarla, es decir, disminuir irreparablemente su

calidad o la posibilidad de utilizarla o sus fuerzas naturales. (Cfr. Soler, op. cit.:408)

A juicio de SANTA CELICLIA GARCIA, la consumación del delito de daños se produce "con la objetiva producción del resultado típico, realizando todos los elementos del tipo, consistentes en la destrucción, deterioro, menoscabo o inutilización de la cosa, mermando o eliminando su valor". (Santa Cecilia García, op. Cit.: 359.)

En el caso del tipo agravado del delito de daño estamos ante un delito que se consuma cuando se logre destruir, inutilizar, romper o dañar una cosa utilizando medios o instrumentos informáticos.

En cuanto al sabotaje informático la doctrina ha indicado que la consumación se presenta cuando el sujeto logra destruir, inutilizar o dañar alguna cosa ajena sea esta o no relacionada con una computadora y sus elementos sean físicos o lógicos, como también si se logro el fin mediante la utilización de medios computacionales o relacionados con las tecnologías de la información y comunicación. (CFR Cáceres, op. cit:204-205)

En opinión de otros como lo es, CORCOY BIDASOLO, "se entiende como consumación la lesión de un interés de un sujeto sobre los datos modificados, la mera orden de que se modifiquen los datos tras un lapso de tiempo o en determinadas circunstancias no se podrá considerar como inicio de la ejecución". (En Mir Puig, op. cit:165)

2.2.4.4.2 Tentativa

En el delito de daños, se permite configurar la tentativa, por tratarse de un delito de resultado.

En el tipo agravado de daños relacionado con el sabotaje informático, somos de la consideración de que es admisible la tentativa, sin embargo en cuanto al sabotaje informático escasamente se ha discutido sobre la admisibilidad de la figura de la tentativa.

Sobre este tema CORCOY BIDASOLO, ha establecido que está, "se dará únicamente, en los supuestos en que el sujeto introduzca una orden destinada a provocar, en su momento, la alteración de los datos y esta orden no llega a hacerse efectiva por algún motivo". (en Mir Puig, 165)

Se pueden dar casos en que los comportamientos iníciales de introducción de las rutinas deban ser calificados como actos de ejecución, configuradores de la tentativa o de actos de preparación impunes, cuestión que dependerá de las características del caso concreto.

2.1.4.4.2 Autoría y Participación criminal

El instituto de la Autoría en el Derecho Penal, ha tenido diferentes fundamentos en lo que se refiere a su naturaleza, así en la actualidad la teoría objetiva-material, del dominio final del acto, defendida por el sistema finalista, es del criterio que autor es quien domina finalmente la realización del mismo, es quien decide en líneas generales el

sí y el cómo de su realización.

Para la Doctrina el instituto de la Autoría, al tratar de clasificarla, se divide en tres distintas clases las cuales son:

a. Autoría Directa:

   El autor directo es aquel que realiza personalmente el delito, de manera directa y personal realiza el hecho:

b. Autoría Mediata

   La autoría mediata o indirecta es aquella en donde el autor no realiza directamente y personalmente el delito, en este caso el autor, mediante otra persona, sirviéndose de está, la cual es quien realmente ejecuta directamente el delito.

c. Coautoría

   Esta es el hecho de cuando se realiza en conjunto un delito por varias personas, las cuales han de tener un plan de colaboración conciente y voluntario. Se dice que lo importante de la Coautoría es que el dominio del hecho lo tienen varias personas que, por razón de una división o reparto del trabajo o de los roles dentro del plan se hacen responsables de estos para completar correctamente cometer el ilícito.

La Autoría desde la perspectiva del Código Penal de Panamá según el artículo 43 se entiende que será autor de un delito, quien lo realice por sí mismo o por interpuesta

persona, tal como lo establece el Código Penal de Panamá, al decir:

> *"Artículo 43. Es autor quien realiza, por sí mismo o por interpuesta persona, la conducta descrita en el tipo penal."*

La participación criminal en Derecho Penal contiene dos clases o formas distintivas desde, las cuales se ven desde la perspectiva de la doctrina.

Así entonces se habla de la Inducción, la cual se refiere a la conducta donde la persona (inductor) hace surgir en otra persona (el inducido) la idea de cometer un delito, pero el que decide y domina la realización del mismo es el inducido, también consta la Complicidad, en la cual recaen todas esas contribuciones a la realización del delito con actos anteriores o simultáneos a la realización de este, los cuales nunca podrían ser considerados como figura de autoría, ya que esa ayuda nunca será del mismo grado a lo hecho por el mismo autor del delito.

Nuestra legislación como la doctrina referente a la participación establece la inducción y la complicidad, pero dando una distinción de cómplices primarios y de cómplices secundarios, dependiendo de la actuación de estos dentro del acto ilícito o la comisión del hecho punible.

Para nuestro derecho Penal y se considera que será cómplice primario aquella persona que ayude al autor con una ayuda de tanta importancia, que si no se hubiese prestado, el ilícito o la comisión del hecho punible no se hubiese logrado; así dice el

Sobre la participacion criminal y en especifico sobre el complice primario el Articulo 44 de nuestro Codigo Penal establece

> Articulo 44 Es *complice primario quien toma parte en la ejecucion del hecho punible o presta al autor una ayuda sin la cual el hecho no habria podido cometer el delito*

Por lo que respecta a la figura del cómplice secundario nuestro derecho positivo lo considera como aquel auxilio al autor dado por una persona que no pueda calificarse como el auxilio que da el complice primario y de manera especifica que ayude a ocultar el producto del delito como parte de una promesa hecha con anterioridad a la ejecucion del hecho Asi entonces establece el articulo 45 de nuestro Código Penal al decir sobre el complice secundario que

> *Articulo 45 Es complice secundario*
>
> *1 Quien ayude de cualquier otro modo al autor o a los autores en la realizacion del hecho punible o*
>
> *2 Quien de cualquier otro modo brinde ayude u oculte el producto del delito en cumplimiento de una promesa hecha con anterioridad a su ejecucion*

Sobre la Instigación no hay que recaer en mucha discusión por los motivos de este análisis simplemente se resalta que la posicion de nuestra legislacion no difiere para

nada con la de la doctrina, teniendo como se observa en el artículo 47 de nuestro Código Penal, que dice:

> *Artículo 47. Es instigador quien determina a otro u otros a cometer delito.*

Luego del análisis de la autoría y de la participación criminal, no se puede observar razón para negar la posibilidad de haber casos donde concurra una participación criminal. Teniendo siempre claro que el Autor será aquel que caso la destrucción o inutilización de una cosa ajena utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza.

2.1.4.5 Consecuencias Jurídicas

El que destruya, inutilice, rompa o dañe esa cosa mueble o inmueble ajena, será sujeto a una sanción de uno a dos años de prisión o su equivalente en días-multa o arresto de fines de semana, así como lo establece el artículo 226 del Código Penal.

Igualmente el sancionado por cometer el delito de daños, puede estar sujeto a un aumentó de una cuarta parte a la mitad de la pena en los casos que el sujeto cometa el delito en una situación establecida en el catalogo de agravantes del delito de años, como lo establece el artículo 224 del Código Penal, así el sujeto será sancionado con el aumento previamente descrito si el delito lo hace en perjuicio de un servidor público, a

causa del ejercicio de sus funciones, mediante intimidación o violencia contra tercero, con destrucción o grave daño en residencia, oficina particular, edificio o bien público, bien destinado al servicio público, edificio privado o destinado al ejercicio de algún culto, vehículo oficial, monumento público, cementerio o cosa de valor científico, cultural, histórico o artístico, en una plantación, sementera o en las cercas protectoras de fundos agrícolas o pecuario, mediante la utilización de sustancia venenosa o corrosiva y si el daño total ocasionado supera la suma de dos mil balboas (B/.2,000.00), independientemente del valor del bien que se haya afectado directamente con la acción.

Finalmente el legislador se reservo otro aumento a la sanción en el caso de que el daño se ocasione utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza, donde la pena será de dos a cuatro años de prisión.

Sobre el concurso de delitos en el sabotaje informático no puede desestimarse la posibilidad de encontrar un concurso ideal, como también el real, como también se acepta el caso del delito continuado, por la causación de daños de manera repetida al sistema informático.

En el derecho comparado podemos encontrar que países como Bolivia y Guatemala, toman en cuenta en específico el causar un perjuicio al momento de configurar el delito, mientras países como Alemania o Argentina tipifican el delito desde la partida de que se pueda producir el daño, sin importar o no de que este daño cause perjuicio o no.

Finalmente es necesario destacar que no hay en el derecho comparado muestras de proporcionalidad entre la pena y el daño al momento de configurar el delito, sino más bien mantienen penas pequeñas que no superan los 3 años, salvo que ocurra alguna agravante la cual simplemente eleva la pena a cuatro o cinco años, lo que hace discutible la proporcionalidad o no de la pena frente actos minúsculos de daño o contrario sensu en aquel caso donde el daño sea cuantificado a una cantidad astronómica.

2.1.5 El delito de Sabotaje informático en el Derecho Comparado

2.1.5.1 Alemania

El Código Penal Alemán establece el delito de daños en el artículo 303, en la sección vigésimo-séptima, de la siguiente manera:

"Artículo 303

(1)Quien antijurídicamente dañe una cosa ajena o la destruya, será castigado con pena privativa de la libertad hasta dos años o con multa.

(2) La tentativa es punible."

Por su parte, el artículo 303a, en la misma sección contiene el delito de alteración de datos y el sabotaje informático, mediante la cual se considera conducta punible el borrar, suprimir, inutilizar o cambiar antijurídicamente datos.

El artículo 303a del Código Penal Alemán establece:

"§ Artículo 303a:

(1) Quien borre, suprima, inutilice, o cambie antijurídicamente datos (§ 202 a, inciso 2), será castigado con pena privativa de la libertad hasta dos años o con multa.

(2) La tentativa es punible"

Por otro lado, el artículo 303b sanciona el dañar, inutilizar o modificar un equipo de procesamiento de datos o un medio de datos con el fin de perturbar un procesamiento de datos que sea de importancia esencial para una empresa, industria o autoridad ajena, de la siguiente manera:

"§ 303b. Sabotaje de computadoras

(1) Quien perturba un procesamiento de datos que sea de importancia esencial para una empresa ajena, una industria ajena o una autoridad para

1. cometer un hecho según el § 303 a, inciso 1, o

2. destruir, dañar, inutilizar, eliminar o modificar un equipo de procesamiento de datos o un medio de datos será castigado con pena privativa de la libertad hasta cinco años o con multa.

(2) La tentativa es punible".

De lo antes expuesto, la legislación alemana contempla normas referentes a los

distintos ataques provocados por delitos informaticos o cibernetıcos creando figuras delictivas para proteger la intimidad y el secreto personal tutelando de manera distinta el daño causado al dato dependiendo de si el afectado por ese dano es o no una empresa, industria o autoridad o si el daño se causa sobre un equipo de procesamiento de datos o un medio de datos

Resulta necesario resaltar que la legislacion penal alemana establece claramente que será dato para los efectos de la legislacion asi entonces dato sera todo aquel que se almacene o trasmita de forma electrónica magnética o de otra manera o forma no inmediatamente perceptible esto como lo establece el articulo 202a que castiga tambien la de pirateria informatica en el articulo 202a, de la siguiente manera

§ 202a Pirateria informatica

(1) Quien sin autorizacion se procure para si o para otros datos que no esten destinados para el y que esten especialmente asegurados contra su acceso no autorizado sera castigado con pena privativa de la libertad hasta tres años o con multa

(2)Datos en el sentido del inciso 1 son solo aquellos que se almacenan o trasmiten en forma electronica magnetica o de otra manera en forma no inmediatamente perceptible

De la legislacion Alemana podemos valorar de manera positiva y tratar de incorporar a nuestra legislación una definición de dato como también diferenciar la

alteración de datos del sabotaje informático, a fin de evitar tener algo tan ambiguo como en la actualidad consta en nuestro Código Penal.

2.1.5.2 Argentina

La legislación Argentina no contiene normas específicas sobre la tutela penal contra el delito de sabotaje informático, luego de la reforma introducida por la ley 26.388 de 24 de junio de 2008 se da una reforma para introducir temas de contenido informático al texto del Código Penal.

De esta manera, en la actualidad su punición solo puede darse a través del delito de daño como lo establecen los artículos 183 y 184 del capítulo VII daños, del Título VI de los delitos contra la propiedad, del libro segundo, la norma descrita establece:

> ***ARTICULO 183.*** *- Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado.*
>
> *En la misma pena incurrirá el que alterare, destruyere*

o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

El artículo 183 del Código Penal de Argentina describe la figura simple del delito de daños en su primer párrafo, siguiendo el mismo sistema panameño, el cual en el ultimo párrafo describe igual pena será para quien alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático cualquier programa destinado a causar daños.

De la lectura del segundo párrafo del artículo 183 del Código Penal de Argentina se debe entender que no solo equiparan al delito simple de daños, el causar daños a través de medios informáticos, sino también la venta, distribución, puesta en circulación o introducción en un sistema informático cualquier programa destinado a causar daños, equiparación que no se hace en nuestra legislación penal.

ARTICULO 184. *- La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:*

1. Ejecutar el hecho con el fin de impedir el libre ejercicio

de la autoridad o en venganza de sus determinaciones

2 Producir infeccion o contagio en aves u otros animales domesticos

3 Emplear substancias venenosas o corrosivas

4 Cometer el delito en despoblado y en banda

5 Ejecutarlo en archivos registros bibliotecas museos o en puentes caminos paseos u otros bienes de uso publico o en tumbas signos conmemorativos monumentos estatuas cuadros u otros objetos de arte colocados en edificios o lugares publicos o en datos documentos programas o sistemas informaticos publicos

6 Ejecutarlo en sistemas informaticos destinados a la prestacion de servicios de salud de comunicaciones de provision o transporte de energia de medios de transporte u otro servicio publico

La redacción del articulo 184 del Codigo Penal de Argentina, la cual contiene las agravantes del delito de daños resulta ser una recopilación de agravantes normalmente aceptadas en lo que se refiere al delito de daños asi incluye casos como el de impedir el

ejercicio de una autoridad o en venganza de esta como tambien en el caso de que se pueda causar infección o contagio en animales el uso de sustancias corrosivas o cometer el delito en despoblado o en banda

Resalta en cambio las otras dos agravantes al delito de daños contenidas en el articulo 184 del Código Penal de Argentina ya que debido a su contenido informático es necesario diferenciarlas de las anteriores En estos dos ultimos casos se agravara la pena del delito de daños cuando este sea ejecutado en archivos registros bibliotecas museos o en puentes caminos paseos u otros bienes de uso publico o en tumbas signos conmemorativos monumentos estatuas cuadros u otros objetos de arte colocados en edificios o lugares publicos o en datos documentos programas o sistemas informaticos publicos como también cuando sea Ejecutado en sistemas informáticos destinados a la prestacion de servicios de salud de comunicaciones de provision o transporte de energia de medios de transporte u otro servicio publico

En ambos casos la justificación de las agravantes es comprensible ya que un ataque a datos programas o sistemas informáticos publicos ha de causar grandes perjuicios de igual manera ocurre aquel caso que el ataque ocurra en sistemas informaticos destinados a la prestacion de servicios de salud de comunicaciones de provision o transporte de energia o de medios de transporte u otro servicio publico

2 1 5.3 Bolivia

En materia de delitos informaticos y en especial del sabotaje informatico la Republica de Bolivia, los ubica en el Titulo XII De los Delitos contra la Propiedad Capitulo XI Delitos Informaticos del Libro Segundo del Código Penal

Este criterio segun hemos apreciados no es muy comun en el derecho comparado sin embargo ya que los delitos de sabotaje informatico se regulan en leyes especiales lo que supone que la legislacion Boliviana al ubicarlo en un capitulo autónomo demuestra un interés por tutelar estas conductas relacionadas con las nuevas tecnologias

En este sentido el capítulo XI Delitos informáticos del codigo Penal Boliviano incrimina dos conductas delictivas distintas la llamada manipulación informatica en el articulo 363°bis y el delito de alteracion acceso y uso indebido de datos informáticos en el articulo 363°ter

> *Art 363° bis (MANIPULACION INFORMATICA)*
>
> *El que con la intencion de obtener un beneficio indebido para si o un tercero manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habria sido correcto ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero sera*

sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

La figura de la manipulación informática boliviana tipifica el manipular el procesamiento o transferencia de datos informáticos donde se produzcan resultados incorrectos o eviten uno correcto causando un perjuicio patrimonial a un tercero, en este caso por solo referirse a la manipulación o transferencia de datos, queda incompleta la tutela penal frente los delitos informáticos y cibernéticos en especial el sabotaje informático, pero esta carencia es complementada con el artículo 363ter, que contiene la figura de la alteración, acceso y uso indebido de datos informáticos, así el artículo 363ter establece:

Art. 363° ter.- (ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS).

El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o

multa hasta doscientos días.

El delito de alteración, acceso y uso indebido de datos informáticos como esta tipificado tutela diversos bienes jurídicos, así la intimidad y el patrimonio están

protegidos por constituirse el dato en si el objeto material de este delito y a la vez desde la perspectiva de daño recae la tutela sobre el patrimonio en general al castigar cualquier daño a la computadora o soporte informatico con tal que se vea afectado algun tipo de dato

La legislacion Boliviana a nuestro parecer carece verdaderamente de una tutela especifica del delito de sabotaje informático ya que esta mas bien se concentra en la protección de los datos datos que al parecer se refieren mas bien a los datos personales aunque por estar tipificado el delito de alteración acceso y uso indebido de datos informáticos de una manera ambigua sin definir que sera dato para la legislación se comprende que de este delito se tutela no solo la intimidad desde el punto de vista de la protección de datos sino también al patrimonio desde la perspectiva del causar un perjuicio al tutelar de el daño afectado

2 1 5 4 Chile

La regulacion de la criminalidad informática en Chile se da en la Ley 19223 de 1993 relativa a los delitos informáticos que a continuacion dice lo siguiente

> **Articulo 1° -** El que maliciosamente destruya o inutilice un sistema de tratamiento de informacion o sus partes o componentes o impida obstaculice o modifique su

funcionamiento sufrira la pena de presidio menor en su grado medio a maximo

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema se aplicara la pena señalada en el inciso anterior en su grado maximo

Articulo 2° *El que con el animo de apoderarse usar o conocer indebidamente la informacion contenida en un sistema de tratamiento de la misma lo intercepte interfiera o acceda a el sera castigado con presidio menor en su grado minimo a medio*

Articulo 3° - *El que maliciosamente altere dañe o destruya los datos contenidos en un sistema de tratamiento de informacion sera castigado con presidio menor en su grado medio*

Articulo 4° *El que maliciosamente revele o difunda los datos contenidos en un sistema de informacion sufrira la pena de presidio menor en su grado medio Si quien incurre en estas conductas es el responsable del sistema de informacion la pena se aumentara en un grado*

Esta regulacion especial sobre delitos informaticos de la republica de Chile resulta ser muy interesante porque se que logra tipificar de manera concreta aquellos

posibles ataques donde medie la informática, protegiendo no solo el patrimonio sino que también el derecho a la intimidad.

Por lo que se refiere al sabotaje informático en la legislación chilena se puede observar que dentro de la ley 19233 de 1993, su artículo primero tipifica la conducta del que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, concretando los ataques que afecten al sistema de tratamiento de información en general, dejando como agravante aquellos casos en que se cause un perjuicio en los datos contenidos en aquel sistema.

Igualmente tenemos, la figura autónoma de alteración o destrucción de datos contenidos en un sistema de información, tipificada en el artículo tercero de la ley 19233.

De lo anterior se observa que la presente ley es bastante completa porque regula de manera amplia los ataques relacionados a la informática, lo que en si resulta ser un modelo practico a seguir al momento de buscar guías para la construcción de una nueva legislación penal acorde al desarrollo de las nuevas tecnologías.

2.1.5.5 Colombia

La legislación Colombiana en lo que se refiere al sabotaje informático y a los

delitos informáticos en general no presenta una regulación taxativa de estos, por lo que habrá de aplicarse las normas ya existentes.

En lo que respecta a los datos, la regulación colombiana, le dio el carácter de documento dentro del Código Civil, por lo cual la información contenida en un dato tendrá el mismo valor legal de una carta, tendrá la misma tutela y se podrá utilizar como medio probatorio, debido a la equiparación de los términos.

En lo que respecta a la regulación penal, el sabotaje informático podrá ser castigado siguiendo lo establecido en el delito de daños, contemplado en los artículos artículo 265 y 266, como un ataque contra el patrimonio económico, cuyo texto dice lo siguiente:

> *Artículo 265. Daño en bien ajeno. El que destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bien ajeno, mueble o inmueble incurrirá en prisión de uno (1) a cinco (5) años y multa de cinco (5) a veinticinco (25) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.*
>
> *La pena será de uno (1) a dos (2) años de prisión y multa hasta de diez (10) salarios mínimos legales mensuales vigentes, cuando el monto del daño no exceda de diez (10) salarios*

mínimos legales mensuales vigentes.

Si se resarciere el daño ocasionado al ofendido o perjudicado antes de proferirse sentencia de primera o única instancia, habrá lugar al proferimiento de resolución inhibitoria, reclusión de la investigación o cesación de procedimiento.

El artículo 266 establece agravantes para el delito de daños por otras circunstancias, en la que no se menciona los problemas de sabotaje informático, pero que indirectamente pueden ser sancionados, cuando dice lo siguiente:

Artículo 266. Circunstancias de agravación punitiva. La pena se aumentará hasta en una tercera parte, si la conducta descrita en el artículo anterior se cometiere:

1. Produciendo infección o contagio en plantas o animales.

2. Empleando sustancias venenosas o corrosivas.

3. En despoblado o lugar solitario.

4. Sobre objetos de interés científico, histórico, asistencial, educativo, cultural, artístico, sobre bien de uso público, de utilidad social, o sobre bienes que conforman el patrimonio cultural de la Nación.

En el Capitulo VIII de los Delitos contra la Libertad de Trabajo y Asociación el articulo 199 contempla una modalidad de sabotaje informatico que recae sobre una base de datos de la siguiente manera

> *Articulo 199 Sabotaje El que con el fin de suspender o paralizar el trabajo destruya inutilice haga desaparecer o de cualquier otro modo dañe herramientas bases de datos soportes logicos instalaciones equipos o materias primas incurrira en prision de uno (1) a seis (6) años y multa de cinco (5) a veinte (20) salarios minimos legales mensuales vigentes siempre que la conducta no constituya delito sancionado con pena mayor*
>
> *Si como consecuencia de la conducta descrita en el inciso anterior sobreviniere la suspension o cesacion colectiva del trabajo la pena se aumentara hasta en una tercera parte*

El delito de sabotaje del Codigo Penal colombiano resulta ser interesante por el hecho que dentro de los objetos en los cuales puede recaer el delito establecidos por el legislador colombiano se incluyen bases de datos y soportes logicos ambos objetos demuestran que como situacion especial es posible encontrar que un caso menor de sabotaje informatico que donde el concurso no le de preferencia al delito de daños se

podrá contar con la posibilidad de que una conducta típica de sabotaje informático que tenga un perjuicio cuantificado en una cuantía pequeña resulte ser delito de sabotaje para el Código Penal colombiano, resulta interesante que las bases de datos o soportes lógicos sean considerados dentro de la tipificación de un delito, esto demuestra que el codificador colombiano tomó en cuenta los cambios tecnológicos modernos, aunque resulte ser necesario incluirlos dentro del mismo tipo, ya que sería más sencillo establecer de manera genérica cualquier cosa que no

permita el libre trabajo o asociación.

2.1.5.6 Costa Rica

Por lo que se refiere a Costa Rica, es necesario destacar que desde la ley 4573, de 4 de mayo de 1970, adiciona los artículos 296 bis, 217bis, y 229 bis, al Código Penal, con el fin de reprimir y sancionar los delitos informáticos, incrimina la Violación de las comunicaciones electrónicas, el fraude informático, y la alteración de datos y el sabotaje informático, de la siguiente manera:

> *"Artículo 196 bis.-Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere,*

suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."

"Artículo 217 bis.-Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

"Artículo 229 bis.-Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio

accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años".

La legislación de Costa Rica, es práctica en cuanto a que las infracciones que ha incorporado son de hechos que se realizan muy frecuente y son necesitados de protección penal, y en el caso del sabotaje informático, contempla las conductas de acceder, borrar o suprimir, modificar e inutilizar características esenciales de este delito. En la actualidad este articulado fue subrogado a favor de normas de distinta índole por lo que en la actualidad no se consta con una tutela específica de esta materia.

Así resulta lamentable la realidad de Costa Rica en lo que se refiere a la tutela de la alteración de datos y el sabotaje informático, por ser que durante el año 2002 se reforma el Código Penal de Costa Rica en especifico el artículo 229 Bis, el cual luego de

la reforma quedo transformado en una norma relativa al abandono dañino de animales, ya que la norma relativa a la alteración de datos y al sabotaje informático quedo derogada de manera tácita. En la actualidad se discute en Costa Rica, la existencia o no de la tutela relativa al Sabotaje luego de su derogación, norma que hasta la fecha no a vuelto a ser incluida en el Código Penal de Costa Rica.

2.1.5.7 España

Por lo que se refiere a España, la regulación del sabotaje informático se encuentra en el Capítulo IX "De los Daños" en el Titulo XIII "Delitos contra el patrimonio y contra el orden socio-económico"en el artículo 264 del Código Penal, que establece en el tipo agravado del delito de daños, que a continuación dice lo siguiente:

> ***Artículo 264***
>
> *1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriere alguno de los supuestos siguientes:*
>
> > *1º. Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien*

contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2º. Que se cause por cualquier medio, infección o contagio de ganado.

3º. Que se empleen sustancias venenosas o corrosivas.

4º. Que afecten a bienes de dominio o uso público o comunal.

5º. Que arruinen al perjudicado o se le coloque en grave situación económica.

2. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Así se puede observar que el sabotaje informático en España, consiste en "destruir, alterar, inutilizar o de cualquier otro modo dañar los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

Por otro lado, hay que resaltar que la legislación española contiene no solo la tutela penal de los delitos informáticos sino también armoniza con la tutela del bien

jurídico intimidad y en especifico a la protección de datos de carácter personal, lo que conlleva a los tipos penales integren penal frente a nuevas tecnologías diferentes bienes jurídicos los cuales en principio a veces resultaran ser dispares como la propiedad y la intimidad. Aunque en la práctica se resuelve muy bien.

2.1.5.10 Francia

La legislación penal francesa, en la Sección Séptima "Daños", del Título Séptimo "Delitos contra la propiedad", en el artículo 229bis, tipifica la alteración de datos y sabotaje, de la siguiente manera:

> ***ARTÍCULO 229 BIS.-***
>
> *Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.*
>
> *Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter*

publico se impondra pena de prision hasta de ocho años

Del análisis del texto del articulo 229 BIS del Codigo Penal frances observamos que se tipifica la conducta de acceder de cualquier modo el borrar suprimir modificar o inutilizar sin autorizacion de datos registrados en una computadora aquel acceso o puesta en contacto con un dato encontrado en una computadora ajena sin la debida autorización de su titular supone que igualmente a la propiedad se tutela la privacidad o intimidad del titular de los datos

Las sanciones son de uno a cuatro años en el caso del tipo básico mientras que en el caso que se produzca un daño en el programa se establece una agravante de tres a seis años en la pena, y si llegará a darse el caso en que el programa, base de datos o sistema informatico contuvieren datos de carácter publico la pena es de ocho años

La importancia de cualquier dato de caracter publico su valor intrinseco para el resto de la sociedad y para el Estado en si hace que se justifique el aumento de la pena

2 1 5 11 Guatemala

La legislación Penal de Guatemala establece en materia de delitos informáticos y en especifico a sabotaje informatico en el Titulo VI De los delitos contra el Patrimonio el Capitulo VII De los delitos contra el derecho de autor la propiedad industrial y delitos informáticos capitulo que presenta toda la tutela relacionada a estas nuevas

conductas penales relacionadas con la tecnología.

Así este capítulo contiene diferentes conductas que se asemejan con el delito de sabotaje informático o con los daños por medios informáticos que cuenta con la legislación panameña, conductas que en específico se refieren a la destrucción de registros informáticos, la alteración de programas, la reproducción de instrucciones o programas de computación, registros prohibidos, manipulación y uso de la información como también los programas destructivos.

De estas conductas encontradas en el capítulo VII del Código Penal de Guatemala, como dice el título "de los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos" contiene tipos penales que no se relacionan en específico al tema tratado así la reproducción de instrucciones o programas de computación encontrada en el artículo 274 C, los registros prohibidos que atenten contra la intimidad del artículo 274 D y lo que se refiere la manipulación y uso de la información artículos 274 E y 274 F, son conductas que no se relacionan directamente con el sabotaje informático, sino mas bien con otros delitos informáticos comunes relacionados a la piratería y a la tutela de la intimidad.

Analizando la legislación penal de Guatemala, se observa que diferentes delitos de su código se relacionan con nuestro delito de daños por medios informáticos, así el artículo 274A del Código Penal de Guatemala establece el delito de destrucción de registros informáticos, el cual se relaciona simplemente por el hecho de destruir o

inutilizar un registro informatico seria una conducta tipificada por nuestro delito de daños por medios informaticos un sabotaje informático dirigido especificamente a un registro informático asi como se observa de la lectura del articulo 274 A que establece lo siguiente

> *DESTRUCCION DE REGISTROS INFORMATICOS*
>
> *ARTICULO 274 A Sera sancionado con prision de seis meses a cuatro años y multa de doscientos a dos mil quetzales el que destruyere borrare o de cualquier modo inutilizare registros informaticos*

Otra conducta incluida por el Código Penal de Guatemala que de igual manera se podra tutelar en la panameña es la encontrada en el articulo 274 B la alteracion de programas que hace punible el alterar borrar o de cualquier modo inutilizar las instrucciones o programas de que utilicen las computadoras este delito al igual del delito de daños por medios informaticos de Panamá lo que hace delito cualquier daño que recaiga sobre los programas de la computadora la diferencia radica en que la version de Guatemala esta mucho mas desarrollado el objeto material del delito a diferencia de la panameña, asi entonces el articulo 274 B establece

> *ALTERACION DE PROGRAMAS ARTICULO 274 B La misma pena del articulo anterior se aplicara al que alterare borrare o de cualquier modo inutilizare las instrucciones o*

programas que utilizan las computadoras.

Al igual que el delito de alteración de programas, la legislación penal de Guatemala también contiene el delito de programas destructivos, que tipifica el distribuir o poner en circulación programas o instrucciones destructivas que puedan causar perjuicio a registros o programas de equipos de computación, este delito tiene como fin evitar la propagación de virus informáticos, los cuales sin mucho esfuerzo son capaces de causar mucho daño en un periodo diminuto de tiempo, cabe destacar que resulta atinado la penalidad de este delito encontrado en el artículo 274 G del Código Penal de Guatemala, por ser que pone como mínimo seis meses de prisión y un máximo de cuatro años, sin contar una pena pecuniaria, esta penalidad es favorable por ser que le permite al juez ser capaz de ajustar la penalidad a la gravedad del ataque producido por el virus informático, esta norma igualmente tiene similitudes con el delito de daños informáticos de Panamá por ser que un daño causado por virus informático, así entonces al artículo 274 G establece:

> *PROGRAMAS DESTRUCTIVOS ARTICULO 274 "G". Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.*

La legislacion de Guatemala presenta similitudes con la panamena en el sentido de que ambas castigan los daños causados por medios informaticos pero esa similitud es a su vez marcada diferencia entre ambas legislaciones ya que Guatemala dividi muy claramente las diferentes conductas que pueden llegar a causar ese daño más en cambio Panamá simplemente acepta que cualquier dano causado por medio informático será considerado delito

2 1 5 12 Honduras

Honduras contiene dentro de su Código Penal Libro II parte especial titulo VII delitos contra la propiedad en lo que se refiere al capitulo *X daños* el articulo 254 que tipifica la conducta simple del delito de daños como tambien en su segundo parrafo equipara la pena del delito de daños simples a quien destruya altere inutilice o de cualquier modo dañe los datos programas o documentos electrónicos ajenos contenidos en redes soportes o sistemas informáticos Asi se observa en el articulo 254 del Código penal de Honduras que establece

> *ARTICULO 254 Se impondra reclusion de tres (3) a cinco (5) años a quien destruya inutilice haga desaparecer o de cualquier modo deteriore cosas muebles o inmuebles o animales de ajena pertenencia*

siempre que el hecho no constituya un delito de los previstos en el capitulo siguiente

La misma pena se impondra al que por cualquier medio destruya altere inutilice o de cualquier otro modo dane los datos programas o documentos electronicos ajenos contenidos en redes soportes o sistemas informaticos

De esta redacción es destaca la puesta del daño simple junto con los daños informáticos donde tutelando los datos programas o documentos electronicos encontrados en redes soportes o sistemas informaticos se castiga el daño a estos con la misma pena al delito de daños simple de su legislación Este manera de tipificar el sabotaje informatico equiparando al delito de daño simple tipifican en un párrafo después de la figura simple de daño es parecida a la estructura del delito de dano por medios informáticos con que cuenta Panama, pero a diferencia de nuestro pais Honduras si tipifica correctamente la conducta estableciendo de manera mas estructurada el tipo penal de su delito de daños en especifico su párrafo relacionado al sabotaje informatico

2 1 5 13 México

En lo que se refiere a Mexico en materia de derecho comparado se observa que en el Código Penal Federal contiene en su titulo noveno Revelación de secretos y acceso

ilícito a sistemas y equipos de informática", específicamente en su capítulo segundo "Acceso ilícito a sistemas y equipos de informática" conductas relevantes para esta investigación.

En lo que se refiere en específico a este capítulo se puede encontrar una tutela de diversos bienes jurídicos íntimamente relacionados con la información y la tecnología. El artículo 211 Bis 1 y Bis 2 tipifican el modificar, destruir o provocar la pérdida de información contenida en sistemas protegidos, como también el conocer o copiar la información en estos sistemas, con la diferencia de que en el artículo 211 Bis 1, afectado por esta acción podrá ser cualquier persona, mientras que en el artículo 211 Bis 2 el ataque debe darse contra sistemas protegidos que sean del Estado. Así entonces el artículo 211 Bis 1 establece:

> *ARTICULO 211 BIS 1 - Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.*

El artículo 211 Bis 2, resulta ser idéntico al artículo 211 Bis 1, simplemente difiriendo por ser que el objeto material en este se refiere a sistemas informáticos protegidos de propiedad del Estado, así establece el articulo al decir:

> *ARTICULO 211 BIS 2 - Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

El artículo 211 Bis 3, resulta tener la misma estructura en el tipo como los artículos anteriores simplemente tomando en cuenta que el sujeto activo debe estar autorizado para acceder a esos sistemas y equipos informáticos del Estado, así dice el artículo 211 Bis 3:

> *ARTICULO 211 BIS 3 - Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que*

contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

En lo que se refiere a los artículos 211 Bis 4 y 5 hay que mencionar que estos están dirigidos a tutelar de manera especial las instituciones que integran el sistema financiero, el cual es definido en el mismo Código Penal Federal, así entonces el artículo 211 Bis 4 y el Bis 5 establecen:

ARTICULO 211 BIS 4 - Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo

de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

ARTICULO 211 BIS 5 - Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan,

se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

De la lectura del artículo 211 Bis 4 y 5 aunque ambos tengan como mira el proteger los sistemas informáticos de instituciones que integran el sistema financiero, el

artículo 211 Bis 4 esta dirigido en especifico al acceso no autorizado, mientras que el artículo 211 Bis 5 se refiere al acceso autorizado del sujeto activo.

Por último hay que mencionar que el artículo 211 Bis 7, prevé una agravante para las penas en los articulo ya mencionados, en el caso de que la información que se obtenga sea utilizado en provecho propio o ajeno, así establece el artículo 211 Bis 7, al decir:

> *ARTICULO 211 BIS 7 - Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.*

Del análisis de la legislación mexicana en materia de delitos informáticos y en especifico al sabotaje informático no podemos negar que es muy detallada en comparación con la legislación panameña, pero a nuestra opinión contiene demasiados artículos para conducta tan reducida como lo es el sabotaje informático o simplemente el ocasionar un daño por medio informáticos como esta tipificado en Panamá.

2.1.5.14 Nicaragua

En lo que se refiere a Nicaragua, podemos observar que el Código Penal no contiene normas especificas contra los delitos informáticos, lo que ni contra el sabotaje informático en especifico, lo que ciertamente es desventajoso y posiblemente presente

problemas interpretativos, aunque se contempla el delito de daños, en el Capítulo VIII, del Titulo IV "Delitos contra la propiedad" en el artículo 293, que establece lo siguiente:

> *Art. 293.- Comete delito de daño el que destruyere, inutilizare o deteriorare una cosa ajena, cuyo valor exceda de cien córdobas cuando el hecho no estuviere sancionado como delito en otros capítulos de este Código. El autor del delito de daño, sufrirá la pena de multa de cien a quinientos córdobas cuando el valor de la cosa dañada no exceda de un mil córdobas, sin perjuicio de la indemnización por el daño causado.*
>
> *Si el valor de la cosa fuere mayor de un mil córdobas, la pena será arresto de 10 días a 3 meses y multa equivalente a la tercera parte del valor de la cosa dañada sin perjuicio de la indemnización por el daño causado.*

De la lectura del artículo 293 del Código Penal de Nicaragua podemos decir que se podrá castigar las conductas típicas del sabotaje informático con la redacción del artículo, no obstante esta situación no es la más ventajosa para la legislación penal en general, ya que esta norma parece estar establecida como una red que permite atrapar cualquier ilícito que cause daño al patrimonio no tipificado de manera especifica en el Código Penal, lo que hace posible la falta de una proporción en caso de los daños que

pudiesen provocarse de un sabotaje informatico

El delito de daños segun la legislacion de Nicaragua tiene diferentes agravantes a la conducta simple estas en algunos casos especificos podran relacionarse igualmente a un caso de sabotaje informatico

Las agravantes del delito de daños en el Código Penal de Nicaragua, segun el articulo 294 suponen un aumento de la pena para el delito de prision de nueve meses a tres años si en el hecho ocurriere el caso de que el daño se ejecute para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones cuando se efectue empleando electricidad o sustancias venenosas o corrosivas o produciendo infección o contagio en animales domésticos de cualquier especie ambas muy parecidas a la estructura de las agravantes para el delito de daño en el Codigo Penal de Panamá igualmente se tiene en Nicaragua como agravante el caso que se perpetre en cuadrilla (con el auxilio de dos o mas personas) cuando el daño se cause en archivos registros bibliotecas museos templos puentes caminos paseos y otros bienes de uso publico o en signos conmemorativos monumentos estatuas cuadros y otros objetos de arte colocados en edificios o lugares publicos o en tumbas y demas construcciones de los cementerios

De la observancia de estas agravantes es aceptable que se den en algunos casos de sabotaje informatico cuando el perjuicio sea causado sobre alguno de estos bienes de especial cuidado igualmente se podrá dar en el caso de la agravante de empobrecimiento

que contiene el artículo 295 del Código Penal de Nicaragua, la cual establece:

De igual forma, el artículo 295, se refiere al delito de daño en los siguientes términos:

> *Art. 295.- Si por razón del daño se causaren grandes pérdidas en los bienes del ofendido, que causaren su empobrecimiento, la pena será de 2 a 5 años de prisión, sin perjuicio de la indemnización correspondiente.*

De lo antes expuesto se desprende, que los preceptos señalados no hacen mención especifica a los delitos informáticos en general, ni mucho menos del sabotaje informático en específico, por lo que desde el año 2005 en Nicaragua se discute sobre la posibilidad de crear una ley especial sobre delitos informáticos.

En este sentido, el texto del anteproyecto de Ley especial sobre delitos informáticos de Nicaragua contiene dos normas aplicables al delito de sabotaje informático, un delito de daño a datos o sistemas informáticos y otro de sabotaje informático en sentido estricto.

En el artículo 6 del anteproyecto de ley especial sobre delitos informáticos de Nicaragua, contiene el delito de daño a datos o sistemas informáticos, que se centra en el causar daño, alterar o inutilizar los datos o las funciones sean parciales o totales de un sistema informático, cuyo texto dice así:

> ***Arto. 6.- Daño a datos o sistemas informáticos.*** *Comete delito*

de daño a datos o sistemas informáticos, el que sin autorización destruye, dañe, altere o inutilice los datos o funciones parciales o totales de los sistemas informáticos integrados en equipos físicos, será sancionado con la pena de uno a tres años de prisión.

Esta figura resulta ser un típico sabotaje informático, ya que se refiere al acto de causar la destrucción, daño, alteración o inutilización de los datos o funciones parciales o totales de los sistemas informáticos integrados en un equipo físico, este delito será aplicable a aquellos atentados contra los datos encontrados en cualquier sistema informático, no distingue si el objeto no incluye aquellos soportes informáticos del sistema, por lo que un atentado contra un USB o disco de información igualmente será penado por este artículo.

En lo que se refiere al artículo 7 del texto de anteproyecto de ley especial de sobre delitos informáticos de Nicaragua, establece un delito de sabotaje informático él cual tiene como figura simple de la conducta al delito de daño a dato o sistema informático, el cual dice así:

Arto. 7.- Sabotaje informático. *Comete delito de sabotaje informático, cuando los hechos descritos en el artículo anterior recaigan sobre los sistemas informáticos de los ficheros automatizados que almacenan datos o información de carácter*

destinada a los servicios públicos, será sancionado con la pena de tres a ocho años de prisión.

Este delito de sabotaje informático, según lo que establece el texto del anteproyecto del ley sobre delitos informáticos de Nicaragua, resulta ser más bien una agravante del mismo delito de sabotaje informático común, aunque por alguna razón en Nicaragua prefieren llamar al sabotaje informático delito de daño a los datos o sistemas informáticos y reservarse el nombre de sabotaje informático para aquellos casos especiales donde el perjuicio recae sobre sistemas informáticos de ficheros automatizados que almacenan datos o información de carácter destinada a los servicios públicos con el respectivo aumento en la penalidad por la necesidad de asegurar cierto grado de prevención frente un atentado que puede causar grandes estragos al causar directamente perjuicio sobre información o datos relacionados a servicios públicos.

2.1.5.15 Paraguay

En materia de sabotaje informático, el Código Penal de Paraguay contiene en su libro segundo parte especial hechos punibles, Libro Segundo Parte Especial, Título II: Hechos punibles contra los bienes de la persona Capítulo II Hechos punibles contra otros derechos patrimoniales, contiene lo relacionado a los delitos informáticos y en especial al Sabotaje informático.

La estructura del Codigo Penal paraguayo resulta muy interesante ya que correctamente separa de los delitos contra el patrimonio clásicos estos delitos que aunque atenten contra el patrimonio en si por su misma naturaleza y complejidad es mejor no relacionar tan directamente con las clasicas concepciones de los delitos contra el patrimonio

Antes de desarrollar el sabotaje informatico en si es necesario mencionar que la legislacion paraguaya a parte del sabotaje informatico tambien tipifica otra conducta relacionada con los delitos informaticos asi el articulo 174 del Codigo Penal de Paraguay contiene el delito de alteracion de datos el cual esta concebido desde la perspectiva del derecho de disposicion que tiene toda persona sobre sus datos esto es importante mencionar porque no solo se tutelan los datos en si sino tambien se puede observar que muy atinadamente definen que sera dato para el CódigoPenal asi

Articulo 174 Alteracion de datos

1 El que lesionando el derecho de disposicion de otro sobre datos los borrara suprimiera inutilizara o cambiara sera castigado con pena privativa de libertad de hasta dos años o con multa

2 En estos casos sera castigada tambien la tentativa

3° Como datos en el sentido del inciso 1 se entenderan solo

aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible.

Es novedoso, la definición legal de dato, que permite determinar su alcance legal para evitar todo tipo de interpretaciones distintas, al igual que permite delimitar la conducta de alteración de datos, en el Código Penal de Paraguay, es decir, todos aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible, definición acorde a la definición legal de dato encontrada en otras legislaciones.

En cuanto al sabotaje informático, la legislación Paraguaya, lo denomina "sabotaje de computadora", en el artículo 175, que dice lo siguiente:

Artículo 175.- Sabotaje de computadoras

1º El que obstaculizara un procesamiento de datos de importancia vital para una empresa o establecimiento ajenos, o una entidad de la administración pública mediante:

1. un hecho punible según el artículo 174, inciso 1º; o

2. La destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra parte accesoria vital, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2 En estos casos sera castigada tambien la tentativa

El delito de sabotaje de computadoras esta relacionado con el articulo 174 que sanciona la alteración de datos y se establece como conducta la de obstaculizar un procesamiento vital para una empresa o establecimiento ajeno o una entidad de la administración publica, acción que se puede cometer mediante un acto de alteracion de datos como lo establece el articulo 174 del Código Penal paraguayo inciso primero sobre la alteración de datos o sino en aquella conducta que destruya inutilice sustraiga o altere una instalación de procesamiento de datos de una unidad de almacenamiento o de otra parte accesoria vital

El sabotaje de computadoras paraguayo integra para si los elementos de la alteración de datos por ser que utiliza la definicion de dato que contiene ese delito como también incluye la acción comun de sabotaje al tipificar que la conducta punible será para quien destruya, inutilice sustraiga o altere una instalación de procesamiento de datos una de unidad de almacenamiento o de otra parte accesoria vital este delito mantiene como objeto material no solo el dato en si tomado de la alteración de datos sino que incluye todos los elementos posibles de un sistema o red informática, como tambien la misma computadora en si con tal que sea un elemento vital

2 1 5 16 Perú

El Codigo Penal del Peru destina una tutela a los delitos informáticos en el Capitulo X del Titulo V De los delitos contra el patrimonio mediante la Ley 27309 de 2000 que adiciono al Codigo Penal estos comportamientos delictivos

En primer lugar tenemos que el denominado delito informático se contempla en el artículo 207A de la siguiente manera

Articulo 207 A Delito Informatico

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 informacion en transito o contenida en una base de datos sera reprimido con pena privativa de libertad no mayor de dos años o con prestacion de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas

Si el agente actuo con el fin de obtener un beneficio economico sera reprimido con pena privativa de libertad no mayor de tres años o con prestacion de servicios comunitarios no menor de ciento cuatro jornadas

Como se desprende de lo anterior el articulo 207 A del Codigo Penal tipifica la conducta de utilizar o ingresar indebidamente a una base de datos sistema o red de computadoras o cualquier parte de la misma conducta que debe tener la finalidad de diseñar ejecutar o alterar un esquema u otro similar o para interferir interceptar acceder o copiar informacion en tránsito o contenida en una base de datos

Se observa que la norma contempla de manera amplia el delito informático por lo que hubiera sido mas práctico que se incriminaran por separado el acceso indebido del acceso indebido que tiene como fin afectar los datos o información contenida en un sistema

Otro de las figuras delictivas contempladas en la legislación Peruana es el delito de alteracion daño y destruccion de base de datos sistema, red o programa de computadoras que es el que verdaderamente se asemeja a lo que deberia ser el sabotaje informatico el cual dice lo siguiente

> *Articulo 207 B Alteracion daño y destruccion 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 sera reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa*

dias multa

El sabotaje informático desde el punto de vista de la legislacion Peruana, consiste en aquellos actos en los que se utiliza se ingresa se o interfiere indebidamente con una base de datos sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos dañarlos o destruirlos hechos que son positivos pues incluye el daño fisico a la computadora como tambien los realizados a todos los elementos que pudiesen ser objeto de este delito sea el dato en si el sistema, red o algun programa de la misma computadora asi se tutela en todos los sentidos la computadora y sus elementos

Por su parte el artículo 207 C contiene una serie de agravantes relacionadas a los delitos informaticos y en especifico al sabotaje informático en si por lo que establece agravantes que dependen de la calidad del sujeto cuando el sujeto activo sea una persona que obtenga información privilegiada gracias al ejercicio de su cargo como tambien en relación al peligro que suponga el tener dicha información cuando este acto pueda poner en peligro la seguridad de la nación

El articulo 207 C dice lo siguiente

Artículo 207 C Delito informatico agravado

En los casos de los Articulos 207 A y 207 B la pena sera 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 informacion privilegiada obtenida en funcion a su cargo

2 El agente pone en peligro la seguridad nacional

Es necesario señalar que el sabotaje informático resulta incriminado de manera limitada, ya que no tiene alcance para los delitos cibernéticos en general como también es necesario detallar mas claramente el objeto material del delito el definir el termino dato en estos casos resulta muy importante para evitar problemas de interpretacion como también evitar que se no se pueda distinguir la diferencias entre las dos figuras creadas en el titulo de los delitos

2 1 5 17 Venezuela

La regulación penal de los delitos informáticos en la Republica de Venezuela, aparece en la ley especial de 30 de octubre de 2001 publicada en Gaceta Oficial numero 37 313

En cuanto al delito de sabotaje informático la ley especial contra los delitos informáticos regula cuatro conductas distintas relacionadas con el sabotaje informatico a saber el sabotaje o daño a sistemas en el artículo 7 el favorecimiento culposo del sabotaje

o daño en el artículo 8. el acceso indebido o sabotaje a los sistemas protegidos en el artículo 9 y la posesión de equipos.

El artículo 7 que incrimina el sabotaje o daño a sistemas dice lo siguiente:

> *" Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.*
>
> *Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.*
>
> *La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión intencional, por cualquier medio, de un virus o programa análogo.*

Para el derecho penal Venezolano, plasmado en la ley especial contra los delitos informáticos, la figura del sabotaje informático como se ha establecido previamente es

divida en cuatro distintas figuras su figura simple tipifica como conducta la intención de destruir dañar modificar o realizar cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologias de informacion o cualesquiera de los componentes que lo conforman igualmente estableciendo como agravante el destruir dañar modificar o inutilizar la data o la informacion contenida en cualquier sistema que utilice tecnologías de información o en cualesquiera de sus componentes esta configuración de la figura simple del sabotaje informatico resulta muy interesante porque utiliza el termino de tecnologia de la información a fin de poder permitir la persecución de cualquier atentado contra algun sistema o medio informático igualmente incluye bajo su tutela los datos o información que este contenida en el sistema informático

A nuestro modo de ver es innecesario el contemplar en tres párrafos distintos todas las posibles formas del sabotaje informático ya que hubiera podido señalarse en una sola, aunque esto demuestra que el codificador ha preferido individualizar todas las posibles conductas a fin de permitir una mayor claridad posible al momento de aplicar la ley

Por otro lado tenemos que en la figura simple del sabotaje informático se incluye como agravante especial el supuesto de que el sabotaje informático se realizare mediante la creación introducción o transmisión intencional por cualquier medio de un virus o programa análogo

Por otro lado esta ley contempla el tipo culposo del delito de sabotaje informático

en el artículo 8 d ella siguientes manera:

> *Artículo 8. Favorecimiento culposo del sabotaje o daño. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.*

De igual forma, tenemos que el artículo 9 contempla en el sabotaje informático la figura del acceso indebido o sabotaje a sistemas protegidos, de la siguiente manera:

> *Artículo 9. Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.*

Por último la ley especial contra los delitos informáticos eleva a categoría de delito, la posesión de equipos para realizar el sabotaje informático, en el artículo 10, que

dice lo siguiente:

> *Artículo 10. Posesión de equipos o prestación de servicios de sabotaje. Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.*

La incriminación de la conducta de prestar servicios de sabotaje, a mi juicio resulta innecesario, porque la acción en sí del sabotaje informático no distingue si es hecho como servicio a favor de otro o no simplemente le interesa el daño, si se desea evitar que las personas presten servicios de sabotaje informático resulta más práctico agregarlo como una agravante, pero esto de por sí es innecesario, por que las figuras de la autoría y la participación criminal se encargarían de repartir la suficiente responsabilidad para la persona que contrata el servicio de sabotaje informático como también de quien lo haga.

2.1.5.18 Uruguay

En Uruguay el derecho penal no ha legislado la materia de los delitos informáticos en el Código Penal, ni mediante alguna legislación especial. Así entonces delitos de sabotaje informático se tendrán que analizar desde la perspectiva del delito de daños.

El Código Penal de Uruguay, en el Capítulo VI del Título XIII"Delitos contra la Propiedad mueble o inmueble"se castiga el delito de daño, en el artículo 358, cuando se destruya, deteriore, inutilice todo o parte de una cosa mueble o inmueble ajena.

De la norma, se determina que se puede castigar aquellos ataques que produzcan daños sobre cosa ajena sea mueble o inmueble independientemente de que el daño sea mediante computadora o medios informáticos, igualmente se permitiría aplicar delito de daño si ese objeto ajeno es algún objeto material típico en el delito de sabotaje informático.

Así entonces el artículo 358 que tipifica la figura simple del delito de daños establece:

> *ARTICULO 358. (Daño)*
>
> *El que destruyere, deteriorare o de cualquier manera inutilizare en todo o en parte alguna cosa mueble o inmueble ajena, será castigado, a denuncia de parte, cuando el hecho no constituya delito más grave, 20 U.R. (veinte unidades reajustables) a 900*

U R (novecientas unidades reajustables) de multa

Cabe destacar que la legislacion de Uruguay en materia del delito de daños las agravantes son muy parecidas a las que contiene la legislacion panameña como lo son el agravar en caso de que el daño recaiga sobre objetos publicos si es contra un funcionario por el ejercicio de su deber aunque resulta interesante una agravante que establece que si el delito se cometiera con violencia o amenazas o por empresarios con motivo de paros o por obreros con motivo de huelga lo cual demuestra el interés de evitar que en un paro o huelga se de una escalada de violencia por los participantes El articulo 359 del Código Penal de Uruguay dice asi

ARTICULO 359 (Circunstancias agravantes)

Se procede de oficio y la pena sera de tres meses de prision a seis años de penitenciaria cuando concurran las circunstancias agravantes siguientes

1° Si mediare alguna de las circunstancias previstas en los incisos 3 y 4° del articulo 59

2° Si el delito se cometiera sobre cosas existentes en establecimientos publicos o que se hallaren bajo secuestro o expuestas al publico por la necesidad o por la costumbre o destinadas al servicio publico o de utilidad defensa

beneficencia o reverencia publicas

3° Si el daño se efectuare por venganza contra un funcionario publico un arbitro un interprete un perito o un testigo a causa de sus funciones

4° Si el delito se cometiera con violencia o amenazas o por empresarios con motivo de paros o por obreros con motivo de huelga

Para terminar en la actualidad se discute en Uruguay el tema de los delitos informaticos fin de poder actualizar el Codigo penal frente a este tipo de delincuencia moderna, a fin de evitar lagunas legales y actualizar el Codigo penal a los requerimientos de esta época

CAPÍTULO 3

MARCO METODOLÓGICO

3.1 Tipo de Investigación

Esta investigación es de carácter documental, ya que es un análisis de la información escrita relacionada a los Delitos Informáticos, la Cibrecriminalidad y su relación con el delito de Daños a fin de poder entender como se relacionan entre sí estos objetos de estudio, en lo relacionado a posturas, diferencias y en general al estado del conocimiento relacionado a este tema.

Del estudio de las numerosas obras del Derecho Comparado y de distintas legislaciones internacionales relacionadas con el objeto de estudio, podemos entonces analizar el tratamiento que da la doctrina y el derecho penal extranjero en si al delito de daños y su relación con el cibererimen y los delitos informáticos.

A su vez esta investigación es Descriptiva, ya que estudiamos y analizamos el tratamiento que se da en nuestro país al delito de daños, en especial a aquellos casos relacionados con la criminalidad informática, buscando entender las cualidades y atributos del fenómeno, como también describir los problemas que son inherentes a este delito y su tratamiento en Panamá.

3.2 Sujetos o Fuentes de Información

En el investigar se entiende por fuente de información aquellos conocimientos,

datos o elementos que nutren el desarrollo de la investigacion en si

Asi por ser que esta investigacion es de caracter documental la fuente primaria de información ha sido obtenida del analisis de obras existentes en la materia, el estudio de leyes pasadas y vigentes de nuestro pais y del extranjero Aunque elemento importante de la investigación fueron los datos proporcionados por la Sección de Informática forense encontrada en la Subdireccion de Criminalistica del Instituto de Medicina Legal y Ciencias Forenses

3 3 Variables o Fenómenos de Estudio

Una variable es una propiedad que puede variar y cuya variación es susceptible de medirse u observarse

En nuestro trabajo hemos establecido como enunciado que el delito de sabotaje informático requiere ser regulado como una figura delictiva autonoma en nuestra legislación de manera que se proteja eficazmente el patrimonio economico de los afectados desde la perspectiva tecnológica constituyendo por lo tanto nuestra **variable independiente**

Por su parte la **variable dependiente** en nuestra investigacion es que la inadecuada regulación del delito de sabotaje informático se equipara con un simple delito de daños

3 3 1 Del Concepto

Esto es la abstracción articulada de palabras las cuales facilitan el entender alguna idea, nocion pensamiento requerido en la investigacion asi desarrollaremos

Delito Aquella accion atipica y antijuridica y culpable analizada desde el punto de vista del sistema finalista

Delito de Daño Aquel delito que cometido por que daña, destruya o inutilice una cosa mueble o inmueble ajena, que desde este trabajo se verá bajo la optica del Codigo Penal de 1982 y el de 2007 como también el derecho comparado

3 3 2 Definición Operacional

Nuestra definicion de trabajo sera lo que nuestros elementos y datos que arroje nuestra investigacion asi entonces nos centramos en los datos proporcionados en lo referente al año 2008 y 2009 de la Sección de Informatica Forense del Instituto de Medicina Legal la cual tiene como funcion atender las solicitudes de apoyo técnico provenientes de la Policia, como tambien del Ministerio Publico a fin de confeccionar informes tecnicos correspondientes a las investigaciones originadas por faltas cometidas a traves de equipo de alta tecnologia en especifico lo relacionado al delito de daños

3 3 3 Definición

Para medir las variables hemos utilizado los datos proporcionados por la seccion de Informatica Forense del Instituto de Medicina Legal en lo relacionado a Delito de daños desde la perspectiva de la tutela al patrimonio y a la investigacion del sabotage informático

3 4 Descripción de los Instrumentos

Se utilizaron las estadisticas de la Sección de Informatica Forense del Instituto de Medicinal Legal y Ciencias Forenses en lo relativo a la cantidad de casos relacionados con el objeto de estudio durante el periodo del 2008 y el transcurso del año 2009 hasta el mes de septiembre

3 5 Tratamiento de la Información

La información recabada para esta investigación se refleja en gráficas a partir de datos obtenidos de la Sección de Informática Forense del Instituto de Medicina Legal y Ciencias Forenses entidad que cuenta con personal idoneo en el tratamiento de la delincuencia informática

Luego de obtenida y seleccionada la información se tabularon los datos

representando en graficas los resultados que manifiestan la problemática de la delincuencia informatica en nuestro pais

CAPÍTULO 4

ANÁLISIS E INTERPRETACIÓN DE DATOS

4 1 Generalidades

En esta sección se desarrolla la información obtenida de la sección de informática forense del Instituto de Medicina Legal por ser la fuente más clara al momento de entender el tratamiento que se da al delito de daños y al sabotaje informático en general desde una perspectiva informática

Así nos centramos en el trabajo de la Sección de Informática Forense del Instituto de Medicina Legal debido al alto grado de preparacion tecnica y doctrinal de sus miembros y por los distintos procedimientos que tienen para investigar cualesquiera ataque logrado a traves de medios informáticos sea fraude a través de computadora falsedades de carácter informatico daños o modificaciones de programas o datos computarizados terrorismo secuestro etc

Es necesario mencionar que al momento de hacer esta investigación no encontramos jurisprudencia nacional que relacionada con el delito de daños cometido por medios informáticos lo cual hace suponer que desde la puesta en vigencia del Código no ha llegado ningun delito de daño cometido por medios informaticos o de sabotaje a la esfera judicial

Igualmente se expresa que aunque se cuenta con una fiscalia especializada en

delitos contra la propiedad intelectual y seguridad informática al momento de recabar información sobre esta no encontramos investigación alguna ya que aunque este constituida como tal no han recibido casos relativos a la seguridad informatica para investigar

Por la falta de denuncias relativas a seguridad informática en sentido estricto y por tratar de buscar una fuente más directa y de uso más comun en materia de delitos informáticos nos centramos en los resultados de investigar la actuación de la sección de informática forense del instituto de medicina legal antigua división de la antigua Policía Técnica Judicial en la cual sus funcionarios fueron instruidos en temas de investigación informática y forense por parte de diversas agencias de investigación como lo son la Guardia Civil de España o agencias como el FBI de Estados Unidos muestra que en Panamá, por lo menos contamos con agentes especializados para lograr una adecuada investigación relacionada con delitos informaticos o de relación al cibercrimen

4 2 Interpretacion de los datos obtenidos

El analisis de la información provista por la seccion de informatica forense del Instituto de Medicina Legal resulta ser muy interesante así tenemos que durante el año de 2008 se investigaron un total de 135 casos mientras que durante el periodo de enero hasta septiembre de 2009 se habian investigado un total de 99 casos con lo que se demuestra que al ritmo que se va este año se mantendria la cifra de casos investigados por

la seccion aunque seria posible que aumentara la cantidad de casos relacionados al cibercrimen investigados en Panamá

De la totalidad de casos investigados delitos relacionados al patrimonio no eran la mayoria ya que solo el 32 59% de los casos investigados durante el año 2008 causaron perjuicios sobre el patrimonio de algun sujeto mientras que en lo que va hasta la fecha de septiembre de 2009 se nota un incremento mayor en la incidencia de casos relacionados al patrimonio por ser que del total investigado un 37 37% son relacionados al patrimonio

Probablemente el mayor dato de importancia en esta investigación es el hecho de que como entiende de la doctrina y de la misma practica y labor de la sección de informática forense del Instituto de Medicina Legal los casos de sabotaje informático no son reportados para ser investigados por el personal idóneo o simplemente no son investigados ya que de una totalidad de 135 casos investigados en el 2008 solo se investigo un solo caso que fuera por daño no estando demas mencionar que hasta septiembre de 2009 no se habia investigado ningun caso relacionado a daños

Esto resulta ser preocupante porque casos de sumo interés nacional como lo es el ataque a computadoras de una entidad publica como lo fue el caso del sabotaje a las computadoras y página de internet de la Asamblea Nacional de Diputados no fue investigado con la ayuda del personal idóneo para este tipo de investigaciones personal preparado por agencias policiales de Europa y Estados Unidos para combatir contra los

flagelos comunes de una sociedad cada vez mas inmersa en la tecnología y la informática. Por no decir de otros casos que acaban como meros rumores como por ejemplo la supuesta desaparición de la lista de morosos del IDAAN, la cual supuestamente debido a un virus en el sistema se perdió.

El hecho de constatar la existencia de un solo caso reportado en estos dos últimos años demuestra que en casos relacionados a daños informáticos, al sabotaje informático, no se están haciendo las respectivas denuncias, ya que como se observa de la cantidad de casos investigados, el uso de la tecnología por parte de los criminales ya es algo común en Panamá por la cantidad de diversos casos relacionados al cibercrimen investigados en estos últimos 2 años.

4.3 Presentación de Gráficas

Gráfica No.1 Delitos Informáticos Investigados

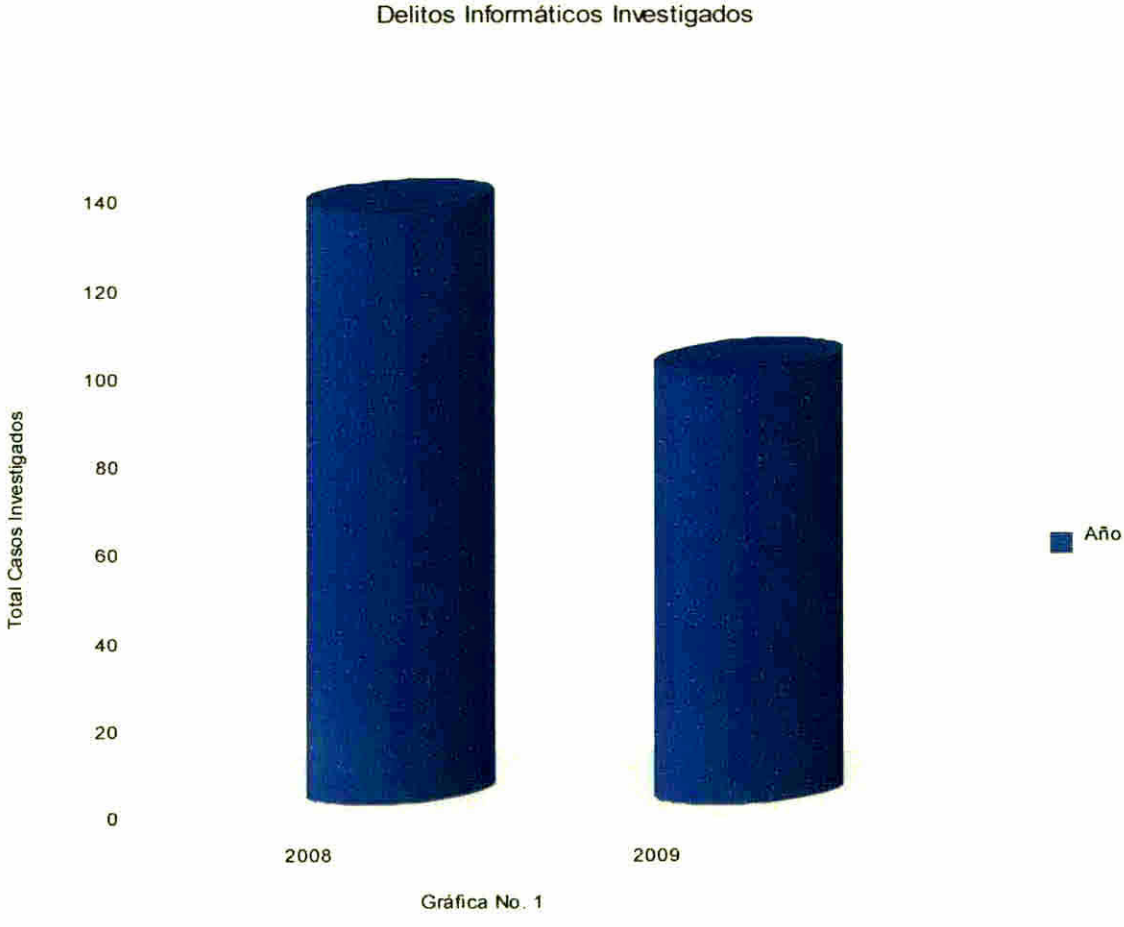
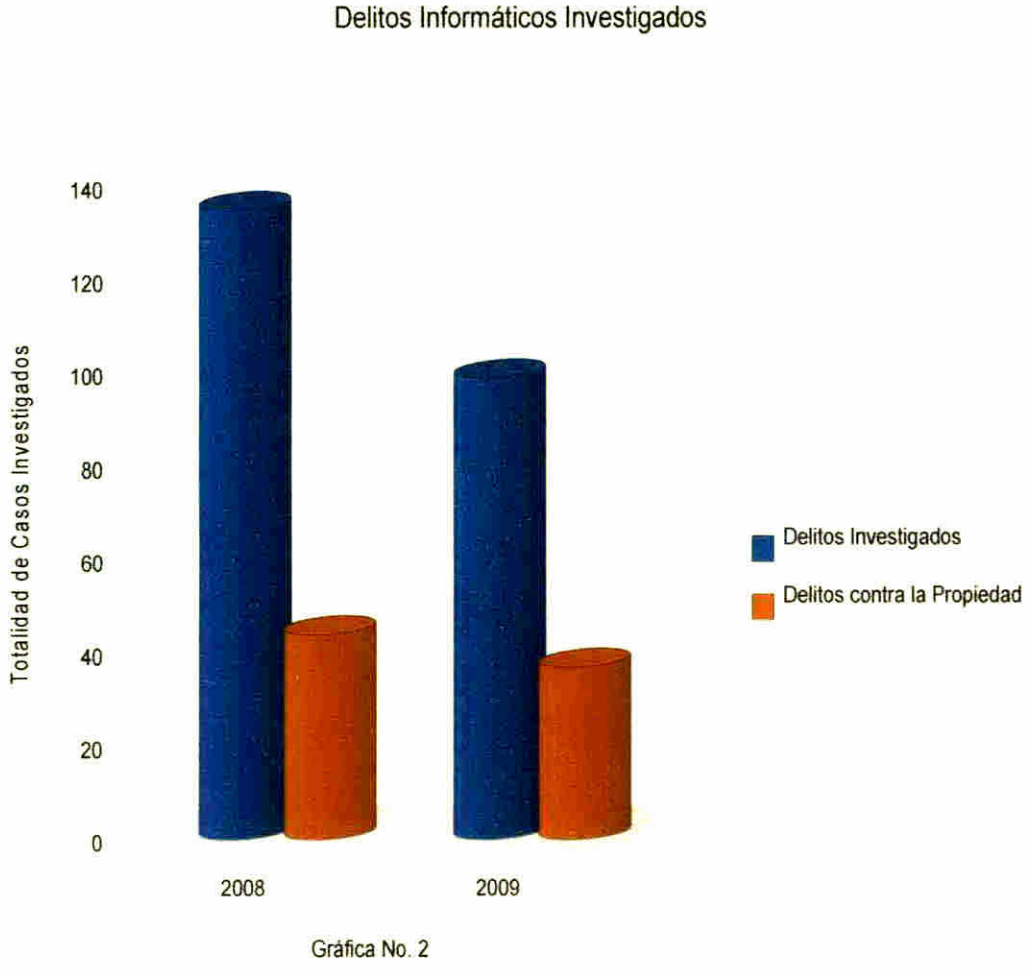


Ilustración 1

Gráfica No. 2 Delitos Informáticos Investigados



Gráfica No. 2

Ilustración 2

Gráfica No. 3 Delitos Informáticos Investigados 3

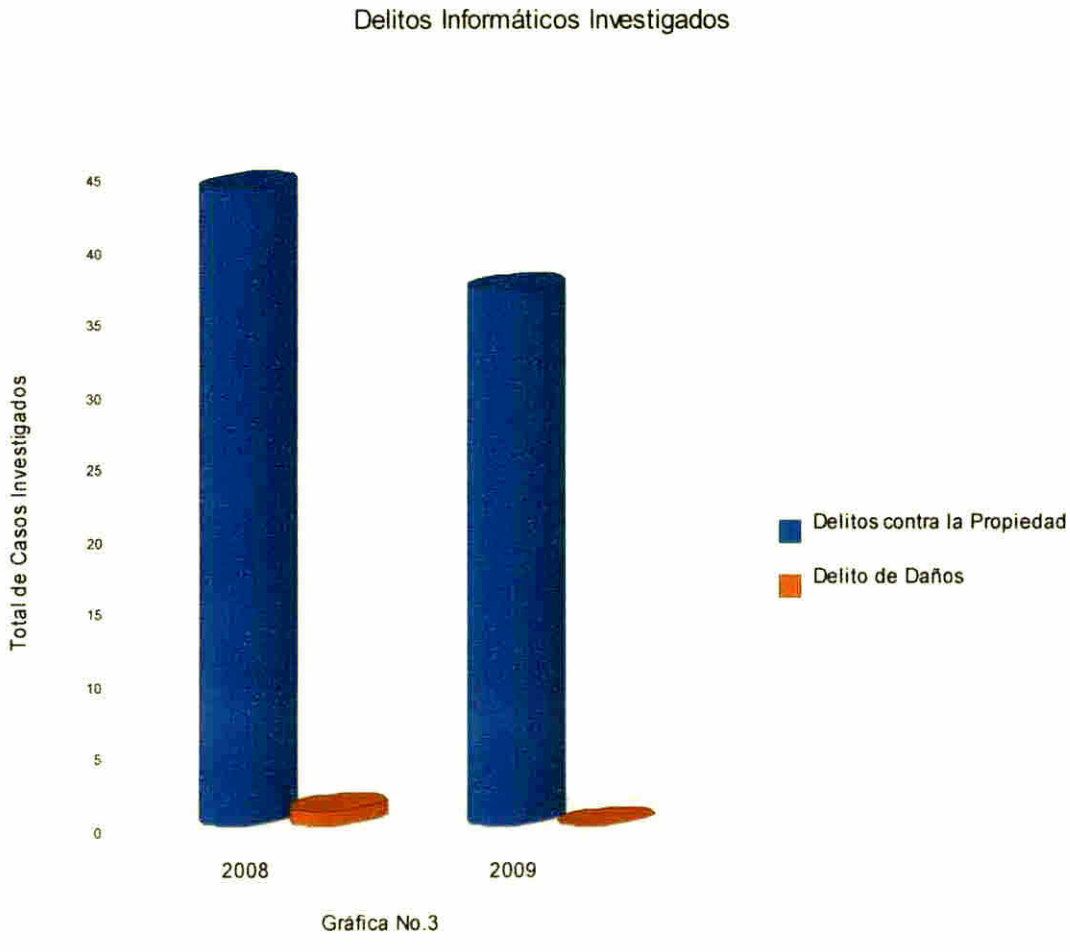


Ilustración 3

CONCLUSIONES

Luego de completada nuestra investigación sobre el delito de daños y su relación con la delincuencia informática en especial con el delito de sabotaje informatico luego del análisis jurídico dogmático del delito de daños y de la doctrina nacional y extranjera sobre este tema concluimos lo siguiente

Se entiende por delito informatico aquel comportamiento antijuridico no ético o no autorizado relacionado con el procesado automatico de datos y/o transmisiones de datos

Se entiende por cibercrimen el conjunto de conductas relativas al acceso apropiacion intercambio y puesta a disposición de informacion en redes telematicas las cuales constituyen su entorno comisivo perpetradas sin el consentimiento o autorización exigibles o utilizando informacion de contenido ilicito pudiendo afectar a bienes juridicos diversos de naturaleza individual o supraindividual

Es importante para el Estado correctamente identificar las diferentes formas de conductas criminales relacionadas con las tecnologias de la información y comunicacion no solo por lo que respecta al derecho sustantivo (Derecho Penal) sino también facilitar la

investigación y el posterior enjuiciamiento de aquellas conductas, lo que resulta ser un problema del procedimiento penal en sí, por lo que fallar en la construcción de la fase procesal, afecte el sentido de la norma penal.

- Se entiende por sabotaje informático aquellos ilícitos que consisten en la destrucción o el daño que se produce al sistema informático, ya sea el hardware o el software.
- En lo que se refiere a la legislación Penal Panameña, hubieron numerosos intentos a fin de introducir la correcta tutela a los delitos informáticos, la cual se logro en parte con el Código Penal de 2007, el cual crea el título de los delitos contra le seguridad informática.
- En Panamá, no existe un verdadero delito de sabotaje informático, más bien dentro del delito de daños encontramos la agravante de causar daños a través de medios informáticos, lo cual supone en principio una figura análoga al delito de sabotaje en si, pero con algunas diferencias marcadas.
- El delito de sabotaje informático mantiene un doble bien jurídico, el patrimonio como también la información, aunque en los últimos tiempos la protección a esa información perjudicada por un sabotaje informático resulta ser más preponderante según la doctrina como

bien jurídico a tutelar en casos de sabotaje informático.

- El Objeto material del delito de daños, será la cosa material o inmaterial, mientras que para el delito de sabotaje informático el objeto material lo serán los datos, documentos, programas de naturaleza electrónica mantenidos en redes, soportes o sistemas informáticos.
- El sujeto activo del delito de daños, es de carácter común, monosubjetivo; por su parte el delito de sabotaje informático no puede ser calificado de delito especial, pues si bien se identifica con un sujeto que tiene ciertos conocimientos, la doctrina lo ha descartado aunque lo usual se trate de sujetos que tienen un conocimiento en el manejo de computadoras.
- En lo relativo al dolo, ambos delitos, el de daños y el sabotaje informático, requieren un dolo directo y el ánimo en el agente de querer dañar la cosa, no son necesarios móviles o fines especiales en el agente, ni siquiera el móvil de perjudicar al propietario de la cosa, que constituye por sí un dolo directo. Igualmente se acepta la posibilidad de encontrar un dolo eventual, más no la posibilidad de culpa ya que está no es aceptada por nuestra legislación.
- La consumación del delito de daños se produce con la objetiva

producción del resultado típico, realizando todos los elementos del tipo, consistentes en la destrucción, deterioro, menoscabo o inutilización de la cosa, mermando o eliminando su valor, este admite la tentativa.

- Del análisis del Derecho Comparado, es necesario mencionar países como Alemania, que de manera autónoma se tiene como delito el borrar, suprimir, inutilizar, o cambiar de manera antijurídica datos, resulta provechoso el definir que será para el código dato, como se hace en Alemania; como también teniendo el sabotaje informático en sí a fin de distinguirlos entre sí.
- El derecho comparado muestra dos maneras de tratar el tema de sabotaje informático, sea utilizando leyes especiales relativas a delitos informáticos, o manteniendo en el mismo Código Penal, desde la perspectiva de la política criminal dependerá del legislador que método utilizar, sea incluir el sabotaje informático, de manera autónoma dentro del título de los delitos contra la propiedad o sino incluirlo dentro de los delitos contra la seguridad informática.
- El análisis de los datos utilizados en la investigación, demuestran que en los últimos años la utilización de medios informáticos para cometer actos criminales va en aumento. Aunque este aumento no

se refleja en denuncias relativas al delito de daños, ya que en la mayoría de los casos los afectados no admiten ser víctimas, ni mucho menos hacen las respectivas denuncias a fin de iniciar investigaciones relativas a la comisión de tal delito.

- Esta cifra negra es preocupante al ser que mientras que en los periódicos y noticieros de televisión del país se mencionan casos de sabotaje informático o por como esta actualmente configurado en nuestro Código el daño causado por el uso de medios informáticos, encontramos que por parte del Órgano Judicial y del Ministerio Público tal realidad no es reflejada al haber ningún caso investigado.
- Que aunque por Resolución No. 19 de 10 de julio de 2008, se creo la fiscalía especializada en delitos contra la propiedad intelectual y seguridad informática, oficina del ministerio público con mando y jurisdicción en toda la república, no se observa entre los datos analizados caso alguno investigado por esta fiscalía.
- Si bien es cierto que nuestro Código Penal actual prevé normas contra la delincuencia informática, es necesario proponer a futuro una reforma a fin de lograr estructurar de mejor manera el delito de daños y el sabotaje informático de manera autónoma, como también

proponer la colocación del delito de sabotaje informático dentro de los delitos contra la seguridad informática.

RECOMENDACIONES

El propósito de esta investigación de acuerdo a nuestra hipótesis era el demostrar que nuestra legislación penal no contenía de manera expresa el delito de sabotaje informático con el fin de demostrar la necesidad de actualizar nuestra legislación para que este actualizada frente este tipo de delincuencia informática.

Así entonces es necesario hacer las siguientes recomendaciones:

1. Modificar el Código Penal de 2007, a fin de que modifique el delito de daños, a fin de que su agravante relacionada con los daños cometidos por medios informáticos, sea convertida en delito autónomo o en caso de que esto no sea posible, insertar esta agravante como delito autónomo en entre los delitos contra la seguridad informática como delito de sabotaje informático.

2. Educar a la sociedad general, como también a los miembros de Ministerio Público y Órgano Judicial, a fin de lograr establecer un ambiente de confianza a fin de que al momento de que una persona sea victima de un delito de sabotaje informático, esta lo denuncie y que se investigue tal delito de una manera acorde a lo que exige según su naturaleza informática. Es necesario evitar que siga como en la actualidad esa

situación de denuncias en los medios que en la realidad jurídica del país no pasan a ser mas nada que un rumor o comentario noticioso

3 Fortalecer la labor de la sección de informatica forense del Instituto de Medicina Legal ya que en un ambiente donde se denuncie este delito seria necesario dotar esta sección de más elementos y personal para estar a la par con el aumento de estos delitos

4 Con la creacion de la fiscalia especializada en delitos contra la propiedad intelectual y la seguridad informatica, se hace un gran avance a fin de lograr castigar la comisión del delito de sabotaje informático pero no se puede permitir ese desuso de personal especializado al ser que en la práctica de esa fiscalia utilizan peritos del ministerio publicos los cuales no conocen el correcto procedimiento al momento de tratar una investigación relacionada a delitos informáticos

5 A manera de aporte planteamos nuestra version de lo que pudiese ser una reforma a fin de estructurar el sabotaje informático dentro de nuestra legislación penal sin entrar en la discusion sobre donde colocar el delito sea dentro de los delitos contra el patrimonio o dentro de los delitos contra la seguridad informática Asi entonces proponemos introducir en el Código Penal la siguiente norma

Articulo Quien borre suprima inutilice o altere datos

programas, documentos electrónicos ajenos, contenidos en redes, soportes o sistemas informáticos será sancionado con pena de dos (2) a años (4) años de prisión o su equivalente en dias-multa o arresto de fines de semana."

BIBLIOGRAFÍA

ABOSO Gustavo Eduardo y ZAPATA Maria Florencia **Cibercriminalidad y Derecho Penal** Editorial B de F Buenos Aires 2006

ACEVEDO José Rigoberto **Derecho Penal General y Especial Panameño Comentarios al Código Penal** Taller Senda Panama 2008

AMUCHATEGUI REQUENA Irma **Derecho Penal** Colección textos Juridicos Universitarios Harlam Mexucim 1993

ANDRES DOMINGUEZ Ana Cristina El delito de daños Consideraciones Juridico politicas y dogmáticas Servicio de Publicaciones Universidad de Burgos Burgos 1999

ARANGO DURLING Virginia **Las Causas de Inculpabilidad** Ediciones Panamá Viejo Panamá 1998

BAJO FERNANDEZ Miguel PEREZ MANZANO Mercedes y SUAREZ GONZALEZ Carlos **Manual de Derecho Penal Parte Especial. Delitos Patrimoniales y Económicos** Editorial Centro de Estudios Ramón Areces S A Madrid 1993

BRAMONT ARIAS Luis Alberto y GARCIA CANTIZANO Maria del Carmen **Manual de Derecho Penal. Parte Especial** 3ª Edición Editorial SM Lima 1994

BUOMPADRE Jorge E **Delitos contra la propiedad** Mario Viera Editor Buenos Aires 1998

BUSTOS RAMIREZ Juan **Obras Completas Tomo I Derecho Penal Parte General** Ara Editores Lima 2004

CACERES RUIZ Luis **Delitos contra el patrimonio aspectos penales y criminológicos** Editorial Vision Net Madrid 2006

CALDERON CEREZO Antonio y CHOCLAN MONTALVO Jose Antonio **Derecho Penal. Tomo II Parte Especial** Editorial BOSCH Barcelona 1999

CAMACHO LOSA Luis **El delito Informático** Gráficas Condor Madrid 1987

CHOCLAN MONTALVO Jose Antonio Fraude informático y estafa por computación **En Internet y Derecho Penal** Cuadernos del Derecho Judicial Consejo General del Poder Judicial Madrid 2001

CORCOY BIDASOLO Mirentxu en MIR PUIG Santiago (Coompilador) **Delincuencia Informática,** PPU Barcelona 1992

CRUZ DE PABLO Jose Antonio Derecho **Penal y Nuevas Tecnologías Difusión Jurídica y Temas de Actualidad** Madrid 2006

- DAMIANOVICH DE CERREDO. Laura. **Delitos contra la propiedad**. Editorial Universidad. Tercera edición. Buenos aires. 2000.
- DAVARA RODRIGUEZ. Miguel Ángel. **Manual de Derecho Informático.** Editorial Aranzadi. Madrid. 2003.
- DONNA. Edgardo Alberto. **Derecho Penal. Parte Especial**. Tomo II-B Rubinzal-Culzoni Editores. Buenos Aires. 2001.
- ESTRADA GARAVILLA, Miguel. **Delitos Informáticos**. http://www.unifr.ch/ddp1/derechopenal/articulos/pdf/DELITOS.pdf
- ESTRADA POSADA, Rodolfo y SOMELLERA, Roberto, **Delitos Informáticos**, en Informática y Derecho 28, Mérida. 1998.
- FEBRES CORDERO, Héctor. **Curso de Derecho Penal**. Tomo I. Caracas 1993.
- FERNANDEZ TERUELO, Javier Gustavo. **Cibercrimen. Los delitos cometidos a través de internet** Constitutio Criminalis Carolina CCC, 2007.
- GALAN MUÑOZ. Alfonso. **El Fraude y la estafa mediante sistemas informáticos. Análisis de artículo 248.2 C. P**. Tirant lo Blanch. Valencia. 2005.
- GONZALEZ RUS, Juan José, "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del Código Penal)": **La Ciencia del Derecho Penal ante el nuevo Siglo. Libro homenaje a José Cerezo Mir**. Tecnos, Madrid, 2002.

GONZALEZ RUS Juan José Daños a traves de internet y denegación de servicios **Homenaje al profesor Dr Gonzalo Rodríguez Mourullo** Thomson Civitas Madrid 2005

GONZALEZ RUS Juan José COBO DEL ROSAL Manuel CARMONA SALGADO Concepción **Curso de Derecho Penal Español. Parte Especial I** Marcial Pons Madrid 1996

GUERRA DE VILLALAZ Aura Están tipificados los delitos informáticos en la Legislación Panameña **Revista Lex No 4 abril-agosto** Panama 1993

GUERRA DE VILLALAZ Aura **Derecho Penal Parte Especial** Editorial Mirzachi & Pujol 1° edicion Panama 2002

GUTIERREZ FRANCES Maria Luz **Fraude Informático y Estafa.** Ministerio de Justicia Secretaria General Técnica Centro de Publicaciones Madrid 1991

JAEN VALLEJO Manuel **Cuestiones actuales del derecho penal económico** Editorial Adhoc Buenos Aires 2004

JIMENEZ VILLAREJO Francisco La delincuencia económica y las nuevas tecnológicas el fraude informático **Revista de Derecho Penal No 27 Mayo 2009** Editorial Lex Nova Valladolid 2009

LAMARCA PEREZ Carmen ALONSO DE ESCAMILLA Avelina MESTRE DELGADO Esteban y GORDILLO ALVAREZ VALDEZ Ignacio **Manual de derecho Penal. Parte Especial** Colex Madrid 2001

LUZ CLARA Bibiana **Manual de Derecho Informático** Editorial Jurídica Nova Tesis Rosario 2001

MATA Y MARTIN, **Ricardo Delincuencia Informática y Derecho Penal.** Editorial Hispamer Nicaragua 2003

MIR PUIG Santiago **Delincuencia Informática** PPU Barcelona 1992

MARCHENA GOMEZ Manuel El sabotaje informatico entre los delitos de daños y desordenes publicos **En internet y derecho Penal** Cuadernos de Derecho Penal X 2001 Consejo General del Poder Judicial Madrid 2001

MARTINEZ PEREDA RODRIGUEZ José Manuel y ROMA VALDEZ Antonio **Derecho Penal (Parte Penal)** J M Bosch Editor Barcelona 1999

MORALES GARCIA Oscar **Derecho Penal y sociedad de la Información Derecho y nuevas tecnologías** Editorial UOC Barcelona 2005

MORANT VIDAL Jesus **Protección Penal de la Intimidad frente a las nuevas tecnologías** Editorial Practica del Derecho Valencia 2003

MORON LERMA Esther **Internet, y Derecho Penal Hacking y otras conductas ilícitas en la Red** Aranzadi 2° Edicion Navarra 2002

MUÑOZ RUBIO Campo Elias y GUERRA DE VILLALAZ Aura **Derecho Penal Panameño** Ediciones Panamá Viejo Panamá 1980

PABON PARRA Pedro Alfonso **Delitos contra el patrimonio económico** Ediciones Doctrina y Ley Bogota 2002

- PALAZZI, Pablo. **Delitos Informáticos**. Editorial Ad Hoc. Buenos Aires. 2000.
- QUERALT JIMENEZ, Joan Josep. **Derecho Penal Español. Parte Especial.** 3ª Edición J.M. Bosch Editor. Barcelona. 1996.
- RIGHI, Esteban y FERNANDEZ, Alberto. **Derecho Penal. La Ley. El delito. El proceso y la Pena**. Editorial Hamurabi. Buenos Aires. 1996.
- ROMEO CASABONA, Carlos María. **De los delitos informáticos al cibercrimen. Una aproximación conceptual y político criminal. En El cibercrimen nuevos retos jurídicos-penales, nuevas respuestas político-criminales**. Estudios de Derecho Penal y Criminología, Editorial Comares, Granada. 2006.
- ROMERO SOTO, Luis Enrique. **El delito de Estafa**. Carvajal S.A. Bogota. 1990.
- ROXIN, Claus. **Derecho Penal Parte General, Tomo I. Fundamentos. La Estructura de la Teoría del Delito.** 2° Edición. Thomson Civitas. Madrid. 2003.
- SALT, Marcos "Delitos Informáticos": **Justicia Penal y Sociedad**, Revista Guatemalteca de Ciencias Penales. Año 4. No. 6 Abril 1997. Managua 1997.
- SÁEZ CAPEL, José. **Informática y Delito**. 2ª edición. Buenos Aires 2001.
- SANTA CECILIA GARCIA, Fernando. **Delito de Daños. Evolución y Dogmática (art. 263 Código Penal)**. Universidad Complutense Facultad de Derecho. Servicio de Publicaciones. Madrid. 2003.

SERRANO GOMEZ Alfonso **Derecho Penal Parte Especial** 8ª Edición Dykinson Madrid 2003

SOLER Sebastián **Derecho Penal Argentino IV** Tipografica Editora Argentina Buenos Aires 1970

SUAREZ MIRA Carlos **Manual de Derecho Penal II Parte Especial** Thomson Civitas Madrid 2003

SUAREZ SANCHEZ Alberto **Delitos contra el patrimonio económico** Universidad del externado de Colombia Bogota 2000

TIEDEMANN Klaus **Lecciones de Derecho Penal Económico** PPU promociones y publicaciones universitarias S A 1 edicion Barcelona 1993

VILLALOBOS Edgardo **Diccionario de Derecho informático** Litho Editorial Chen Panama 2002

VIVES ANTON Tomás **Comentarios al Código Penal de 1995 Volumen II** Tirant lo Blanch Valencia 1996

WALDEN Ian **Computer Crimes and Digital Investigations** Oxford University Press Inglaterra 2007

WASHINGTON RODRIGUEZ Agustin y GALLETA DE RODRIGUEZ Beatriz **Delitos contra la propiedad** Editorial Juris Buenos Aires 2001

ZUGALDIA ESPINAR José Miguel **Delitos contra la propiedad y el patrimonio** Ediciones Akal Madrid 1988