UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL

JUAN DANIEL OXLAJ NOJ

GUATEMALA, JUNIO DE 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

JUAN DANIEL OXLAJ NOJ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICA Y SOCIALES

Y los títulos profesionales de

ABOGADO Y NOTARIO

Gutemala, junio de 2021

HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	Licda. Astrid Jeannette Lemus Rodríguez
	VOCAL I, en sustitución del Decano
VOCAL II:	Lic. Henry Manuel Arriaga Contreras
VOCAL III:	Lic. Juan José Bolaños Mejía
VOCAL IV:	Br. Denis Ernesto Velásquez González
VOCAL V:	Br. Abidán Carías Palencia
SECRETARIA	Licda. Evelyn Johanna Chevez Juárez

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Lic. Fredy Hernan Arrivillaga Morales
Vocal:	Lic. Milton Estuardo Riveiro Gonzalez
Secretario:	Licda. Paula Estefani Osoy Chamo

Segunda Fase:

Presidente:	Lic. Hector Manfredo Maldonado Méndez
Vocal:	Lic. Edwin Xitumul
Secretario:	Licda. Ileana Villatoro Fernández

RAZÓN: Únicamente el autor es responsable de las doctrinas sustentadas en la tesis". (Artículo 43 de Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público)

Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.

Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala. Ciudad de Guatemala, cinco de mayo de dos mil veintiuno.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante JUAN DANIEL OXLAJ NOJ, titulado REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

RFOM/JP.

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C. A.

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANATO
GUATEMALA, C. A.

Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.

Guatemala 19 de febrero del 2021

Jefatura de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
16 MAR. 2021
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Le informo que corregí en forma virtual la tesis del alumno **JUAN DANIEL OXLAJ NOJ** con número de carné **201212311** que se denomina: **"REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL".**

La tesis efectivamente cumple con lo requerido en el instructivo respectivo de la Unidad de Asesoría de Tesis de la Facultad de Ciencias Jurídicas y Sociales, habiendo sido las modificaciones señaladas llevadas a cabo, razón por la cual es procedente la emisión de **DICTAMEN FAVORABLE.**

Atentamente.

"ID Y ENSEÑAD A TODOS"

Dr. Carlos Herrera Recinos
Docente Consejero de Estilo

LICENCIADO ANGEL ERNESTO REYES BAUTISTA
ABOGADO Y NOTARIO
31 Calle 20-50 colonia santa Elisa zona 12, Guatemala, Guatemala
5020-5328

Guatemala, 06 de Julio de 2020

Licenciado

Roberto Fredy Orellana Martínez

Jefe de Unidad de Asesoría de Tesis

Facultada de Ciencias Jurídicas y Sociales

Universidad de san Carlos de Guatemala

Su despacho

Licenciado Orellana:

De manera muy atenta me dirijo a usted para hacer de su conocimiento que procedí asesorar la tesis del bachiller JUAN DANIEL OXLAJ NOJ, según nombramiento de fecha 25 de junio de 2020, la cual se titula: REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL.

Posteriormente de las atribuciones asignadas a mi persona le informo lo siguiente:

a. Del contenido científico y técnico de la tesis es importante mencionar que la investigación realizada no se limita a cumplir únicamente con los presupuestos de presentación y desarrollo, sino también a la sustentación de teorías, análisis y aportes, tanto de orden jurídico como académico, por lo que su contenido científico y técnico es satisfactorio, logrando comprobar el supuesto en el que baso su investigación.

b. En cuanto al enfoque metodológico al momento de realizar la revisión, se evidencia que existe una secuencia ideal para un bien entendimiento de la misma, así como la utilización de la metodología concerniente a los métodos: deductivo, analógico, analítico y sintético.

c. La redacción en el desarrollo del trabajo demuestra conocimiento y dominio en la aplicación de las normas de ortografía y redacción, es evidente también que la emisión de sus propios comentarios, los cuales indudablemente dejan de manifiesto el interés de comprobar los supuestos de la investigación

ANGEL ERNESTO REYES BAUTISTA
ABOGADO Y NOTARIO
31 Calle 20-50 colonia santa Elisa zona 12, Guatemala, Guatemala
5020-5328

d. Conclusión discursiva en cuanto a las investigaciones que a lo largo del trabajo realizo el bachiller llego a conclusiones que considero que tienen fundamento y van acordes al tema abordado, por lo que considero que si es factible que se regule en nuestra legislación lo relacionado a los delitos informáticos como se define en los términos expuestos en este trabajo.

e. La contribución científica considero que la presente tesis, provee una serie de elementos relacionados con la temática de cómo debe aplicarse y respetarse las normas contempladas en la Constitución Política de la República de Guatemala, por lo que estimo que el tema es de relevancia dentro del ámbito jurídico penal pues es un aporte científico que busca que el derecho penal sea aplicado de acuerdo a la realidad humana que se vive en Guatemala, siempre respetando el debido proceso, los controles de la administración pública y sobre todo las normas constitucionales aplicables al derecho penal.

f. Considero que la bibliografía utilizada en la elaboración del presente trabajo es actualizada y específica, lo cual preveo a la investigación un carácter formal.

g. Declaro expresamente no ser pariente del bachiller JUAN DANIEL OXLAJ NOJ dentro de los grados legales de parentesco.

Por lo anterior, y habiendo cumplido con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Publico procedo a emitir DICTAMEN FAVORABLE al estudiante JUAN DANIEL OXLAJ NOJ, para que prosiga con los trámites necesarios para su graduación.

Con todo mi respeto, me suscribo de usted.

LICENCIADO ANGEL ERNESTO REYES BAUTISTA
ABOGADO Y NOTARIO
COLEGIADO NO. 16874

LICENCIADO
Angel Ernesto Reyes Bautista
ABOGADO Y NOTARIO

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Facultad de Ciencias Jurídicas y Sociales. Unidad de Asesoría de Tesis. Ciudad de Guatemala, 31 de agosto de 2020.

Atentamente pase al (a) Profesional, **ANGEL ERNESTO REYES BAUTISTA**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **JUAN DANIEL OXLAJ NOJ**, con carné **201212311**, intitulado **REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL**.

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
UNIDAD DE ASESORÍA DE TESIS
GUATEMALA, C. A.

LIC. GUSTAVO BONILLA
Jefe(a) de la Unidad de Asesoría de Tesis

Fecha de recepción 21 / 09 / 2020

Asesor(a)
(Firma y Sello)

LICENCIADO
Angel Ernesto Reyes Bautista
ABOGADO Y NOTARIO

DEDICATORIA

A DIOS: Por ser mi guía y fortaleza en este camino para llegar a culminar esta etapa de mi vida y conseguir este logro.

A MI PADRE: Juan Oxlaj Chaj por apoyarme siempre en cada etapa de mi vida en especial en este camino para culminar esta etapa.

A MI MADRE: Teodora Noj por dar todo por mí sin importar nada y guiarme siempre por el camino correcto y nunca desampararme.

A MI ESPOSA E HIJO: Por llegar a mi vida y ser siempre un motivo para culminar esta etapa de mi vida y gozar siempre de su amor y apoyo

A MIS HERMANAS: Por brindarme su apoyo incondicionalmente y ser siempre un parte importante en mi vida.

A MI FAMILIA: A mis abuelos, tíos y tías que siempre han sido importantes en mi vida desde pequeños, gracias por todo su cariño y apoyo.

A MIS COMPADRES: Alejandro Cruz y Yoselin Flores, por su amistad, por cada uno de sus consejos y por haber aceptado ser parte de mi familia.

A MIS AMIGOS: A cada uno de mis amigos con los cuales hemos vivido momentos alegres y momentos difíciles, y a pesar de esto continúa nuestra amistad. Gracias por su apoyo y por su amistad.

A: Mi *Alma Mater* la tricentenaria Universidad de San Carlos de Guatemala por haberme permitido ser un estudiante San Carlista.

A: La Facultad de Ciencias Jurídicas y Sociales por forjar la enseñanza superior universitaria para poder ser una profesional del derecho al servicio de la población de esta hermosa patria que es Guatemala.

PRESENTACIÓN

El trabajo de tesis contiene un análisis que tiene relación a la reproducción no autorizada de los programas informáticos, así como la obligación del Estado para prevenir y erradicar dicha problemática; dicha problemática se ha incrementado en los últimos tiempos conforme ha evolucionado la tecnología debido a que no se han considerado las debidas providencias en la normativa de Guatemala.

La problemática que se plantea se enfoca en la falta de providencias por parte de la normativa en el Estado de Guatemala para prevenir la reproducción no autorizada de programas informáticos; ya que el Estado no cumple con su obligación de prevenir dichos delitos.

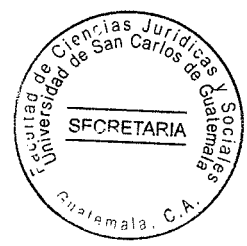
La investigación pertenece a la rama del derecho penal y es de tipo cualitativo ya que se realizó un estudio de las clases y las causas por las cuales se lleva a cabo la reproducción no autorizada de programas informáticas y del impacto que produce tanto económica como jurídica dentro del Estado de Guatemala; se propone que se apruebe la iniciativa de Ley 4055 Ley de Delitos Informáticos del Congreso de la Republica con el fin de que el Estado de Guatemala cumpla con su función de prevenir y erradicar dichos actos.

HIPÓTESIS

En la actualidad el Código Penal no cuenta con regulación con relación al problema de la reproducción no autorizada de programas informáticos de protección legal esto debido a la existencia de un vacío legal, ya que las normas que regulan este tipo de delitos no se encuentran actualizadas, el Estado de Guatemala al no implementar normativa para prevenir y erradicar la reproducción no autorizada de programas informáticos de protección legal no cumple con su función de proteger los derechos que de autor o inventor, ya que debe existir un control sobre estos tipos de delitos los cuales vulneran los derechos de los autores.

COMPROBACIÓN DE HIPÓTESIS

Se comprobó la hipótesis en la investigación utilizado los siguientes métodos: analítico, sintético, deductivo, inductivo, y analógico. Por lo que es evidente la validación de la hipótesis formulada, al quedar confirmado que en el Artículo 274 "C" del Código Penal Decreto 17-73 del Congreso de la República de Guatemala en relación a la reproducción de programas informáticos, la problemática es evidente tanto en la regulación como en la aplicación de la norma penal antes mencionada, generando así, incongruencia al exigir determinado tipo de delito y dando como resultado una serie de inobservancias que permiten la violación de derechos de autor que afectan directamente a los legítimos autores como al Estado de Guatemala.



ÍNDICE

Pág.

CAPÍTULO II

Pág.

CAPÍTULO III

CAPÍTULO IV

Pág.

INTRODUCCIÓN

Debido a la problemática que existe en el país con la excesiva reproducción y comercialización de programas informáticos que se encuentran bajo la protección legal, esto es debido a que en actualidad la regulación sobre estos delitos es escasamente y así mismo la problemática de la poca o nula aplicación de estas regulaciones, ya que este hecho afecta negativamente la imagen de nuestro país, dado que reduce la inversión Internacional en Guatemala. El adquirir programas informáticos piratas genera una violación al derecho de autor, la mayoría de personas no son conscientes del grave daño que la piratería causa. De esta forma se decidió investigar, analizar y describir el delito de la Reproducción no autorizada de programas informáticos de protección legal, debido a que en la normativa actualmente existe un vacío legal y no concede las providencias necesarias para este tipo de delito puede entrañar una pérdida económica sustancial para los propietarios legítimos.

Entre los métodos utilizados en la investigación se encuentran en primer lugar el método analítico, el cual se aplicó como clasificador dado que se separó los delitos informáticos en tipos, porque era necesario determinar en qué tipo de delito informático se encontraba la reproducción no autorizado de programas informáticos de protección legal; el método sintético, se aplicó este método al identificar cada uno de los tipos de delitos informáticos que existen, por medio de este método se identificó que la reproducción no autorizada de programas de protección legal se encuentran dentro de los delitos informáticos; el método deductivo, se aplicó para deducir que los delitos informáticos es la utilización tanto de equipos de cómputo como programas informáticos por lo que se estableció que la reproducción no autorizadas de programas informáticos de protección legal es un delito informático; el método analógico al utilizarlo en la comparación de la problemática de la reproducción ilegal de los programas informáticos, así como la comercialización de estos en el país, así como afrontan esta problemática en distintos países.

En el capítulo I hace referencia a lo delitos informáticos, desde su origen así como los sujetos en la comisión de los delitos informáticos y los bienes jurídicos tutelares que se vulneran; el capítulo II desarrolla la clasificación de los delitos informáticos según la legislación extranjera; en el capítulo III, se refiere a la regulación legal de los delitos informáticos en Guatemala; en el capítulo IV se desarrolla la reproducción no autorizada de programas informáticas de protección legal así como las consecuencias de la reproducción no autorizada de programas informáticos de protección legal.

Debido a la carencia de normas para regular la reproducción no autorizada de programas informáticos de protección legal, ya que únicamente se encuentra regulado ciertos aspectos de este delito en el Código Penal Decreto Número 17-73 del Congreso de la República de Guatemala en el Artículo 274 "C", es necesario que se emita una norma donde se regule lo relativo a este delito y los distintos delitos informáticos, los cuales por la magnitud que ha tenido en el país la informática estos suelen ser más comunes y peligrosos.

CAPÍTULO I

1. Los delitos informáticos

El delito informático es la acción, típica, antijurídica y dolosa cometida mediante el uso normal de la informática, o sea, un elemento informático o telemático, contra el soporte lógico o *software*, de un sistema de tratamiento autorizado de la información. Es una acción socialmente peligrosa, prohibida por ley bajo la conminación de una sanción penal.

Santiago Acurio Del Pino sostiene que la informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información, para ejecutar tareas que en otros tiempos realizaban manualmente. conforme se observa en la actualidad esto concuerda con lo manifestado con el doctor Del Pino, ya que para utilizar cualquier medio y programa informático estos solicitan casi de manera obligatoria que se ingresen datos o cuentas personales para iniciar la sesión, dentro de los cuales se pueden mencionar nombres, fechas de nacimientos, cuentas de correos electrónicos, etc.

El mundo en la actualidad cambia rápidamente. Antes se tenía la certeza de que nadie podía acceder a información sobre la vida privada de las personas. La información era solo una forma de llevar registros. Ese tiempo ha pasado, y con él, lo que se puede llamar intimidad.

La información sobre la vida personal se está volviendo un bien muy cotizado por las compañías del mercado actual. La explosión de las industrias computacionales y de comunicaciones ha permitido la creación de un sistema, que puede guardar grandes cantidades de información de una persona y transmitirla en muy poco tiempo. Cada vez más y más personas tienen acceso a esta información, sin que las legislaciones sean capaces de regularlos.

Debido a lo que se ha desarrollado en el pasado y conforme a lo que se observa en la actualidad, es necesario que en la legislación actual se tome en consideración estos aspectos y se haga énfasis en estos temas para que en su momento se tomen las medidas necesarias y se actualice la regulación de los delitos informáticos que evolucionan continuamente y que afectan a las personas por medio de los ataques informáticos y la reproducción no autorizada de programas informáticos de protección legal.

"En la actualidad, las redes de comunicación electrónica y los sistemas de información forman parte de la vida diaria de los ciudadanos en el mundo y desempeñan un papel fundamental en el éxito de la economía universal. Cada vez están más interconectadas y es mayor la convergencia de los sistemas de información y las redes. Esta tendencia

implica, sin duda, numerosas y evidentes ventajas, pero va acompañada también de un riesgo inquietante de ataques malintencionados contra los sistemas de información."[1]

La informática hoy en día, es un elemento esencial dentro de la vida de cada persona, ya que en la actualidad es una herramienta que se utiliza tanto en el trabajo como en diferentes tareas que se realiza a diario, dado que esta concede facilidad para comunicarse sin necesidad de viajar, por lo que ahorra tiempo, sin embargo, esto a lo largo del tiempo ha llegado a causar problemas, porque se han utilizado estas herramientas para cometer actos ilícitos, esto ha derivado a que se tome con más seriedad el tema de los delitos informáticos, ya que las personas están expuestas a que se le vulnere algún bien jurídico tutelado.

1.1. Antecedentes

En la actualidad el uso de las computadoras y programas informáticos es indispensable, lo que vuelve a las personas posibles víctimas de delitos informáticos. Los delitos informáticos aparecen junto a las tecnologías de la información, con el desarrollo de la tecnología, la sociedad se ha visto en un panorama de avance y desarrollo en todas sus áreas; por desgracia, la delincuencia también se ha beneficiado de esto.

[1] Téllez Valdés, Julio. **Derecho informático**. Pág. 187

"Uno de los primeros y más importantes ataques en la historia de Internet se remonta a CREEPER en 1971, escrito por el ingeniero Bob Thomas, es considerado el primer virus informático que afecto a una computadora el cual mostraba un mensaje en los equipos infectados, el cual, si no causaba daño alguno, fue la base para el desarrollo de ataques posteriores con pérdidas multimillonarias, como se menciona en la página de internet de la INTERPOL se estima que en 2007 y 2008 la ciberdelincuencia tuvo un coste a escala mundial de unos 8.000 millones de USD".[2]

"En 1978, habiendo ya saltado a la prensa algunos de los primeros casos de delincuencia informática patrimonial, BEQUAI realizó un análisis de estos delitos considerando que en la definición del delito informático el acento debe ponerse en que los ordenadores pueden ser usados por el autor del delito no sólo como instrumentos para cometer el mismo sino también como objeto del delito. Este autor incluyó entre los *computer crimes* los delitos de sabotaje informático, robo de información digitalizada y programas, espionaje industrial, hurto de tiempo de uso del ordenador, robos de mercancías por manipulación de datos o fraudes financieros."[3]

"Se suele considerar que el primer *bug* o fallo informático tuvo lugar en el laboratorio de cálculo Howard Aiken de la universidad de Harvard. Hasta finales de 1988 muy poca gente se tomaba en serio el tema de la seguridad en redes de ordenadores. Sin embargo,

---

[2] http://eprints.uanl.mx/3536/1/**Delitos_informaticos**.pdf (consultado: 15 de enero de 2015)
[3] https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf. **El Delito Informático**. (consultado: 14 de noviembre de 2020)

el 22 de noviembre de 1988 Robert Morris protagonizo el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso *worm* o gusano de internet, miles de ordenadores conectados a la red se vieron inutilizados durante días y las pérdidas se estimaron en millones de dólares. Desde ese momento el tema de la seguridad en las redes de ordenadores ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos".[4]

Posteriormente a los incidentes y debido a que existían potenciales peligros de ataques contra los sistemas informáticos de los Estados Unidos, la Agencia Avanzada de Defensa, DARPA, por sus siglas en inglés, desarrolló el Equipo de Respuestas a Emergencias Informáticas, el cual era constituía por un grupo de personas expertas en informática y cuyo objeto principal era contrarrestar y tener una respuesta inmediata a los posibles problemas que afectaran la seguridad de las redes y ordenadores que se encontraban conectadas a internet.

El primer virus se desarrolló sin intención de causar daño alguno al patrimonio de las personas, únicamente se utilizó para realizar bromas, sin embargo, este fue tomado como una guía para realizar actos ilícitos y así causar daños. En este incidente se creó por accidente un *worm* o también llamado gusano y causó daños que fueron accidentales ya que la intención no fue paralizar los ordenadores, sin embargo, debido a este incidente se tuvo que realizar un respaldo de emergencia ya que se tuvo una preocupación mayor

[4] Gómez Vietes, Alvaro. **Auditoría de seguridad informática**. Pág.15

por la seguridad informática ya que esto podría afectar directamente los intereses de la economía de un Estado.

1.2. Origen y evolución

"El origen exacto del delito cibernético, el primer caso en el que alguien cometió un delito a través de una red de ordenadores, es imposible saberlo. Lo que es posible saber es el primer gran ataque a una red digital y luego usar eso como punto de referencia en la evolución de los delitos cibernéticos". [5]

Uno de los primeros acontecimientos relacionados con los delitos informáticos surgió en 1973 cuando un cajero de un banco local de Nueva York usó una computadora para desviar más de $2 millones de dólares. Posteriormente en 1982 un virus, fue escrito como broma por un niño de 15 años. Es uno de los primeros virus conocidos en dejar su sistema operativo original y propagarse. Cuatro años después en 1986 El Congreso aprueba la Ley de Fraude y Abuso Informático, convirtiendo el *hackeo* y el robo en algo ilegal.

En 1990 *The Legion Of Doom y Masters Of Deception*, dos bandas cibernéticas, se involucran en una guerra en línea. Bloquean activamente las conexiones del otro, *hackean* las computadoras y roban datos. Estos dos grupos eran manipuladores telefónicos a gran escala, famosos por numerosos *hackeos* en la infraestructura

[5]https://www.le-vpn.com/es/**delito-cibernetico-origen-evolucion/** (consultado: 27 de abril de 2017)

telefónica central. La proliferación de los dos grupos, junto con otras pandillas cibernéticas, llevó a una agresión del FBI contra la BBS promocionando el robo de tarjetas de crédito y el fraude del cable.

En 1994 se lanza la *World Wide Web*, la cual permitió a los *hackers* obtener y mover información a sus propios sitios, debido a esto un estudiante en el Reino Unido utilizó información para *hackear* programas nucleares de Corea y otras agencias de Estados Unidos usando solamente un ordenador personal. Un año más tarde aparecen los macro-virus. Los macro-virus son virus escritos en lenguajes informáticos integrados en aplicaciones. Estos macros se ejecutan cuando se abre la aplicación, como documentos de procesamiento de textos u hojas de cálculo y son una forma fácil para que los *hackers* puedan enviar el *malware*.

Según la página de Internet Le VPN "En 1997 el *FBI* informa que más del 85% de las empresas estadounidenses habían sido *hackeadas,* y la mayoría ni siquiera lo sabía. El *Chaos Computer Club hackea* el *software Quicken* y puede hacer transferencias financieras sin que el banco o el titular de la cuenta lo sepan".[6] En 1999 fue lanzado el virus denominado Melissa el cual se convertiría en el virus informático más agresivo hasta esa fecha, el cual consistía en un Macro-Virus cuyo objetivo era apoderarse de cuentas de correos electrónicos y de igual forma mandar correos masivamente. En consecuencia,

[6] **Ibíd.**

a este ataque el creador de dicho virus fue acusado de causar daños en redes informáticas valoradas en 80 millones de dólares y fue condenado a cinco años de prisión.

En 2003 se crea un gusano el cual fue llamado *SQL Slammer* el cual se convertiría en el virus de más rápido propagación, el cual infectó diversos servidores *SQL* y creó una denegación de servicios, el cual se extendió e infectó casi 75,000 ordenadores en menos de 10 minutos. Posterior a ese ataque cuatro años después los casos de *hackeo*, robo de datos e infecciones por medio de virus toma más importancia a tal grado que el gobierno de China fue acusado de *hackear* al gobierno de los Estados Unidos, así como a otros sistemas gubernamentales. Con base a estos antecedentes, se originaron varias acciones para evitar y contrarrestar este tipo de ataques en las cuales fueran vulnerados los sistemas y la seguridad informática.

Con el pasar de los años ha ido evolucionando la forma de cometer delitos informáticos a tal punto de que se han utilizado todo tipo de medios informáticos para la comisión de los delitos. Se han realizado ataques a servidores que han provocado muchas pérdidas tanto económicas como de datos e información.

Uno de los ataques más famosos fue el que se realizó en contra de la empresa Sony, a través del cual hicieron colapsar las plataformas *online* del gigante japonés. El origen del ataque obedeció a que en abril del 2011 Sony inició acciones judiciales en contra de los usuarios Geohot y Graf-Chokolo por realizar filtración de datos. El grupo de *hackers* realizó ataques **DDos** contra los sitios web de la compañía y de la firma de abogados que

los representaba. Tiempo después Sony responsabilizó a **Anonymous** de haber sustraídos datos personales y bancarios de más de 100 millones de jugadores *online*, pero estos negaron dichas acusaciones.

En este caso se acusó a un grupo de *hackers* de haber sustraído información y haber realizada un daño económico a la empresa y a los usuarios de esta. En este sentido se puede afirmar que los ataques cibernéticos tomaron un nivel mayor, en la cual ya no se realizó en un sentido social, o para dañar el sistema como amenaza de las empresas, si no, llegó al nivel de cometer un delito y un daño en el patrimonio de las personas.

Un año después en el año 2012, se realizó un ataque a los sitios informáticos de la iglesia católica mexicana el cual consistió en el bloqueo de las páginas relacionadas con el Instituto de Comunicación y Filosofía, esto derivado de la visita del Papa Benedicto XVI a México, ya que los *hackers* encargados de realizar este ataque consideraban que la visita del pontífice favorecía al gobierno que se encontraba en el poder, además protestaban por el costo elevado de las entradas para asistir al evento.

1.3. Sujetos del delito informático

En los delitos informáticos existe un sujeto activo y otro pasivo, pero en el caso del primero no se pueden considerar delincuentes comunes a pesar de que se refiere tanto a las personas naturales como a las personas jurídicas. El hecho de que no sea considerado el sujeto activo como un delincuente común está determinado por el

mecanismo y medio de acción que utilice para llegar a producir el daño. El reconocimiento de varios tipos de conductas antijurídicas que puede manifestar el sujeto activo, es preciso para conocer las posibles formas de comisión delictiva y profundizar en las posibles formas de prevención y detención de estas conductas. De tal manera que es importante precisar quiénes pueden ser los sujetos del delito informático.

1.3.1. Sujeto activo

"Se trata del llamado **delincuente informático**, que es aquella persona que realiza la conducta descrita en el tipo penal. Principalmente hay que buscarlo en medio de los **cuellos blancos**, porque en realidad se trata casi siempre de un **delito de cuello blanco** que requiere condiciones técnicas o profesionales muy avanzadas, aquellas que permitan manejar una herramienta muy sofisticada con el computador". [7]

En los sujetos activos se pueden encontrar a los operadores, estos pueden modificar, agregar, eliminar, sustituir información o programas y copiar archivos para venderlos a competidores. De igual forma se encuentran los programadores, quienes pueden violar o inutilizar controles protectores del programa o sistema, con el objeto de dar información a terceros. Otro de los sujetos activos puede ser el analista de comunicaciones, este puede enseñar a otras personas la forma de violar la seguridad del sistema de comunicación de una empresa, con fines de fraude. El personal técnico y de servicios se

[7] Solano Bárcenas, Orlando. **Manual de informática jurídica**. Pág. 293.

puede agregar a este listado ya que posee la libertad de acceso al centro de cómputo y de esta forma puede dañar el sistema operativo .

1.3.2. Sujeto pasivo

"Son las víctimas de los actos dañosos de los delincuentes informáticos: las personas, los bancos, los aseguradores, el Estado, las universidades, los colegios, etc. Los bienes jurídicos tutelados afectados pueden ser varios, entre los cuales se pueden mencionar: El honor de las personas, la intimidad de las personas, la propiedad, la fe pública".[8]

Como en todo delito siempre existe un sujeto pasivo, el cual sufre los daños, ya sea en su integridad, en su moral, en su patrimonio físico o al ser dañado en cuanto en la violación de su intimidad. En los delitos informáticos la mayoría de daños se realizan en la violación de intimidad del sujeto pasivo y de igual forma daño a la propiedad del sujeto pasivo causándole pérdidas económicas.

1.4. Bienes jurídicos tutelados vulnerados por los delitos informáticos

En la actualidad debido al uso de la informática dentro de cada una de las actividades que se realiza por parte de las personas en su diario vivir, se vuelve vulnerable a que pueda ser víctima a que se le vulnere un bien jurídico tutelado.

---

[8] **Ibíd.** Pág. 294.

"Dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente."[9]

Jesús Molina Salgado, citado en la obra de José Alvarado y Ronald Morales, los clasifica los delitos informáticos como instrumento o medio y como fin u objeto. En la primera categoría se encuentran las conductas criminógenas que se valen de la computadora como método, medio o símbolo en la comisión de ilícitos. Por otro lado, en la segunda categoría se encuadran las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

En relación a la clasificación a los bienes jurídicos tutelados que se vulneran José Alvarado y Ronald Morales sugieren en su obra *Cibercrimen* que los delitos informáticos deben clasificarse atendiendo al bien jurídico que específicamente se trata de tutelar como: La integridad, la disponibilidad, la confidencialidad, la dignidad de las personas y la propiedad intelectual.

[9] https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf. **Delitos Informáticos: Generalidades**. (Consultado: 15 de noviembre de 2020)

1.4.1. Delitos contra la integridad

En esta categoría se pueden encuadrar el daño informático, la falsificación informática y el fraude informático.

- **Daño informático**

"Cuando se habla de daño informático se está haciendo referencia a la alteración negativa de la integridad, disponibilidad y confidencialidad de cualquier activo digital ya sea redes, sistemas computacionales, computadoras, programas de computadoras, datas computacionales, el contenido de los datos y el tráfico de los datos. Un acto dirigido a la infraestructura critica informática, se puede considerar el acto más paradigmático de un daño informático, puesto que, lo que se busca es la inutilización, por cualquier medio, de los activos informáticos." [10]

En el daño informático los principales motivos que se tienen para cometer dicho delito es el de inutilizar un sistema informático, suprimir información o datos informáticos importantes con el fin de dañar el funcionamiento de un sistema informático.

[10] Alvarado Lemus, José. **Ciber crimen**. Pág. 48

- **Falsificación informática**

"En materia informática el objeto lo constituyen los datos informáticos. Los datos son hechos que describen sucesos, son representaciones simbólicas, los datos pueden ser comunicados por varios tipos de símbolos, tales como letras, números, gestos, etcétera. Técnicamente, a los datos procesados se le denomina información, de manera que los datos deben ser procesados para constituir información. Cuando se refiere a la información electrónica, los datos se refiere a: archivos, bases de datos, documentos de texto, imágenes, voz y video, codificados en forma digital y que están contenidos en un sistema informático o en uno de sus componentes". [11]

El bien jurídico tutelado en la falsificación informática es la información y, específicamente, la integridad de la información, la cual no debe alterarse o modificarse. En lo que se refiere al delito de la falsificación informática, estamos ante un tipo de delito informático que su fin primordial es la de alterar o modificar información de una base de datos en específico con el fin de utilizarlos para cometer dicho ilícito, y así dañar a las personas en su patrimonio, así mismo este tipo de delitos se puede utilizar para falsificar o alterar documentos por medio de computadoras, los cuales violentan la integridad del documento.

[11] **Ibíd.** Pág. 94.

- **Fraude informático**

El delito de fraude informático está dirigido a vulnerar o atacar el patrimonio de una persona, esto con el uso de datos que se encuentran en la red o que se encuentran almacenados en un sistema informático, ya que se utilizan ciertas maniobras o engaños para que la persona proporcione información confidencial y con ello puedan atacar el patrimonio de una manera informática en la cual se obtiene acceso a cuentas bancarias de las víctimas y así poder apropiarse de sumas de sumas dinerarias.

1.4.2. Delitos contra la disponibilidad

Dentro de esta categoría se encuentra el delito de violación a la disponibilidad el cual consiste en ingresar a un sistema informático, sin autorización, y con ello obstaculizar el uso del mismo. En materia de derecho informático, el bien sobre el cual se tiene el derecho de uso o posesión, lo constituye la información que se encuentra contenida en un sistema informático. Cuando un sujeto impide u obstaculiza el derecho de uso o disfrute de esa propiedad, se considera al sujeto activo, como un usurpador o detentador, según sea el caso. En el derecho informático es necesario crear mecanismos para regular dicha conducta. En cuanto en la disponibilidad de información esta requiere que se tenga *back-ups* para el mejor manejo de algún tipo de incidente en la cual se intente violentar la disponibilidad de dicha información.

1.4.3. Delitos contra la confidencialidad

El espionaje informático, el acceso ilícito, la reproducción de dispositivos de acceso y la Interceptación ilícita son delitos que atentan contra confidencialidad y la privacidad de las personas.

- **El espionaje informático**

"En el delito de espionaje informático, el delincuente no se limita al puro acceso al sistema, toda vez que es necesario que se apodere, obtenga, revele, transmita o difunda el contenido, parcial o total, del sistema o dato informático. En el delito de espionaje informático, el bien jurídico tutelado por el legislador lo constituye la información y, específicamente, el atributo de confidencialidad de la misma".[12]

El espionaje informático es una forma en la cual el delincuente informático ataca un sistema informático para poder extraer información que se encuentra protegido y este divulga dicha información ya sea para su beneficio o para el beneficio de otro obteniendo beneficios económicos. Un claro ejemplo que se puede mencionar en este delito es la de extracción de secretos de las empresas, para el uso comercial.

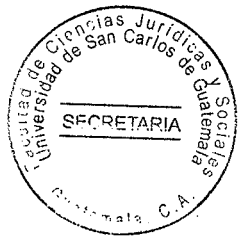
[12] **Ibíd.** Pág. 66.

- **El acceso ilícito**

"El delito de acceso ilícito se refiere al ingreso no autorizado a uno o varios sistemas que utilicen tecnologías de la información. Este tipo de delito tiene relación con la confidencialidad, como un atributo de la información. La conducta ilícita, de acceso ilícito, puede considerarse como una conducta ilícita principal o accesoria. Es principal si la intención del sujeto activo es simplemente la intromisión al contenido de un sistema informático. Es accesorio o preparatorio el acceso ilícito, cuando se acceda a un sistema informático para realizar otro tipo de acciones preparatorias de otro delito".[13]

En este tipo de delitos podemos considerar como principal cuanto tenemos el caso de aquel sujeto, que la apasiona conocer el funcionamiento interno de un sistema informático, aunque su finalidad no sea la de causar un daño. Para considerar este delito como accesorio se debe tener en cuenta que se pueden utilizar medios para obtener una contraseña o para la instalación de interceptores de teclado, denominados comúnmente como *keyloggers*, los cuales registran cada una de las teclas pulsadas y, por consiguiente, todas las contraseñas que se utilizan en el sistema informático pasan a manos del sujeto que ataco dicho sistema y con eso violenta la confidencialidad de la víctima.

[13] **Ibíd.** Pág. 20.



- **La reproducción de dispositivos de acceso**

"cuando se habla de reproducción de dispositivos de acceso, se refiere a la replicación intencional de un componente tecnológico, que permite ingresar a un sistema que tiene a resguardo información o activos de diferente índole".[14]

Este delito puede llegar a ser tan común en el país dado que se puede considerar que los dispositivos instalados en los cajeros automáticos son un claro ejemplo, aunque este puede estar relacionado con el fraude informático, los delincuentes realizan réplicas de los dispositivos de captura de información de las tarjetas de crédito o débito de los cajeros automáticos utilizando teclados que sobreponen en el teclado original, el cual contiene dispositivos de comunicación o de otra especie, que permite la transmisión de la información contenida en la banda magnética, al delincuente que se encuentra cerca del área.

- **La interceptación ilícita**

En términos de informática, el objeto de la interceptación lo constituye la transferencia de datos informáticos de un sistema a otro, los cuales pueden ser definidos como toda representación de instrucciones, caracteres o información que son expresados de

[14] **Ibíd.** Pág. 62.

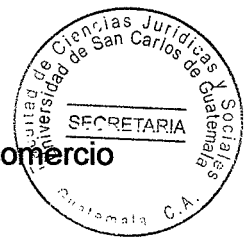
cualquier forma que se presente, incluidos los programas diseñados para que un sistema informático ejecute alguna función para compartir información.

1.4.4. Delitos contra la dignidad de la persona

En este delito se empieza a desarrollar cuando por medio de un sistema informático se adquiera contenido de la intimidad sexual de una persona sin su consentimiento ya sea que se encuentre en mensajes, imágenes o videos en la cual se afecte o se atente contra la dignidad de esta persona, sin embargo no solo el hecho de adquirir puede ser contemplado en este delito, ya que la persona que utilice el sistema informático para realizar el delito, puede de la misma forma comercializar dichos contenidos o utilizar los mismos para obtener beneficio económico de parte de la víctima hacia el delincuente informático.

1.4.5. Delitos contra la propiedad intelectual

"La protección de la propiedad intelectual en el mercado mundial ha tomado creciente significación en los recientes años. Los propietarios de tecnología del mundo desarrollado, particularmente los Estadounidenses, han presionado recientemente para obtener un régimen legal de propiedad intelectual fuerte y relativamente uniforme, como



piedra de toque para obtener un tratamiento equitativo en el sistema global del comercio que emerge."[15]

Al momento en el que se utilice una creación intelectual original en el campo artístico y literario, en la cual el autor obtiene ganancias dinerarias por exportar dichas obras y las cuales se encuentran protegidas por el Estado y estos derechos que son otorgados al ser vulnerados por una persona o varias personas a través del uso de un sistema informático se encuadra en un delito informático contra la propiedad intelectual.

[15] Ríos Estavillo, Juan. **Derecho e Informática en México, informática jurídica y derecho de la informática**. Pág. 88.

CAPÍTULO II

2. Clasificación de los delitos informáticos en la legislación extranjera

En el tema de delitos informáticos en la legislación extranjera existe una amplitud de delitos que se encuentran regulados en las distintas legislaciones de distintos países de América, así como convenio para países europeos y americanos, y de las cuales se trataran algunas en el capítulo.

2.1. Convenio sobre cibercriminalidad o convenio de Budapest

El Articulo 2 de dicho convenio sostiene que "Acceso ilícito: Las partes adoptaran las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Las partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático".

En este Artículo se puede especificar muy uno de los delitos que se trató en el capítulo anterior, en la cual los Estados firmantes tienen la obligación de que tomar las medidas necesarias para combatir este tipo de delitos en los cuales el delincuente informático

accede a la información que se encuentra en el ordenador de otra persona sin su autorización.

De la misma manera dicho cuerpo legal sostiene en el Artículo 3 "Interceptación ilícita: Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos – en transmisión no públicas – en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Las partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático".

Dicho Artículo compromete a que se regule la interceptación ilícita como un delito ya que se está hablando de transferencia de datos informáticos de un sistema a otro y con esto no se sabe qué clase de datos se estarían transmitiendo quedando expuesta información importante a merced de los delincuentes informáticos.

En este cuerpo legal encontramos el Artículo 4 en su numeral primero que establece lo siguiente: "Atentados contra la integridad de los datos: las partes adoptaran las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos".

En este Artículo se prevé las conductas que están destinadas a dañar, alterar o suprimir los datos informáticos que se encuentran en un sistema informático la cual se debe proteger ya que estos datos perteneces a las personas y estos no deben ser obtenidos sin su autorización.

De igual forma en el Artículo 5 del este cuerpo legal regula otro de los delitos ya mencionados y sostiene lo siguiente "Atentados contra la integridad del sistema: las partes adoptaran las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos".

En este Artículo se señala los distintos escenarios que se puede dar al atacar el funcionamiento de un sistema informático, al momento de que es atacado, los delincuentes informáticos pueden simplemente optar por un acto o atacar con todas estas formas, ya sea dañando, alterando o suprimiendo datos informáticos. De esta forma los Estados firmantes se comprometen a regular este delito en su legislación interna porque estos pueden ser perjudicados al ser atacados.

El Artículo 7 sostiene "Falsedad informática: Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y

sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, como independientes de que sean directamente legibles e inteligibles. Las partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal".

Este delito es muy importante regularlo ya que, al obtener datos de un ordenador, este se vuelve muy vulnerable y se pueden falsificar la información que se encuentra en el ordenador afectado para poder utilizarse de una manera no apropiada. Por ese motivo los Estados firmantes se comprometieron a regularlo dentro de sus legislaciones.

De igual forma el Artículo 8 en su literal A regula "Estafa informática: las partes adoptaran las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de: la introducción, alteración, borrado o supresión de datos informáticos".

Es importante la regulación de este tipo de delitos dado que el delito de Estafa informática va encaminada a vulnerar el patrimonio de las personas y de esta manera debe ser regulado, y no solamente a las personas, si no, de esta misma forma se puede vulnerar el patrimonio de un Estado.

De este mismo modo la literal B del Artículo 8 regula "Cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para terceros".

Este apartado es interesante ya que no solo abarca el patrimonio en si del afectado, si no que incluye el solo hecho de intentar afectar el funcionamiento y tratar de obtener un beneficio de esa cuenta ya como constitutivo del delito.

2.2. Código penal de Argentina, con reforma por la ley 26.388

El Artículo 77 del Código Penal Argentino en su párrafo décimo segundo establece "El término **documento** comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión".

En la legislación argentina ya se regula el hecho de que un documento puede ser representado de manera digital, y no solamente a través de un documento físico a través de papel, de esta forma se reformo esta normativa y se protegió esta forma de elaborar documentos.

De esta forma en el Artículo 77 pero en el párrafo décimo tercero regula "Los términos **firma** y **suscripción** comprenden la firma digital, la creación de una firma digital o firmar digitalmente".

Este párrafo lo que establece es la creación y protección de la utilización de la firma digital, con esta implementación da más seguridad y certeza jurídica en las acciones que se realicen con este medio informático.

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

Este Artículo se refiere a las intercepciones que se pueden realizar electrónicamente, el cual el fin primordial es apoderarse de información valiosa con el cual se pueda a llegar a dañar el patrimonio de las personas.

Siguiendo este orden el Artículo 153 en su segundo párrafo regula "En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido".

En este sentido se refiere específicamente a las intercepciones que se pueden realizar para dañar a empresas de carácter privado y comercial o inclusive a entidades pertenecientes al Estado, en donde cuyo sistema se encuentra restringido más que para personas autorizadas para poder acceder al contenido de las mismas.

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

Este Artículo hace referencia al acceso que se realiza de forma ilícita a un sistema informático con el objeto de sustraer información o ciertos tipos de datos informáticos almacenados en dicho ordenador.

Así mismo el Artículo 153 Bis en su segundo párrafo regula "La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

Este Artículo ya regula lo relacionado al acceso ilícito por parte de un delincuente informático en la cual su principal objetivo es atacar o dañar los intereses del Estado, y de este mismo modo las instituciones que pueden estar ligadas al Estado cuando estas estén prestando algún servicio.

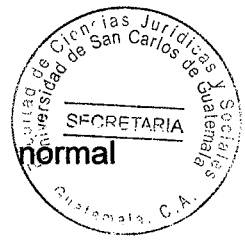
El Artículo 157 Bis en el numeral primero de este cuerpo legal regula "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales".

Este Artículo en dicho numeral regula lo concerniente al delito contra la confidencialidad en la cual se accede un sistema con el fin de violentar los datos que se encuentran en los mismo, los cuales no deben ser públicos por ser muy importantes o de mucha relevancia.

Así mismo este mismo Artículo en el numeral segundo manifiesta "2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley".

Este numeral de dicho Artículo nos hace referencia de igual manera al delito contra la confidencialidad, con la salvedad que este ya no solo regula los datos de algún sistema en general, abarca de una manera amplia los sistemas que guardan datos personales y que la ley protege, estos pueden ser base datos que el Estado maneja.

El Artículo 173 de dicho normativo manifiesta en su numeral dieciséis lo siguiente "Sin perjuicio de la disposición general del Artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece: 16. El que defraudare a



otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

En este Artículo nos encontramos ante un delito contra la integridad, del cual se deriva el delito de daño informático ya que se estaría alterando un sistema y se está afectando su funcionamiento normal.

El Artículo 183 en su segundo párrafo manifiesta "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".

En este Artículo encontramos definido lo relacionado con el delito de daño informático, pero de una forma en la que se está aplicando el resto de los elementos rectores del daño informático la cual es destruir e inutilizar datos de un sistema informático.

Siguiendo el orden de este ordenamiento jurídico citamos el Artículo 184 en su numeral sexto la cual regula "La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

De conformidad con este Artículo se regulan los delitos en la cual se accede ilícitamente y con eso causar un daño a un sistema informático que pertenece específicamente al Estado cuando este está prestando alguno de estos servicios, de igual manera con empresas privadas que presten alguno de dichos servicios.

2.3. Código penal colombiano, con reforma por ley 1273

El Artículo 269 A de este cuerpo legal regula "Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes".

En este Artículo se regula el Acceso Ilícito, ya que se está regulando el acceso a un sistema informático sin autorización y de una forma en la que se acceda hasta el punto en la que el usuario legal no pueda acceder al sistema.

El Artículo 269 B manifiesta "Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos

legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor".

Este Artículo regula la intercepción ilícita, ya que se está obstaculizando ilegítimamente el funcionamiento óptimo de un sistema informático y de igual forma haciendo fallar el sistema al punto de interceptar datos importantes que se transmitan por medio un servidor.

El Artículo 269 D manifiesta "Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes".

Este Artículo regula el daño informático en donde la finalidad del delincuente es la inutilizar o modificar un sistema informático, de igual forma es alterar el normal funcionamiento sin el permiso o el conocimiento del usuario.

El Artículo 269 E de este cuerpo legal regula "Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes".

En este Artículo encuadran varios delitos, en los cuales encontramos la reproducción y alteración de programas informáticos sin autorización del desarrollador y al mismo tiempo el daño informático dado que modifica estos programas con el único objetivo de dañar estos sistemas informáticos.

El Artículo 269 F manifiesta "Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

Este Artículo evidencia que siempre ha sido una necesidad de proteger los datos personales de cada habitante de un Estado, por tanto, el violentar un sistema informático donde se encuentren resguardado estos datos, debe constituirse como un daño y un delito.

El Artículo 269 G de este cuerpo legal regula "Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y

seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave".

En este Artículo se regula lo relacionado a la venta de páginas electrónicas y en la cual se utilizan para la mayoría de ocasiones para estafar a las personas o para realizar fraudes. De este modo se regula lo relativo a diseñar y hasta lo más sencillo que es él envió de los enlaces para acceder a estas páginas.

De la misma manera en el Artículo 269 G en su segundo párrafo manifiesta "En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito".

En este apartado se regula el delito de la manipulación y modificaciones de las direcciones IP de páginas donde se resguarden banco de datos, en la cual se utilicen estos de manera ilícita con el objetivo de acceder a sitios o páginas para poder robar datos, este tipo de delitos normalmente se utilizan para poder acceder a páginas de bancos para poder sustraer datos o en su defecto el capital de la víctima.

2.4. Figuras penales relativas a la informática, ley 19223 de Chile

El Artículo 1 de este cuerpo normativo regula "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo".

Este Artículo regula el delito de daño informático, porque estamos ante los supuestos de destruir o inutilizar un sistema informático, de igual manera tenemos que el que modifique el funcionamiento de un sistema incurrirá en este delito.

El Artículo 2 de este cuerpo legal manifiesta "El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

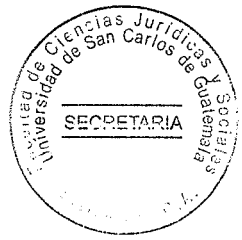
Este Artículo regula la interceptación ilícita, ya que este tipo de ataques lo realizan los delincuentes informáticos mediante ciertos tipos de software los cuales ejecutan y logran interceptar comunicaciones o flujo de información mediante servidores de un sistema informático.

El Artículo 3 de esta ley establece "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio".

En este Artículo se hace énfasis al delito de daño informático, específicamente a las modificaciones que se realizan a un sistema informático, la cual por medio de esta acción se llegue a inutilizar o eliminación permanente de los contenidos de dicho sistema.

Artículo 4 manifiesta "El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

En este Artículo se regula ciertas conductas, las cuales pueden llegar a tener regulado varios delitos informáticos. Uno de ellos será el acceso ilícito, en la cual el delincuente informático accede a un sistema informático, ya sea para dañarlo o para sustraer información, y un segundo delito que puede darse sería el de la falsificación informática porque al acceder se puede utilizar la información que se encuentre en el sistema para cometer actos ilícitos.


Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA

CAPÍTULO III

3. Regulación legal de los delitos informáticos en Guatemala

Como en el capítulo anterior se trató de tocar ciertos delitos regulados en la legislación extranjera, en el capítulo se estudiará lo relativo a dichos delitos, pero en la legislación guatemalteca, es importante estudiar hasta donde está el alcance de estos delitos en Guatemala.

3.1. Constitución Política de la República de Guatemala

El Artículo 2 de la Constitución Política de la República de Guatemala "Deberes del Estado: Es deber del Estado garantizar a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona".

Este Artículo constitucional resguarda a las personas, el estado tiene la obligación de garantizar la justicia, la seguridad, la paz y el desarrollo integral de la persona, sin embargo, estos están siendo violentados al ser objeto de los delitos informáticos, cuando se comete un delito informático se violenta la seguridad de la persona, se perturba la paz de esta y conlleva a que no se lleve a cabo el desarrollo integral de la persona.

El Articulo 42 de la Constitución Política de la República de Guatemala "Derecho de autor o inventor: se reconoce el derecho de autor y el derecho de inventor; los titulares de los

mismos gozaran de la propiedad exclusiva de su obra o invento, de conformidad con la ley y los tratados internacionales".

Este Artículo es el más violentado en relación a la Reproducción no autorizada de programas informáticos, ya que el autor no está gozando en su totalidad la exclusividad de su obra, ya que no está percibiendo ingresos que pudiere tener al ser comercializado sin su autorización.

3.2. Código Penal, Decreto 17-73 del Congreso de la República

El Artículo 4 del Código Penal Decreto 17-73 del Congreso de la República establece "Territorialidad de la ley penal: Salvo lo establecido en tratados internacionales, este código se aplicará a toda persona que cometa delito o falta en el territorio de la Republica o en lugares o vehículos sometidos a su jurisdicción."

En base a este Artículo se hace la salvedad hasta donde se aplicarán las normas relativas a delitos informáticos que se encuentran regulados en el Código Penal de Guatemala, únicamente se aplicara a delitos cometidos en el territorio o vehículos dentro de su jurisdicción, salvo tratados internacionales, que es uno de los puntos en los que Guatemala debe avocarse para estar en la vanguardia en cuanto delitos informáticos.

El Artículo 274 A del Código Penal regula "Destrucción de registros informáticos. Será sancionado con prisión de seis meses a cuatro años y multa de dos mil a diez mil

Quetzales, quien destruya, borre o de cualquier modo inutilice, altere o dañe registros informáticos".

Este Artículo regula el delito de daño informático, sin embargo, el Código lo denomina como Destrucción de registros informáticos. Esto da la pauta que el delincuente pueda inutilizar o dañar el sistema completo, dado que únicamente se regula lo relativo a los registros informáticos.

De este modo, el Artículo 274 A en su segundo párrafo regula "Si la acción contemplada en el párrafo anterior estuviere destinada a obstaculizar una investigación o procesamiento de carácter penal, el responsable será sancionado conforme el Artículo 458 Bis del presente Código".

En el segundo párrafo de dicho Artículo regula lo concerniente a la acción del daño en cuanto sirva para obstaculizar la investigación, sin embargo, esto va relacionado al primer párrafo, no sirve de nada tener tipificado la acción, si no hay un alcance mayor.

Así mismo, el Artículo 274 B del mismo cuerpo legal establece "Alteración de programas. La misma pena del Artículo anterior se aplicará al que altere, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras."

En este Artículo se encuentran lo relativo al daño que se realiza o la alteración que se realiza a los programas que se utilizan para el funcionamiento de un sistema, un ejemplo claro es, cuando se instala un sistema operativo sin licencia del creador.

El Artículo 274 C del mismo cuerpo legal regula "Reproducción de instrucciones o programas de computación. Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación."

En este Artículo se regula lo relativo a la reproducción fraudulenta de programas, es muy común que personas lucren con programas informáticos sin la autorización del creador o desarrollador, de este afecta tanto la economía de este, como de muchas empresas que adquieren los productos de manera legal.

El Artículo 274 D preceptúa "Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas".

Siguiendo el hilo de los delitos informáticos, este delito lo podemos encuadrar en el delito de espionaje informático, dado que se accede de forma ilícita a un sistema con el único objetivo de obtener información y una vez obtenido se divulga ya sea de manera lucrativa o únicamente para afectar a las víctimas.

El Artículo 274 E, regula lo siguiente "Manipulación de Información. Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica".

En este Artículo se puede encuadrar dentro del delito de fraude informático, ya que se utiliza un sistema informático para ocultar información y omitir obligaciones que se tengan con el Estado y con eso se afecta las arcas del Estado, normalmente se realizan para la omisión de pago de impuestos y otras obligaciones tributarias.

El Artículo 274 F regula lo siguiente "Uso de información. Se impondrá prisión de seis meses a dos años, y multa de dos mil a diez mil quetzales al que, sin autorización, utilice u obtenga para sí o para otro, datos contenidos en registro informáticos, bancos de datos o archivos electrónicos".

Acá se encuentra regulado el delito de acceso ilícito, porque se está ingresando de manera ilícita a un sistema y se está obteniendo información valiosa, ya sea que afecte la información personal de una persona o de manera patrimonial, se puede obtener datos de bancos y de cuentas de las mismas.

El Artículo 369 en su numeral 3º manifiesta "Espionaje Genérico. Comete este delito: 3º. Quien procurare u obtuviere, indebidamente, información secreta, concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores del Estado, será sancionado con prisión de seis meses a dos años y multa de doscientos a dos mil quetzales".

Se toma en consideración este Artículo, dado que únicamente se toma en consideración como se regula un espionaje genérico, sin embargo, este cuerpo normativo no regula lo relacionado al espionaje informático, es de suma importancia por el hecho de que ahora se puede llevar a cabo a través de sistemas informáticos los espionajes.

3.3. Ley de Derechos de Autor y Derechos Conexos, Decreto 33-98 del Congreso de la República de Guatemala

El Artículo número 1 de este cuerpo normativo establece "la presente ley es de orden público y de interés social, y tiene por objeto la protección de los derechos de los autores de obras literarias y artísticas, de los artistas intérpretes o ejecutantes, de los productores de fonogramas y de los organismos de radiodifusión".

Cuando se menciona en este Artículo derecho de autor se suele interpretar como los derechos de los creadores sobre sus obras literarias y artísticas. En realidad, las obras que abarca el derecho de autor van desde los libros, la música, la pintura, la escultura y las películas hasta los programas informáticos, las bases de datos, las publicidades, los

mapas y los dibujos técnicos en este sentido es acá donde se debería basar para incluir la violación de estos derechos como un delito informático.

El Artículo 2 en su primer párrafo regula lo siguiente "en la materia que regula la presente Ley, los nacionales de cualquier país gozan de los mismos derechos, recursos jurídicos y medios legales para defender sus derechos, que los guatemaltecos".

Conforme este Artículo, se da la pauta para que los autores extranjeros puedan utilizar los medios legales pertinentes para defender sus derechos, en ocasiones se violentan estos derechos, se reproducen las obras sin la autorización de este porque se encuentra en el extranjero, aunque esta se hubiere publicado en el territorio nacional.

Así mismo este mismo Artículo en su segundo párrafo regula "Las obras publicadas en el extranjero gozan de protección en el territorio nacional, de conformidad con los tratados y convenios internacionales aprobados y ratificados por la República de Guatemala. Las interpretaciones y ejecuciones, los fonogramas y las emisiones de radiodifusión, cuyos titulares sean ciudadanos extranjeros, gozan de la misma protección".

Este Artículo regula lo relacionado con la protección que se le da al artista por obras publicadas en el extranjero y que se reproducen en el territorio nacional sin la previa autorización del autor. Esto se regula con el objetivo de que no hubiere distinción alguna con el autor extranjero.

El Artículo 5 del presente cuerpo normativo regula "Autor es la persona física que realiza la creación intelectual. Solamente las personas naturales pueden ser autoras de una obra; sin embargo, el Estado, las entidades de derecho público y las personas jurídicas pueden ser titulares de los derechos previstos en esta ley para los autores, en los casos mencionados en la misma".

Este Artículo hace una diferencia importante, el autor únicamente puede ser una persona individual, natural o humana, dado que solamente estas tienen la capacidad volitiva para hacer las creaciones de las obras. Sin embargo, como se establece tanto las personas jurídicas como el Estado pueden ser titulares de los derechos de estas obras y pueden obtenerlas del autor.

El Artículo 15 primer párrafo de la presente norma legal regula "Se consideran obras todas las producciones en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión, siempre que constituyan una creación intelectual original".

Este Artículo especifica lo relativo a la obra, el cual es una creación intelectual del ser humano y que es original tanto en el campo artístico como literario. Así mismo en el campo científico podemos incluir lo relativo a programas informáticos.

Así mismo el mismo Artículo en su literal a) regula "a) las expresadas por escrito, mediante letras, signos o marcas convencionales, incluidos los programas de ordenador".

Este Artículo como ya se mencionó se incluye los programas informáticos como una obra, ya que al inscribirse empiezan a gozar de las protecciones de los derechos que derivan de dicha inscripción.

El Artículo 18 preceptúa "El derecho de autor comprende los derechos morales y patrimoniales, que protegen la paternidad, la integridad y el aprovechamiento de la obra".

El derecho de autor cuando se dice que comprende un derecho moral se debe incluir la paternidad y la integridad y eso podemos decir que es el vínculo que existe entre el autor y la obra que se crea, cuando se habla de integridad se refiere al derecho que tiene el autor de que su obra no sea dividida en fragmentos y que esta permanezca integra, así como se publicó.

El Artículo 21 regula "El derecho pecuniario o patrimonial confiere al titular del derecho de autor, las facultades de usar directa y personalmente la obra, de ceder total o parcialmente sus derechos sobre la misma, y de autorizar o prohibir su utilización y explotación por terceros".

Como ya se había mencionado el derecho de autor comprende los derechos morales y patrimoniales, este Artículo menciona específicamente los derechos patrimoniales, los cuales no son más que, los derechos que tiene el autor de la obra de obtener ganancias dinerarias de la misma, ya sea de manera directa o indirecta.

3.4. Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala

El considerando segundo de dicho cuerpo normativo preceptúa "Que la inmersión masiva de la tecnología en nuestra sociedad es una realidad que no podemos ignorar y por ende se debe revisar los conceptos y visiones tradicionales del mundo físico para adaptarlos al actual contexto del mundo digital".

Como se sabe, hoy en día es difícil estar aislado del mundo de la tecnología, ya que es cambiante y es imposible ignorarla, y esto obliga a estar inmerso en ella, por ende, es indispensable agregarlo en las actividades cotidianas y al mundo laboral, con esto se puede competir en el mundo comercial.

De igual manera el Considerando tercero regula "Que la promoción del comercio electrónico en todos sus aspectos requiere de una legislación cuyo fundamento sea, entre otros, la facilitación del comercio electrónico en el interior y más allá de las fronteras nacionales, la validación, fomento y estimulo de las operaciones efectuadas por medio de las nuevas tecnologías de la información sobre la base de la autonomía de la voluntad y el apoyo a las nuevas prácticas comerciales, tomando en cuenta en todo momento la neutralidad tecnológica"

Se entiende que, así como se es indispensable la tecnología en las actividades para el desarrollo, así mismo se necesita una legislación que regule las actividades del comercio

electrónico. Este se basa en la autonomía de la voluntad, tomando en cuenta la neutralidad tecnológica, la que se refiere a la libertad que posee las personas, instituciones, empresas y organismos del Estado para elegir qué tipo de tecnología implementar.

El Artículo 1 en su primer párrafo de esta norma legal regula "Ámbito de aplicación. La presente ley será aplicable a todo tipo de comunicación electrónica, transacción o acto jurídico, público o privado, nacional o internacional"

Este Artículo regula la aplicación de la ley en cuanto a las actividades comerciales electrónicas que se realizaran, tales como la comunicación electrónica y los actos jurídicos públicos o privados, en este apartado podemos ver que se incluyen los actos jurídicos públicos, por lo que abarca actividades que puede realizar el Estado como persona jurídica.

El Artículo 1 en su segundo párrafo regula "El Estado y sus instituciones quedan expresamente facultados para la utilización de las comunicaciones y firmas electrónicas".

Como ya se había mencionado, el Estado como persona jurídica, puede ejercer la facultad que se le otorga de la utilización de comunicaciones y firmas electrónicas, con el objetivo de agilizar los trámites, para un mejor funcionamiento de sus actividades.

El Artículo 1 en su quinto párrafo preceptúa "Las normas sobre la presentación de servicios de certificación de firma electrónica que recoge esta ley, no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos".

En este apartado queda regulado lo relativo a las personas facultadas para dar fe de las firmas en documentos, con esto se refiere al Notario al ejercer su actividad notarial dado que el Notario posee fe pública, por ende, no se puede sustituir por la firma electrónica.

3.5. Iniciativa de Ley Número 4055, Ley de Delitos Informáticos del Congreso de la República

Se toma en consideración esta Iniciativa de Ley, por ser de suma importancia para que Guatemala se encuentre a la vanguardia en legislación en el tema de delitos informáticos, por lo tanto, es importante tomar en cuenta dicha iniciativa para poder tener un campo más amplio de regulación conforme este tema por lo que desarrollaremos lo más relevante de esta iniciativa.

Según El Artículo 1 primer párrafo de esta iniciativa de ley regula "Objeto de la ley. La presente ley tiene por objeto la protección integral de las personas, sus bienes y derechos, mediante el establecimiento de un marco jurídico relativo a los sistemas que utilicen tecnologías de la información, así como la prevención y sanción de los delitos

cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas físicas o jurídicas, en los términos previstos en esta ley".

Siendo el objeto principal de la comisión de los delitos informáticos, la vulneración de los derechos, integridad y sobre todo patrimonio de las personas, por lo que esta iniciativa regula y especifica que el objeto es la protección de estos derechos en la comisión de los delitos que utilice tecnología informática.

El Artículo 2 en el párrafo primero regula "Acceso ilícito. Quien acceda a sistema que haga uso de tecnologías de la información, sin autorización o excediéndola, será sancionado con prisión de dos a cuatro años y multa de cien a quinientas veces el salario mínimo legal vigente".

Este delito lo que busca es la intromisión al contenido que se encuentra en un sistema informático, y a través de estos actos se originan determinadas vulnerabilidades de sistemas burlando la seguridad del mismo

El Artículo 6 preceptúa "Daño informático. Comete el delito de daño informático quien, sin estar autorizado, alterare, destruyere, inutilizare, suprimiere, modificare, o de cualquier modo o por cualquier medio, dañare un sistema que utilice tecnologías de la información o un componente de éste será sancionado con prisión de cuatro a ocho años y multa de cien a quinientas veces el salario mínimo legal vigente".

Cuando se habla del daño informático se refiere a la alteración a la integridad de cualquier sistema informático, con esto nos estamos refiriendo a los sistemas de cómputo, los programas que estos poseen, datos que se encuentran dentro del sistema, así como a las redes a los que este se encuentra conectado.

El Artículo 7 regula "Reproducción de dispositivos de acceso. Quien de manera deliberada, cree, utilice, altere, capture, grabe, copie o transfiera de un dispositivo de acceso a otro similar, o cualquier instrumento destinado a los mismos fines, los códigos de identificación y/o acceso al servicio o sistema que haga uso de tecnologías de la información, que permita la operación paralela, simultánea o independiente de un servicio legítimamente obtenido, será sancionado con prisión de cuatro a ocho años y multa de cien a quinientas veces el salario mínimo legal vigente".

Este delito lo podemos mencionar como la utilización de componente o dispositivo tecnológico o informático, en la cual se utiliza para poder ingresar a un sistema y asi poder acceder a los archivos del mismo. Actualmente este delito se realiza con mayor frecuencia.

El Artículo 8 de esta iniciativa regula lo siguiente "Dispositivos fraudulentos. Quien produzca, utilice, comercialice u ofrezca sin autorización o causa legítima, uno o varios programas informáticos, equipo, material o dispositivo cuyo uso principal sea el de

emplearse como herramienta o medio para cometer los delitos regulados en la presente ley".

En este delito se puede utilizar distintos medios para la comisión del delito, ya sea a través de programas, como equipo y dispositivos informáticos, esto debido a que por medio de estos se puede ingresar a un sistema y así afectar los archivos o incluso a cuentas y dañar el patrimonio de las personas.

El Articulo 9 nos establece "Espionaje informático. Comete el delito de espionaje informático quien, sin estar facultado para ello, se apodere, obtenga, revele, transmita o difunda el contenido, parcial o total, de sistema que utilice tecnologías de la información o dato informático, de carácter público o privado, será sancionado con prisión de seis a diez años y multa desde doscientas a setecientas veces el salario mínimo legal vigente".

Como se explicó, es indispensable que se tomen en cuenta los delitos informáticos dentro de la legislación guatemalteca, y en especial el delito de espionaje informático, ya que este se puede utilizar para atentar contra empresas para obtener formulas o secretos de los mismo, así como, contra el Estado, para obtener información que afecte la seguridad contra la Nación.

El Artículo 10 de esta iniciativa regula "Violación a la disponibilidad. Quien, por cualquier medio, provoque la denegación de acceso a redes, información y sistemas que utilicen tecnologías de información, a las personas que están legitimadas para hacerlo, se

sancionará con pena de seis a diez años de prisión y multa desde cien a quinientas veces el salario mínimo legal vigente".

Al obstaculizarse el acceso a la información contenida a un sistema o una red, se produce consecuencias las que pueden transcender al ámbito jurídico, ya que al ser violentado la disponibilidad del sistema informático de una persona esta puede tener pérdidas de información y esto podría llevar a que posteriormente deba pagar daños a un tercero.

El Artículo 11 preceptúa "Fraude informático. Quien, para obtener algún beneficio para sí mismo o para un tercero, mediante cualquier artificio tecnológico o manipulación de sistema que haga uso de tecnologías de la información, o, a sus componentes, procure la transferencia no autorizada de cualquier activo patrimonial en perjuicio de otro, será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente".

Este delito se enfoca en la manipulación de sistemas informáticos para afectar el patrimonio, ya que al ser atacado un sistema lo que busca en un principio es afectar cuentas bancarias, hoy en día este delito es muy común y es de suma importancia regularlo para resguardar el patrimonio de las personas.

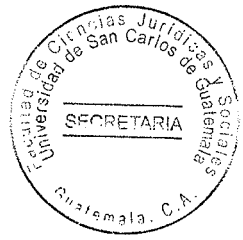
El Artículo 12 regula "Interceptación ilícita. Quien intercepte de forma deliberada e ilegítima por cualquier medio, datos informáticos en transmisiones restringidas, dirigidas u originadas en un sistema que utilice tecnologías de la información, incluidas las

emisiones electromagnéticas provenientes o efectuadas dentro del mismo, que transporte dichos datos informáticos, será penado con prisión de seis a diez años y multa desde cien hasta mil veces el salario mínimo legal vigente".

Este delito es importante regular, ya que pueden ser peligrosa las interceptaciones de datos informáticos, ya sea que, se cometa el delito a una empresa y con ello llegue a sufrir daños, perdidas e inclusive llegar a tener consecuencias legales. Así como podrían ser interceptados datos que sean transmitidas por los organismos del Estado y con eso tener repercusiones en sus actuaciones.

El Artículo 13 regula lo siguiente "Falsificación informática. Quien, a través de cualquier medio, copie, altere, sustituya deliberada e ilegítimamente datos informáticos de un sistema que haga uso de tecnologías de la información o uno de sus componentes, generando un resultado no auténtico o para inducir a usuarios a la provisión de datos personales y/o financieros, será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente".

Este delito es importante encontrarla en la legislación de nuestro país, ya que al existir una ley que reconoce las comunicaciones y el reconocimiento de firmas electrónicas, se vuelve vulnerable que los sujetos activos para cometer el delito, y así acceder a los datos que contiene un sistema informático.


Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.

CAPÍTULO IV

4. Reproducción no autorizada de programas informáticos de protección legal

Los sistemas informáticos y el internet han venido a cambiar nuestro modo de comunicarnos y nuestra forma de trabajar. En la actualidad, es tal la forma de utilizar esos sistemas como herramientas que, más que recursos para el diario vivir, se han convertido en una necesidad que no se puede dejar de lado. En los sistemas informáticos se han depositado gran parte de confianza, a tal grado que se almacena buena parte de información personal, como lo son los datos bancarios, contenidos personales, como fotografías además de contraseñas de cuentas de correo.

Debido a esta necesidad de la utilización de los sistemas informáticos y a su vez la utilización de programas, la reproducción no autorizada de estos programas que cuentan con protección legal puede llegar a convertirse en una pérdida económica considerable para los propietarios o autores de estos.

En cuanto a él bien jurídico que se trata de proteger en este delito no encontramos con que lo que se busca proteger es la información o los datos que contiene el programa en sí, pues el programa informático técnicamente está conformado por datos que son programados de tal forma que constituye el bien informático del que se habla, por tanto, el programa informático es el bien jurídico que se busca proteger por la ley al ser puesto en funcionamiento y así mismo en el mercado para su distribución.

4.1. Que es una reproducción ilegal

Esto ocurre, principalmente, porque el internet es la fuente más importante de información teniendo un ámbito bien amplio y tiene una forma tan sencilla de utilizar, es un arma muy poderosa, no solo por los que desean perjudicar a terceros, sino para quienes buscan lucrar, esto a través de la copia de juegos de computadoras, descargando música sin haber pagado por ella, así como películas y programas informáticos que son distribuidos y que son adquiridos por las personas, esto porque son mucho más económicos a tal punto que son Consumidos de una forma que no se detiene, y que, al ser adquiridos estos productos ilegales, se está contribuyendo a dañar el trabajo de sus autores intelectuales.

4.2. Delitos que se incurre por la reproducción ilegal

Dentro del marco de la reproducción ilegal se pueden encontrar distintos delitos dentro de los cuales encontramos la piratería informática o piratería de *softwares,* también encontramos lo delitos que transgreden los derechos de autor.

En cuanto a los derechos de autor, los programas informáticos y otros tipos de *software* están consideradas obras literarias. Por consiguiente, quedan protegidos sin necesidad de ser registrados. En algunos países, el proceso para el registro se torna voluntario en cuanto a los programas informáticos o *software.*

4.2.1. Piratería informática

Uno de los delitos que se pueden cometer en la reproducción ilegal es la Piratería informática, la cual consiste en la elaboración de copias de los programas informáticos, sin la autorización del autor. El objetivo de la elaboración de las copias de los programas informáticos es para la venta y así obtener ganancias.

Cuando se hace referencia a la piratería informática, se refiere al robo o hurto la cual se realiza a través del plagio ilegal de los programas informanticos los cuales se realizan comúnmente a través de internet, en el caso de Guatemala, se ha tornado muy común que este tipo de acciones se lleven a cabo en ciertos lugares, donde es muy común observar cómo se comercializan los programas de una manera masiva.

Esta distribución masiva de forma de los programas, la cual se puede realizar de forma comercial o a su vez puede ser de uso particular, esta puede acción puede o no ser deliberada al momento de reproducirle, de cualquier forma, es de manera ilegal y esta debe ser sancionada por la ley.

Al realizar la acción de la piratería para uso particular se hace referencia a que se realizan por los denominados usuarios finales, el cual se lleva a cabo cuando la copia es prestada entre amigos, por lo que no se lleva a saber la cantidad de veces en la que fue instalado en un sistema el *software*. Cuando se realiza la acción para uso comercial se refiere a

que, esta forma se realiza al desarrollar copias de una forma mayor y se distribuye a gran escala el software copiado ilegalmente.

De igual forma con el hecho de que se obtenga o se llegue a modificar la información de programas ya sea a través de páginas web, otras computadoras o sistemas informáticos de algunas empresas se incurre en la piratería informática.

Debido a que esta forma de realizar copias de los programas informáticos no se elabora mediante un control, se ofrece al público en una versión más barata, pero con una calidad menor y sin contar con garantía.

Como se comentó la piratería es una forma de reproducir los programas informáticos de una forma no autorizada, sin embargo, después de saber que es, también es importante saber quién realiza este tipo de acciones que se consideran ilegales, a estos sujetos se le denominan pirata informático.

El pirata informático es la persona que regularmente a través de una red, realiza en primer lugar el accede al programa informático y posteriormente reproduce este, ya sea para comercializar con este o para utilización personal y proporcionarlo de manera gratuita a diferentes usuarios.

Ahora que tenemos una idea de los que es un pirata informático y cuál es su objetivo o como realiza la acción, hay que mencionar que existen varios tipos de piratas

informáticos, pero solo tocaremos algunos que interesan al tema, los cuales son *Cracker* y el *Hacker*.

Cracker: "El término cracker (del inglés cracker, 'romper') se utiliza para referirse a las personas que rompen algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío".[16]

Estos piratas informáticos manejan la tecnología perfectamente, ya que utilizan la programación y a su vez utilizan la parte física de un sistema para poder acceder a él. Ya que estos sujetos en su mayoría de veces se dedican a romper todo tipo de protección de los programas en su mayoría comerciales, con el único fin de sacar un provecho al utilizar códigos para que las copias que se realicen se puedan utilizar y así obtener un beneficio económico.

Por su parte se define a el *hacker* como "Es simplemente un programador inteligente, experto en manipular o modificar un sistema o red informática, un *hacker* malicioso es alguien que utiliza sus conocimientos de informática para obtener acceso no autorizado a datos tales como información de tarjetas de crédito o imágenes personales, ya sea para diversión, beneficio, para causar daño o por otras razones".[17]

---

[16]http://www.ictea.com/cs/index.php?rp=/knowledgebase/2090/i**Que es-un- cracker**.html (consultado 13 de febrero de 2020)

[17] https://www.avast.com/es-es/**c-hacker** (consultado 20 de febrero de 2020)

El *hacker* es un sujeto a quien le resulta muy interesante lo relativo al funcionamiento de los sistemas operativos, por lo que le gusta ingresar y acceder a cada una de las partes de los mismos, ya que por su habilidad pueden crear sus propios softwares a partir de los conocimientos que obtienen al ingresar a los sistemas.

4.2.2. Delitos contra los derechos de autor

El derecho de autor es reconocido y protege los derechos reconocidos, al creador de una obra la cual es personal y original, estos derechos nacen por el hecho de la creación. Por lo que, al registrarlo puede servir como prueba de plagio.

La tutela de la creación intelectual de una obra contiene varios fines uno de ellos es la de difusión de los valores culturales, así como el de fomento del desarrollo tecnológico; no se torna atractivo el utilizar talento y esfuerzo en crear una obra para que otras personas aprovechen indebidamente de los frutos del trabajo realizado. Por lo concerniente, la protección jurídica hacia los derechos de autor se puede emplear en dos aspectos fundamentales, los cuales son la propiedad o titulación del autor sobre su obra y el goce de los beneficios que deriven, en especial los económicos, así como las que deriven de su explotación.

Se debe tener presente que no se protegen las ideas, sino la forma en que se desarrollan y exteriorizan esas ideas. La razón de esto es que existe un interés en el libre uso de las

ideas puesto que con ello se desarrolla y se llega a progresar la ciencia y el arte; por lo tanto, no se puede establecer un monopolio o un derecho exclusivo sobre las ideas.

Existe un listado sobre distintas obras que son susceptibles de protección, entre las que podemos mencionar las obras literarias, ya sean que se encuentre en forma escrita u orales; también podemos mencionar las composiciones musicales; las obras audiovisuales; las obras de artes plásticas; las obras fotográficas; y también los programas de ordenador.

Al programa informático se le considera un bien, debido a que se desarrolla a través de un proceso intelectual y a su vez industrial el cual se llega a convertir en un servicio que se utiliza al aplicarlo en un sistema específico.

El programa informático al ser una parte intelectual la cual manifiesta en su esencia lo que realmente representa un computador ya que, como tal, el programa informático tiene un valor comercial ya que alrededor de esta gira una suma de dinero.

El programa informático constituye aquellos derechos inherentes que conforma la propiedad intelectual, de los cuales a su creador se le debe amparar ya que se afecta lo relativo a los derechos de autor, sin embargo, no es simplemente el programa, si no, lo que constituye este, a lo cual se hace énfasis ya que estos programas constituyen una serie de instrucciones los cuales se convierten en datos informáticos.

El dato informático no es más que un conjunto de instrucciones en forma de algoritmos que transportan mensajes y que con los cuales se crea el programa, por lo tanto, estos datos representan un bien o patrimonio económico de una persona o empresa desarrolladora, ya que este se vuelve una mercancía para dicha persona o empresa.

Debido a que el dato informático es parte del programa, estos datos pueden ser susceptibles de ataques que a su vez conllevan a la modificación de su forma original, esto se realiza a través de la realización de copias que no se encuentra autorizadas, también alterando su contenido, así mismo al impedir el acceso de las personas autorizadas para poder acceder a ellos.

En relación a los derechos de autor, no encontramos con el denominado *Copyright* el cual hace referencia al derecho que se tiene de realizar copias autorizadas de ciertos datos, los cuales, si bien no existe un control sobre este derecho, existe un sistema de protección, en el cual el propietario del programa permite que usuarios realicen ciertos tipos de descargas, sin embargo, estos están contenidos en archivos de tal manera de que estas no puedan copiarse y transferidas masivamente.

El *copyright* hace referencia específicamente a los derechos patrimoniales que posee el creador de la obra, en este caso del programa informático, por lo que la violación al copyright debe ser sancionado, ya que produce perdidas inmensas al realizar copias no autorizadas masivamente.

4.3. Formas en las que se puede realizar la reproducción ilegal

En el tema de reproducción ilegal de programas informáticos existen varias formas en las que se pueden llevar a cabo, de las cuales mencionaremos algunas de las que comúnmente se llevan a cabo diariamente en Guatemala y de las cuales se reproducen a gran escala.

4.3.1. Reproducción de usuario final

Esta forma de reproducción a menudo se encuentra en los usuarios comunes a los que se le denomina usuario final, dado que copian el *software* en distintos equipos y sobrepasan el límite que la licencia que otorga el fabricante permite. Es común que cada programa que se instala en un ordenador debe contener su propia licencia.

4.3.2. Reproducción cargada a disco duro

Es común que se encuentre lugares o distribuidores en donde se venden equipos de cómputo de segunda mano, en la cual estos distribuidores cargan previamente los programas informáticos, los cuales no poseen una licencia original y a su vez no les suministran a los clientes las licencias necesarias para que el equipo y los programas funcionen como debe ser. Comúnmente estos programas no provienen del creador o desarrollador, si no que fue adquirido y reproducido ilegalmente.

4.3.3. Reproducción a través de cd-room

Este es otra forma que se observa comúnmente en distintos lugares, existe un sinfín de vendedores ilegales, que frecuentemente venden una copia de los programas sin la autorización del creador, ofreciéndolos como que, si fuera una copia genuina, con el fin de obtener una ganancia al comercializar estos programas utilizando tanto los nombres de las empresas desarrolladoras como las marcas con las que se comercializan.

4.3.4. Reproducción a través de internet

Esto es común en la actualidad, ya que hoy en día un buen número de personas poseen conexión a internet en sus residencias, ya este tipo de reproducción de programas implica la distribución no autorizada de manera electrónica la cual se realiza por medio de internet, así como la descarga de dichos programas por el mismo medio, afectando el *copyright* de los programas informáticos.

4.4. Consecuencias que conlleva la reproducción no autorizada de programas informáticos de protección legal

Como se ha mencionado la reproducción de programas informáticos se puede realizar de distintas maneras, así mismo los delitos a los que se incurre al realizarlos, sin embargo, los consumidores de estos programas que no son los originales tratan de

justificar la adquisición de dichos programas aduciendo que el valor del mismo es mucho más bajo que el programa original, lo cual para ellos es más accesible adquirirlos.

Sin embargo, para el consumidor contrae varias consecuencias, ya que cuando decide hacer una copia no autorizada de programas informáticos de protección legal, está renunciando a ciertos derechos que se adquieren junto con la compra de un programa original, los cuales pueden ser la asistencia por posibles problemas en el futuro, garantías que se ofrecen, así como actualizaciones que se realizan constantemente. Otro de los riesgos a los que el usuario está expuesto al adquirir estos programas es la adquisición de los famosos virus, los cuales podrían dañar el sistema del ordenador.

Desde el punto de vista legal el usuario al adquirir o reproducir sin autorización estos programas que se encuentran protegidos, se pone en riesgo de que se tomen acciones legales tanto en la rama penal por violentar los derechos del autor, como en la civil para la restitución del patrimonio afectado.

Otra de las consecuencias que se deriva de la reproducción no autorizada de programas informáticos de protección legal es la que afecta a los desarrolladores o creadores de los programas, ya que representa una pérdida de ingresos económicos por cada copia que se reproduce de manera ilegal.

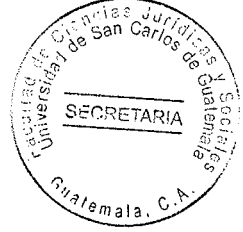
Así mismo el realizar copias sin autorización repercute en los desarrolladores al obtener una baja considerable en el éxito de sus productos ya que estos trabajan y emplean

mucho tiempo tanto intelectual como industrial para elaborar los programas para tener en el mercado su propia existencia.

Las consecuencias que derivan de la reproducción sin autorización de los programas informáticos es muy significante, ya que para los vendedores que poseen la autorización para comercializar los productos, representa una pérdida significante, y esto conlleva a que estos vendedores autorizados ya no quieran seguir poniendo al mercado dichos productos. Y así obteniendo perdidas enormes en sus negocios, ya que ellos pagan impuestos para poder ingresar el producto al país.

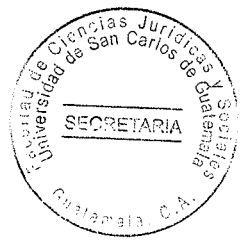
Sin embargo esto no parece importarle a los vendedores y distribuidores que comercializan con copias no autorizadas de los programas informáticos, ya que no solamente afectan al vendedor autorizado, si no, que a su vez afecta a los ingresos del Estado, ya que estos al reproducir y comercializar los programas de manera ilegal no pagan los impuestos que corresponden, eso sumado a que los vendedores autorizados decidan ya no ingresar dichos productos para no tener pérdidas, generan un debacle para los interese del Estado.

Este tipo de accionar, está generando grandes cantidades de perdidas, ya que no solamente los vendedores autorizados pierden, sino que, al existir una dimensión enorme de estos comerciantes que distribuyen sin autorización crean un nivel de desconfianza para los inversionistas o los desarrolladores que quisieran incorporar a nuestro mercado sus programas.



De igual manera la problemática no culmina ahí, ya que al generar ganancias estrepitosas por parte de estas personas que venden sin autorización los programas que poseen protección legal están elaborando una brecha para que la comercialización de estos productos sea más recurrente y con esto más personas empezaran a realizar este tipo de actividades ilícitas.

Sin embargo, es necesario implementar un sistema de información hacia las personas, con el fin de que concientice a la población del mal que se le hace a la economía del país al comercializar de manera ilegal los programas informáticos, ya que muchas personas ignoran la magnitud del problema cuando realiza dichas acciones.

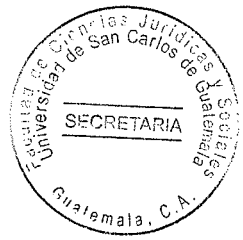

Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.

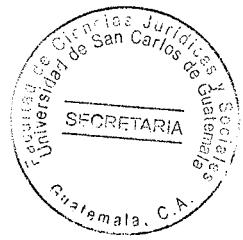
CONCLUSIÓN DISCURSIVA

Se infiere que al llegar a Guatemala los sistemas de informática y la internet, trajo consigo la evolución en la utilización de estos más a menudo dentro del diario vivir de la población, generando una fuente donde se puede delinquir, sin embargo algo tan importante no se encuentra regulado en su totalidad dentro de normativas de observancia general y ha generado un sinfín de conflictos en cuanto a la aplicación de esto tanto en el Departamento de Guatemala como a nivel nacional en relación a la reproducción de programas informáticos de protección legal.

La problemática se puede resolver regulando estos tipos de delitos y la actividad que se realizan dentro de la legislación guatemalteca, con el fin de reducir de cierta manera la utilización de programas informáticos para cometer delitos y así mismo dañar el patrimonio de los interesados e inclusive del mismo Estado, ya que al reproducir un programa informático de protección legal se está dejando de percibir ingresos al importar dichos programas legalmente.

Por lo que es necesario que el Congreso de la República de Guatemala, apruebe la iniciativa de Ley número 40-55, con el objeto de incluir dentro de la legislación nacional los tipos de delitos informáticos, así como las penas que se aplicaran y el procedimiento que se deba utilizar para la aplicación de este cuerpo normativo. Debido a que el actual cuerpo normativo que regula lo relacionado a los delitos informáticos no los regula por completo.


Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.



BIBLIOGRAFÍA

ALVARADO LEMUS, José y coautores. **Ciber crimen**. 1ª ed. Guatemala, Guatemala: Ed. ius ediciones, (s.f)

ACURIO DEL PINO, Santiago. Delitos Informáticos: Generalidades. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf. (Consultado: 15 de noviembre de 2020)

GÓMEZ VIEITES, Álvaro. **Auditoria de seguridad informatica**. 1ª ed. Bogotá, Colombia: Ed. Ediciones de la U, 2013

HERNANDEZ DÍAZ, Leyre. **El delito Informático**. Httpps://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf (Consultado: 14 de noviembre de 2020)

https://www.avast.com/es-es/**c-hacker** (consultado 20 de febrero de 2020)

http://www.ictea.com/cs/index.php?rp=/knowledgebase/2090/i**Que es-un-cracker**.html (consultado 13 de febrero de 2020)

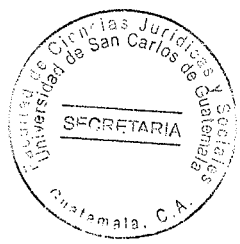
https://www.le-vpn.com/es/**delito-cibernetico-origen-evolucion/** (consultado 27 de abril de 2017)

http://eprints.uanl.mx/3536/1/**Delitos_informaticos.pdf** (consultado 15 de enero de 2015).

RÍOS ESTAVILLO, Juan. **Derecho e Informática en México, Informática jurídica y Derecho Informático**. 1ª ed. D.F, México: Ed. Instituto de Investigaciónes Juridicas, 1997

SOLANO BÁRCENAS, Orlando. **Manual de informatica juridica**. Santa fe de Bogota, Colombia: Ed. juridicas gustavo ibañez Ltda, 1997

TÉLLEZ VALDÉS, Julio. **Derecho Informático**. 4ª ed. D.F, México: Ed. McGRAW-HILL/ Internacional editores, S.A, (s.f)



Legislación:

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, Guatemala, 1986.

Código Penal, Decreto 17-73 del Congreso de la República, 1973.

Ley de Derechos de Autor y Derechos Conexos, Decreto 33-98 del congreso de la República, 1998.

Ley para el Reconocimiento de las comunicaciones y firmas electrónicas, Decreto 47-2008 del congreso de la República, 2008.

Iniciativa de ley Número 4055 del congreso de la República, 2010.

Convenio sobre la ciberdelincuencia o Convenio de Budapest, 2001.

Código Penal de la Nación Argentina, Ley 11.179, 1984.

Código Penal Colombiano, Ley 599, 2000.

Ley 19223, Tipifica figuras penales relativas a la informática, Congreso Nacional de Chile, 1993.