

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



**PROPUESTA DE ESTRUCTURACIÓN DE LAS PRINCIPALES CONDUCTAS  
DELICTIVAS DERIVADAS DEL USO INADECUADO DE LAS PLATAFORMAS  
DIGITALES DE VIDEO JUEGOS**

**JAIRO ISAÍ CURACÁN PASTOR**

**GUATEMALA, NOVIEMBRE DE 2021**

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

**PROPUESTA DE ESTRUCTURACIÓN DE LAS PRINCIPALES CONDUCTAS  
DELICTIVAS DERIVADAS DEL USO INADECUADO DE LAS PLATAFORMAS  
DIGITALES DE VIDEO JUEGOS**



**TESIS**  
Presentada a la Honorable Junta Directiva  
de la  
Facultad de Ciencias Jurídicas y Sociales  
de la  
Universidad de San Carlos de Guatemala

Por  
**JAIRO ISAÍ CURACÁN PASTOR**

Previo a conferírsele el grado académico de

**LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES**

Y los títulos profesionales de

**ABOGADO Y NOTARIO**

**Guatemala, noviembre de 2021**

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

**DECANO:** M.Sc. Henry Manuel Arriaga Contreras

**VOCAL I:** Licda. Astrid Jeannette Lemus Rodríguez

**VOCAL III:** Lic. Helmer Rolando Reyes García

**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. William Armando Vanegas

**Vocal:** Licda. Irma Haydee Godoy Alejandro

**Secretario:** Lic. José Luis Martínez Zúñiga

**Segunda Fase:**

**Presidente:** Licda. Aida Leonor Paz de González

**Vocal:** Licda. Carmelita Ramos Castañeda

**Secretaria:** Licda. Amalia Azucena García Ramírez

**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)".



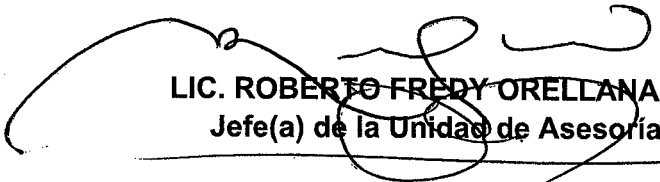
Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala,  
 24 de enero de 2020.

Atentamente pase al (a) Profesional, EDSON WALDEMAR BAUTISTA BRAVO  
 \_\_\_\_\_, para que proceda a asesorar el trabajo de tesis del (a) estudiante  
JAIRO ISAÍ CURACÁN PASTOR, con carné 201112433,  
 intitulado PROPUESTA DE ESTRUCTURACIÓN DE LAS PRINCIPALES CONDUCTAS DELICTIVAS DERIVADAS  
DEL USO INADECUADO DE LAS PLATAFORMAS DIGITALES DE VIDEO JUEGOS.

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.

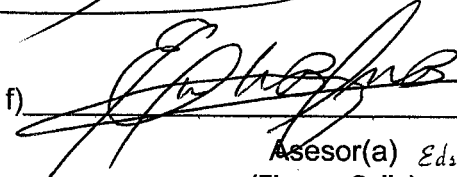
El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros 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.

  
**LIC. ROBERTO FREDY ORELLANA MARTÍNEZ**  
 Jefe(a) de la Unidad de Asesoría de Tesis



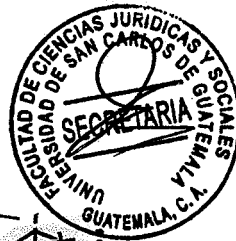
Fecha de recepción 16 / 03 / 2021.

f)   
 Licenciado  
 Asesor(a) Edson Waldemar Bautista Bravo  
 (Firma y Sello) Abogado y Notario



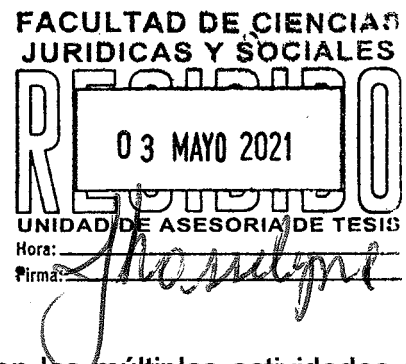


*Bufete Profesional Bautista & Asociados*  
11a. Avenida 13-54, 2o. Nivel, Zona 1.  
Guatemala, C.A. Tel. 5686 2043



Guatemala, 5 de abril del 2,021.

Licda. Astrid Jeannette Lemus Rodríguez  
Jefa de la Unidad de Asesoría de Tesis  
Facultad de Ciencias Jurídicas y Sociales  
Universidad de San Carlos de Guatemala



Respetuosamente se le saluda, augurándole éxitos en las múltiples actividades que realiza en beneficio de nuestra apreciada Alma Mater, así como, en las propias.

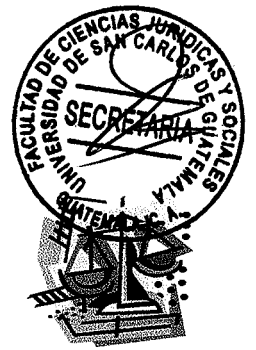
En virtud del nombramiento recaído en su servidor, por este medio me permito emitir **DICTAMEN** en calidad de asesor del trabajo de tesis intitulado: **“PROPUESTA DE ESTRUCTURACIÓN DE LAS PRINCIPALES CONDUCTAS DELICTIVAS DERIVADAS DEL USO INADECUADO DE LAS PLATAFORMAS DIGITALES DE VIDEO JUEGOS”**. Dicho trabajo de tesis ha sido desarrollado por el estudiante **JAIRO ISAÍ CURACÁN PASTOR**, y para el efecto realizo las siguientes consideraciones:

a) El contenido del desarrollo de la tesis referida, es de naturaleza científica-técnica, pues se parte que, es científica, ya que los subtemas abordados se han llevado a cabo después de la amplia consulta bibliográfica sobre el tema mencionado, y se dice que, es técnica, en virtud que, el Código Penal de Guatemala es el que debe de regular los ilícitos penales por el uso inadecuado de las plataformas digitales de video juegos.

b) Aunado a lo anterior, se afirma que en el desarrollo del tema objeto de estudio se aplicaron idóneamente los diferentes métodos y técnicas, en el sentido que a partir de ideas generales se fueron arribando a ideas particulares.



*Bufete Profesional Bautista & Asociados*  
Calz. Roosevelt 10-65, Z. 11, 4to. Nivel. Of. 15.  
Edif. Comerciales Roosevelt.  
Guatemala, C.A. Tel. 5686 2043



c) Los distintos capítulos de la tesis cuyo nombre ha sido descrito, se encuentran redactados de tal manera que, existe congruencia y orden en la expresión de las ideas, esto para una mejor comprensión a la hora que se lea o consulte la presente monografía, por ende, se aclara que, en esta tesis no se presentan cuadros estadísticos.

d) Considero que la conclusión discursiva derivada del presente trabajo de investigación demuestra la necesidad de regular en el Código Penal de Guatemala los ilícitos penales que se comenten por medio de las plataformas digitales de video juegos, o bien, Guatemala se adhiera al Convenio sobre Cibercriminalidad.

e) En relación a la bibliografía consultada para el presente trabajo, se estima que es suficiente y adecuada para su realización.

En virtud del enfoque abordado, con las facultades establecidas en el Artículo 26 de la Normativa aplicable, y con la anuencia del estudiante el nombre correcto de la tesis es: **“PROPUESTA DE ESTRUCTURACIÓN DE LAS PRINCIPALES CONDUCTAS DELICTIVAS DERIVADAS DEL USO INADECUADO DE LAS PLATAFORMAS DIGITALES DE VIDEO JUEGOS”.**

Finalmente, me permito indicar que, con el estudiante JAIRO ISAÍ CURACÁN PASTOR no me une ningún lazo consanguíneo ni de afinidad dentro de los grados que la ley determina.

Por lo anterior, y en base al Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura de Ciencias Jurídicas y Sociales y del Examen General Público, estimo que el presente trabajo de investigación reúne los requisitos para que sea sometido al examen general público de tesis; deferentemente;

  
Licenciado  
Lic. Edson Waldemar Bautista Bravo  
Abogado y Notario

Colegiado Activo No. 7,613.

Magister Scientiae en Derecho Civil y Procesal Civil



**USAC**  
**TRICENTENARIA**  
 Universidad de San Carlos de Guatemala

Reposición por: corrección de datos  
 Fecha emitida: septiembre 2021



**Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 03 de mayo de 2021.**

Atentamente pase a Consejero de Comisión de Estilo, GLADYS MARILU ORELLANA LOPEZ, para que proceda a revisar el trabajo de tesis del (a) estudiante JAIRO ISAÍ CURACÁN PASTOR, con carné número 201112433, intitulado PROPUESTA DE ESTRUCTURACIÓN DE LAS PRINCIPALES CONDUCTAS DELICTIVAS DERIVADAS DEL USO INADECUADO DE LAS PLATAFORMAS DIGITALES DE VIDEO JUEGOS. Luego de que el estudiante subsane las correcciones, si las hubiere, deberá emitirse el dictamen favorable de comisión de Estilo, conforme lo establece el artículo 32 del Normativo para la Elaboración de Tesis de la Licenciatura de Ciencia Jurídica y Sociales y del Examen General Público.

**"ID Y ENSEÑ A TODOS"**



**Dr. Carlos Ebertito Herrera Recinos**  
**Jefe(a) de la Unidad de Asesoría de Tesis**





Guatemala 24 de agosto del 2021.

Doctor  
Carlos Ebertito Herrera Recinos  
Jefe 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**  
24 AGO. 2021  
UNIDAD DE ASESORIA DE TESIS  
Hora:  
Firma: *Jamasud*

Estimado Doctor Herrera:

De manera atenta le informo que fui consejera de redacción y estilo de la tesis titulada: **PROPUESTA DE ESTRUCTURACIÓN DE LAS PRINCIPALES CONDUCTAS DELICTIVAS DERIVADAS DEL USO INADECUADO DE LAS PLATAFORMAS DIGITALES DE VIDEO JUEGOS**, realizada por el bachiller: **JAIRO ISAÏ CURACÀN PASTOR**, para obtener el grado académico de Licenciado en Ciencias Jurídicas y Sociales y los títulos profesionales de Abogado y Notario.

El alumno cumplió con todas las observaciones que le hiciera, por lo que dictamino de manera **FAVORABLE**, por lo que el trámite de orden de impresión puede continuar.

**ID Y ENSEÑAD A TODOS**  
*[Handwritten Signature]*  
Licda. Gladys Marilú Orellana López  
**CONSEJERO DOCENTE DE REDACCIÓN Y ESTILO**  
GLADYS MARILÚ ORELLANA LOPEZ  
ABOGADA  
Y  
NOTARIA

/gmol  
c.c. alumno  
Secretaria  
archivo





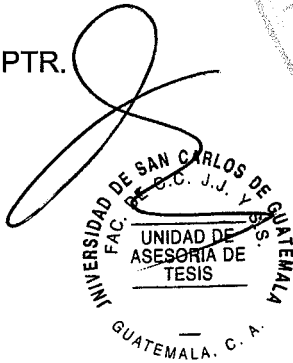
**USAC**  
**TRICENTENARIA**  
 Universidad de San Carlos de Guatemala

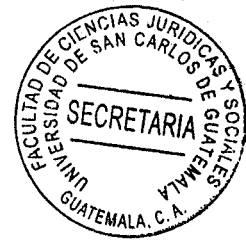


Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala. Ciudad de Guatemala, veintiocho de septiembre de dos mil veintiuno.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante JAIRO ISAÍ CURACÁN PASTOR, titulado PROPUESTA DE ESTRUCTURACIÓN DE LAS PRINCIPALES CONDUCTAS DELICTIVAS DERIVADAS DEL USO INADECUADO DE LAS PLATAFORMAS DIGITALES DE VIDEO JUEGOS. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

CEHR/JPTR.





## DEDICATORIA

- A DIOS:** A ti sea la gloria y honra porque tus promesas son siempre fieles.
- A MI PADRE:** Diego Curacán Salam, por confiar en mí y brindar todo su amor, paciencia y apoyo incondicional.
- A MI MADRE:** Herlinda Pastor Hernández, por todos sus cuidados y atenciones que me brindo durante mi formación profesional.
- A MI ESPOSA:** Anaisa Carrillo, por ser inspiración para ser mejor como persona y profesional del Derecho.
- A MIS HERMANOS:** Por sus constantes palabras de aliento.
- A MIS AMIGOS:** Por todos los momentos vividos y el apoyo brindado durante nuestra época de estudiantes
- A:** La Tricentenaria Universidad de San Carlos, por abrir sus puertas y ayudar a construir mis sueños como profesional.
- A:** La Facultad de Ciencias Jurídicas y Sociales, gracias por arroparme en sus salones y hacer de mí un profesional del derecho consciente de alcanzar el bien común de las personas.



## PRESENTACIÓN

La investigación inicia con el estudio de las características generales a las particulares y de manera puntual se utilizará ayuda de documentación, estadísticas y entrevistas a fiscales del Ministerio Público, con la finalidad de garantizar una correcta interpretación de los delitos informáticos. El estudio de este tema es meramente cualitativo.

Esta investigación pertenece al área cognitiva del derecho denominada derecho penal, debido a que se encarga del estudio de los delitos, penas y procedimientos para resolución de conflictos y ejecución de las penas. Además, el estudio se realizó durante el tiempo comprendido entre los meses de agosto a diciembre de 2019, y enero a octubre de 2020. La investigación se realizó dentro la red de internet del territorio guatemalteco por ser el ámbito de aplicación de la ley penal guatemalteca, siendo el objeto de estudio delitos informáticos que no se encuentran regulados en el derecho penal guatemalteco y el sujeto de estudio aquellas personas que se dedican a delinquir en las plataformas digitales de video juegos.

Como objetivo general se estableció al identificar que conductas ilícitas penales son las más comunes a realizar en las plataformas digitales de vídeo juegos por las personas denominadas delincuentes informáticos establecidos en la República de Guatemala y evitar la impunidad de estas conductas delictivas. El aporte académico de esta investigación es dejar evidencia de las características comunes de los delitos informáticos cometidos en las plataformas digitales de vídeo juegos comparadas con los delitos informáticos tipificados en el Código Penal guatemalteco.



## HIPÓTESIS

En Guatemala, como la mayor parte de los países del mundo, que forman parte del mundo globalizado del medio de comunicación internet, es susceptible de experimentar conductas delictivas cibernéticas tales como: el acceso ilícito, daño informático, reproducción de dispositivos de acceso, violación a la disponibilidad, fraude informático, falsificación informática, interceptación ilícita y delito de spam; esto a causa de que los ciber criminales buscan obtener información personal de los usuarios y beneficiarse de manera económica teniendo como consecuencia un enriquecimiento ilícito e inclusive tener ventajas de sus víctimas al momento de cometer uno o varios delitos.

Es la intención del sustentante de tesis hacer un trabajo que identifique y describa todos los aspectos comunes o la mayor parte posible de ellos, que caractericen a un delito informático desde el punto de vista del autor. A la vez es el objetivo comparar las figuras de lo encontrado como aquellas figuras que se han intentado tipificar en la legislación guatemalteca. De lo anterior, se pretende elaborar en este trabajo de tesis una propuesta de proyecto de ley, que contenga la regulación que el sustentante estime necesaria en las condiciones actuales de este fenómeno casi incontrolable en Guatemala.

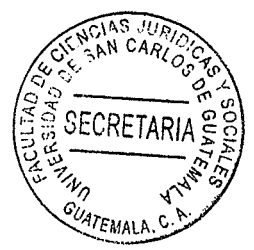


## COMPROBACIÓN DE LA HIPÓTESIS

En Guatemala como la mayor parte de países del mundo que ha sido alcanzado por medios de comunicación como lo es internet, experimenta conductas delictivas cibernéticas, que en la gran mayoría de casos no son constitutivas de delitos por falta de control legal de los delitos cibernéticos.

La comisión de delitos a través de plataformas digitales de video juegos suele realizarse por los ciber delincuentes debido a que desean obtener beneficios económicos. Para ello hacen uso de sus conocimientos y habilidades en informática accediendo a la información personal de los usuarios obteniendo ventajas sobre sus víctimas al momento de cometer el delito que transgrede la integridad, disponibilidad, confidencialidad y patrimonio de las personas. Sin embargo, para ponerle fin a esta problemática es necesaria la implementación de una reforma al Código Penal, Decreto 17-73 del Congreso de la República de Guatemala; o bien, crear una norma especial en materia de delitos informáticos o la incorporación de la Convención sobre Cibercriminalidad al sistema legal de Guatemala.

De esta forma se comprueba que en la actualidad la legislación guatemalteca es insuficiente y desactualizada para controlar los delitos informáticos cometidos en plataformas digitales de vídeo juegos. Por tanto, la hipótesis planteada se comprobó y con fundamentos estables, ya que, la misma sienta sus bases en la realidad de este campo en donde se desarrolla esta problemática, haciendo así de utilidad las posibles soluciones anteriormente planteadas.



# ÍNDICE

**Pág.**

Introducción.....	i
-------------------	---

## CAPÍTULO I

1. Derecho penal.....	1
1.1. Antecedentes .....	2
1.2. Definiciones.....	9
1.3. Características .....	11
1.4. La Ley Penal .....	15
1.4.1. Características .....	15
1.4.2. Formas .....	18
1.4.3. Especies .....	19

## CAPÍTULO II

2. Delitos Informáticos .....	21
2.1. Definición.....	22
2.2. Características .....	23
2.3. Clasificación de los delitos informáticos .....	26
2.3.1. Según el instrumento medio.....	26
2.3.2. Atendiendo al bien jurídico .....	288
2.4. Sujetos .....	30
2.4.1. Sujeto activo.....	30
2.4.2. Sujeto pasivo.....	311
2.5. Características del ciberdelincuente.....	322



### CAPÍTULO III

3. Derecho comparado.....	35
3.1. Soluciones planteadas en otros países.....	38
3.1.1. Alemania.....	39
3.1.2. Argentina.....	41
3.1.3. España.....	44
3.1.4. Estados Unidos.....	45
3.1.5. México.....	47
3.2. Convención sobre la cibercriminalidad de la Unión Europea.....	48
3.3. Organización de los Estados Americanos.....	50
3.4. Situación de los delitos informáticos en Guatemala.....	52

### CAPÍTULO IV

4. Propuesta de estructuración de las principales conductas delictivas derivadas del uso inadecuado de las plataformas digitales de video juegos ...	55
4.1. Bienes jurídicos tutelados.....	59
4.2. Principales métodos utilizados por los ciber delincuentes para la comisión de delitos.....	68
4.3. Propuesta de regulación de los delitos informáticos para su prevención en Guatemala.....	72
4.3.1. Incorporación de los delitos informáticos al Código Penal, Decreto 17-73 del Congreso de la República de Guatemala mediante reformas.....	75
4.3.2. Ratificación del Convenio sobre Ciberdelincuencia.....	79
4.3.3. Creación de un cuerpo normativo especial en materia de delitos Informáticos.....	80
CONCLUSIÓN DISCURSIVA.....	85
BIBLIOGRAFÍA.....	87



## INTRODUCCIÓN

Las redes de telecomunicaciones como internet han neutralizado a la mayor parte de los países del mundo constituyendo una globalización sin fronteras de la cual Guatemala ya es parte. Con la evolución de las sociedades se ha demostrado que siempre habrá personas que evadan las normas de convivencia social. Siendo el caso del uso de la tecnología de internet donde es sumamente complicado para los países del mundo tipificar y castigar los delitos que se cometen en territorio nacional como internacional.

Este trabajo se justifica ya que, en Guatemala, así como en otros países del mundo, experimenta conductas delictivas cibernéticas que en la gran mayoría de casos quedan impunes por no contar con una norma jurídica adecuada a la era digital en la que nos encontramos.

Desde el punto de vista del autor la razón de esta investigación es dejar evidencia, identificación y descripción de todos los aspectos comunes que caractericen a un delito informático cometidos en las plataformas digitales de vídeo juegos; asimismo, comparar las figuras delictivas vigentes en el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala; así como, las figuras que se han tratado de tipificar en la legislación guatemalteca referida.

Este trabajo se realizó obteniendo información en entidades estatales como la Corte Suprema de Justicia, el Ministerio Público, la Policía Nacional Civil y el Ministerio de Gobernación, con la finalidad de indagar antecedentes de denuncias que han existido en contra de las plataformas digitales de vídeo juegos sin dejar por un lado la técnica bibliográfica y distintas doctrinas que sustentan y enriquecen la investigación.

Cabe mencionar que, es importante el derecho comparado, ya que, la investigación se sitúa en los elementos comunes a los delitos posibles de cometerse en plataformas digitales de video juegos y que en Guatemala es difícil de prever, debido a que no cuenta con un control legal estricto, por ello se toma como base las legislaciones de





otros países para tenerlos en cuenta en una posible inclusión al derecho penal guatemalteco.

Este trabajo contiene cuatro capítulos: En el capítulo primero, se abordan los aspectos generales sobre el derecho penal; en el segundo, se desarrolla lo relacionado a los delitos informáticos en general; en el tercero, se realiza un estudio de derecho comparado para determinar cómo otros países han dado solución a esta problemática; y en el capítulo cuarto, se aborda el tema principal de esta tesis, el cual se refiere a la propuesta de estructuración de las principales conductas delictivas derivadas del uso inadecuado de las plataformas digitales de vídeo juegos.

Como objetivo general de la investigación está el identificar aquellas conductas ilícitas penales más comunes a realizar en las plataformas digitales de vídeo juegos por las personas denominadas delincuentes informáticos, con el fin de sentar un precedente para que los delitos informáticos en general sean incluidos dentro de la legislación guatemalteca. De lo anterior, se establece que el objetivo de este trabajo se alcanzó, porque se logran identificar las principales conductas delictivas que se realizan dentro de las plataformas digitales de vídeo juegos y se demuestra la necesidad de regular los ilícitos penales que se plantean en este trabajo.

Los métodos utilizados dentro de este trabajo fueron: el inductivo, deductivo y analítico; mientras que la técnica utilizada fue la investigación documental y bibliográfica.

Por último, se recomienda realizar más estudios sobre el derecho informático, ya que, por ser una nueva área del derecho, resulta difícil la recopilación de información sobre este tema; esto con el fin de poder asentar mejores bases científicas al momento de crear una norma jurídica que tipifique todos los aspectos cotidianos por la utilización de las nuevas tecnologías.



## CAPÍTULO I

### 1. Derecho penal

Es evidente que con el pasar del tiempo la sociedad humana ha inventado y descubierto herramientas que facilitan la realización de sus labores físicas e intelectuales. Es por ello, que, a raíz del descubrimiento de la red de telecomunicación más grande del mundo, que es internet, las personas han adquirido nuevas formas de evadir la justicia, innovando sus formas de delinquir; esto debido a que por medio de internet, tanto en Guatemala y en otros países, se creó un mundo globalizado sin fronteras, haciendo casi imposible tipificar y castigar los delitos realizados a través de la red de internet y que se cometen tanto en ámbitos nacionales como internacionales.

Derivado de lo anterior se hace necesario el estudio del área del derecho penal para indagar sobre las generalidades doctrinarias y legales y así obtener el conocimiento necesario para comprender la falta de tipificación de los delitos informáticos en el ordenamiento jurídico guatemalteco.

A continuación, se describe lo relacionado a los aspectos básicos del área del derecho penal.

## 1.1. Antecedentes

Para comprender la función que cumple el derecho penal en nuestros tiempos, es necesario hacer el análisis de las diferentes etapas históricas que esta área del derecho ha atravesado.

Para algunos autores como Irma Amuchalegui Requena “El surgimiento del derecho penal obedece a las necesidades de regular el comportamiento del hombre en sociedad. El crimen nace con el hombre, cuando también no existe un ordenamiento jurídico, ni una sociedad organizada, ya que el delito se manifiesta en su más rudimentaria forma al inferirle daños ajenos. El hombre no articulaba aún palabras, pero ya desarrollaba conductas que afectan a otros, por ejemplo, el apoderamiento del animal cazado por otro, las violaciones físicas sobre una mujer ... De ahí la necesidad de regular tales conductas y señalar castigos para lograr el orden y la convivencia pacífica”.<sup>1</sup>

El derecho penal surge como respuesta a los constantes abusos de los derechos de las personas en convivencia social y a lo largo de la historia ha ido desarrollando diferentes formas de castigar a través del *ius puniendi* del Estado imponiendo el respeto debido a los derechos de los individuos. Sin embargo, para que esto sucediera el derecho penal atravesó diferentes etapas y para su estudio diferentes autores como Luis Jiménez de Asua, José Francisco de Mata Vela y Héctor Aníbal de León Velasco lo han planteado de la siguiente manera:

---

<sup>1</sup> Amuchalegui Requena, Irma Gabriela. **derecho penal**. Pág. 4.

a) Época de la venganza privada

Se origina durante el asentamiento de las primeras civilizaciones humanas, cuando el poder punitivo del Estado no poseía la fuerza necesaria para imponerse a los particulares, el derecho penal funcionaba en el sentido de venganza; la venganza de los particulares a lo largo de la historia se ha tomado como el inicio del castigo penal, no debe de confundirse con un sistema penal en sí, sino una forma de resarcimiento individual.

La época de la venganza privada es la etapa histórica del derecho penal donde se actúa por defensa propia ante la provocación de un agravio injustificado de la persona y debido a que la sociedad no contaba con una organización jurídica al violarse el derecho de los individuos, por ello éstos hacían justicia por su propia cuenta.

Derivado de ello se produjo una serie de guerras sangrientas entre familias y al momento de cobrar venganza por los males causados se produjo la extinción de familias completas, causando al ofensor y su familia todo el mal posible, para evitar las violentas e ilimitadas reacciones se hizo uso de la ley de talión, la cual limitaba a devolver un mal de igual magnitud al mal causado; de tal forma en el derecho penal moderno la ley de talión equivale a la pena que castiga los diferentes delitos y se diferencia de la venganza ya que esta contaba con el respaldo del colectivo social, mediante ayuda y el respaldo moral hacia el agredido dando vía libre para que el ofendido hiciera uso de la venganza.

Otro aspecto importante del uso de la ley de talión es que aparece como una limitante a la venganza privada, esto mediante una retribución o compensación que entregaba el ofensor y su familia al ofendido con el fin de que éste último o los suyos no utilizarán su derecho a vengarse logrando el resarcimiento del daño causado.

b) Época de la venganza divina

Durante esta época se cree en una figura divina o suprema, donde Dios era el único con derecho a juzgar, los jueces impartían justicia en el nombre de Dios, generalmente ejercían este derecho los sacerdotes quienes se consideraban representantes de la voluntad divina, administrando justicia e imponiendo penas para que el delincuente resarciera el daño causado por el delito cometido, pero ante ello se imponían penas excesivas atribuyendo que el ente divino así lo demandaba para expiar los pecados cometidos.

c) Época de la venganza pública

Es el Estado quien tiene el poder de ejercer justicia social derivado de la realización de un delito. Los castigos de delitos y faltas aplicados por el poder público se representan por el Estado ejerciendo la venganza en nombre de la sociedad y de los bienes jurídicos tutelados que se vulneran o han puesto en riesgo. El castigo penal se convirtió en una de las armas para mantener la tranquilidad de la población, optando por la forma de una venganza pública, donde los castigos eran severos y excesivos siendo su



principal característica la aplicación de las penas inhumanas sin sentido de justicia y de manera desproporcionada con relación al mal que se causaba.

Durante esta época en el derecho penal existió una gran desproporción al momento de administrar justicia imponiendo sanciones leves a los nobles y poderosos en favor de sus intereses, mientras a los plebeyos y los siervos se castigaban de forma severa y dura y su protección era solo una cortina de humo de la justicia. Por último, las sentencias emitidas por los órganos jurisdiccionales eran arbitrarias llegando al límite de imponer penas que la ley no contemplaba, incluso se tipificaban hechos no penados como delitos.

d) Período humanitario

Esta etapa del derecho penal comienza a finales del siglo XVIII con la corriente intelectual del iluminismo aceptando como precursor a César Bonnesana, conocido también como, el Marqués de Beccaria quien a raíz de su obra denominada "De los delitos y de las penas" expresaba que el fin de las penas no era torturar y mortificar a los condenados, ni deshacer un delito cometido; sino impedir que el delincuente cause nuevos daños a la sociedad y advertir a los demás para que se abstengan de la comisión de nuevos delitos; posterior a ello se deberán optar por las penas y el método para imponerlas con el fin de que el delincuente no recaiga en la comisión de nuevos o iguales delitos y sea menos dolorosa la pena sobre el cuerpo del reo.



Es por ello que el Marqués de Beccaria es catalogado como el máximo exponente de esta etapa del derecho penal, y que muchos especialistas han denominado la edad de oro del Derecho Penal.

e) Etapa científica

Con los aportes otorgados por César Bonnessana da inicio al estudio científico del derecho penal. Esta etapa estuvo influenciada por distintas corrientes filosóficas acerca de la forma y objeto de estudio del derecho penal. Muchos autores como Palacios Motta considera como primer escalón de la etapa científica a la escuela clásica, en la cual se veía al derecho penal como una disciplina única, general e independiente, siendo su objeto de estudio el delito y la pena o sanción desde la perspectiva legal.

Posterior a la escuela clásica surge la escuela positivista del derecho penal, cuyas ideas son totalmente contrarias a la escuela clásica. El precursor de esta corriente es Enrico Ferri; quien consideraba que el derecho penal no se debía de tomar en cuenta como ciencia autónoma, ya que a su consideración el derecho penal debía estudiarse auxiliado de un método positivista o experimental. Durante esta etapa se estudia las causas de la delincuencia, resaltando los cambios en los factores individuales, manifestaciones físicas, sociales y culturales que dan origen a la criminalidad; de esta forma el delito deja de ser considerado como una forma jurídica y se estudia como una manifestación de la voluntad del delincuente; la pena es abordada como medio para



corregir al delincuente y de esa manera obtener la defensa de la sociedad, en consecuencia, la pena pierde su carácter retributivo o castigo por la comisión de delitos.

Por último, surge el derecho penal autoritario; derivado de la aparición de corrientes políticas totalitarias, siendo su característica fundamental que el derecho penal se encuentra a favor del Estado, por lo que cuando un funcionario público cometía un delito obtenía un trato benévolo a tal grado que sus conductas delictivas eran encuadradas como infracciones, pero con el pasar del tiempo se fue denotando la gravedad de la situación y pasaron de ser simples infracciones a infracciones de especial gravedad y castigados de forma severa.”<sup>2</sup>

#### f) Época moderna

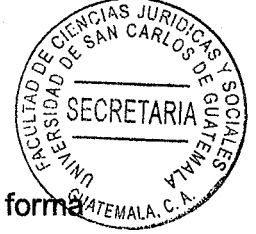
En la actualidad los estudiosos del derecho han concordado en toda la doctrina de separar a la ciencia del derecho penal de las ciencias penales o criminológicas; la ciencia del derecho penal es visto desde una perspectiva eminentemente jurídica para estudiar la problemática que concierne al delito, el delincuente, la pena y medidas de seguridad; por otra parte las ciencias criminológicas, aunque su objeto de estudio es el mismo, debe de hacer su enfoque desde un punto de vista antropológico y sociológico.

Sin embargo, algunos han llegado a considerar al derecho penal como una dogmática jurídica, en la cual se realiza la reconstrucción del derecho penal positivo con base científica sin que sea influenciado por corrientes filosóficas y críticas, afianzándose

---

<sup>2</sup> Jiménez de Asúa, Luis, **Lecciones del derecho penal**. Pág. 20





sobre el derecho existente y evolucionando en la medida que se adapta de forma progresiva a las conductas y tendencias sociales y culturales y tecnológicos.

Derivado de lo anterior, podemos notar que los avances tecnológicos han posibilitado la interacción de las personas a través de Internet. Como consecuencia, en Guatemala y en otros países del mundo, se experimentan conductas delictivas cibernéticas que en la gran mayoría de casos muchas personas evaden el control legal de su accionar.

Actualmente, en Guatemala no se cuenta con normas jurídicas que identifiquen y describan aspectos que caractericen a un delito informático, pues únicamente se cuenta con los Artículos 274 "A" al 274 "H" del Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, que tipifican asuntos relativos a la información que se encuentra contenida en equipos de cómputo, más no tipifica las conductas antijurídicas que se pueden derivar del mal uso de las plataformas digitales que se encuentran en internet. Asimismo, nuestro ordenamiento jurídico no incluye ninguna ley de carácter especial para prevenir y castigar determinadas conductas que se efectúan por conducto de sistemas tecnológicos de informática y que transgreden de manera inminente el patrimonio, la información y el honor de las personas, entre otros bienes jurídicos tutelados.

Sin embargo, se ha presentado ante el Congreso de la República de Guatemala la propuesta de ley número cuatro mil cincuenta y cinco (4055), la cual contiene el proyecto de ley de delitos informáticos, la cual obtuvo dictamen favorable por parte de



la Comisión de Puntos Constitucionales y Comisión de Legislación del Congreso de la República de Guatemala y a pesar de que fue remitida al pleno del Congreso de la República de Guatemala para el trámite legal de discusión, la misma no ha seguido con su trámite correspondiente, previo a su sanción y promulgación, desde mayo de 2009 hasta la fecha de la realización de este estudio.

## 1.2. Definiciones

El estudio de esta ciencia puede ser enfocado desde el punto de vista subjetivo y desde el punto de vista objetivo. El primero, también llamado *Jus Puniendi*, es un punto de vista filosófico del derecho penal y señala que es la facultad del Estado en determinar delitos, tipificar, imponer y ejecutar las penas y sanciones correspondientes o determinar las medidas de seguridad en casos determinados.

Por otra parte, el derecho penal desde el punto de vista objetivo; también llamado *Jus Poenale*, define al derecho penal como un conjunto de normas capaz de regular la actividad castigadora del Estado, haciendo uso de su capacidad legislativa para tipificar los delitos, penas y medidas de seguridad, actuando bajo el principio de legalidad que limita el derecho punitivo del Estado.

Guillermo Cabanellas se expresa respecto a la definición de derecho penal de la manera siguiente: "El derecho penal también suele ser denominado derecho criminal, utilizando la designación primera, se refiere más exactamente a la potestad de penar;



mientras el derecho del crimen no es reconocible, aunque adjetivamente se expresa en la verdad derecho sobre el crimen, como infracción o conducta punible. Comprende los principios doctrinales y las normas positivas referentes al delito, al delincuente y la pena.

El derecho penal es el conjunto de reglas establecidas por el Estado con el fin de unir al hecho del delito y la pena, como su consecuencia jurídica.

El conjunto de aquellas condiciones para el derecho, donde se han perturbado los actos de una voluntad opuesta a él, sea restablecido y restaurado en todas las esferas y puntos donde la violación llegó. Es la ciencia que estudia el delito como fenómeno jurídico y al delincuente como sujeto activo y por tanto, las relaciones que derivan del delito como violación del orden jurídico y de la pena como reintegración de ese orden.”<sup>3</sup>

De lo anterior, podemos establecer que el derecho penal, como ciencia, está conformado de dos partes: La parte general del derecho penal, que atiende a los principios, conceptos, teorías, doctrinas e instituciones referentes al delito, al delincuente, las penas y las medidas de seguridad y que en la legislación guatemalteca se ve inmerso en el Libro Primero del Código Penal, Decreto 17-73 del Congreso de la República de Guatemala; y la parte especial, se encarga del estudio de los delitos y faltas, las penas y medidas de seguridad aplicables a los delincuentes, siendo el caso de Guatemala quien lo regula en el Libro Segundo y Libro Tercero del Código Penal, Decreto 17-73 del Congreso de la República de Guatemala.

---

<sup>3</sup> Cabanellas, Guillermo, **Diccionario enciclopédico de derecho usual**. Pág. 143.



De lo mencionado, y a lo largo de la historia, hemos visto como el derecho penal evoluciona y se ha convertido en una ciencia social fundamental que trata de castigar los hechos delictivos cometidos por seres humanos que transgreden y violan los derechos fundamentales con el fin de causar un daño a las demás personas, es por ello, que para definir al derecho penal no basta con decir que es una disciplina del derecho que trata de castigar los delitos cometidos por los hombres; sino que a consideración el derecho penal se puede definir de la manera siguiente: Es la conducta del hombre, encuadrada en una norma jurídica emitida por el órgano legislador del Estado que determinan los delitos y faltas, así como las penas, multas y medidas de seguridad a imponer en caso de transgredir y violentar los derechos fundamentales de las demás personas.

### **1.3. Características**

El Doctor Héctor Aníbal de León Velasco y Doctor José Francisco de Mata Vela en cuanto a las características del derecho penal hacen mención de las siguientes características:

- a) Es una ciencia social y cultural

A raíz de que el método de estudio de las ciencias naturales es experimental, mientras en las ciencias sociales o culturales es racionalista, especulativo o lógico abstracto; en las ciencias naturales la relación entre fenómenos es causal; mientras que en las



ciencias sociales o culturales es teleológica; las ciencias naturales son ciencias del ser, mientras las ciencias sociales o culturales son del deber ser; de tal manera que el derecho penal, es una ciencia social, cultural o del espíritu, debido a que no estudia fenómenos naturales enlazados por la causalidad, sino regula conductas en atención a un fin considerado como valioso; es pues, una ciencia del deber ser y no del ser.

b) Es normativo

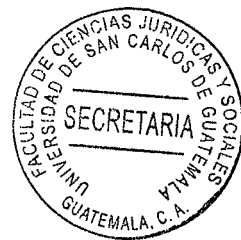
Como toda rama del derecho, está compuesto por normas, que son preceptos que contienen mandatos o prohibiciones encaminadas a regular la conducta humana, es decir, a normar el debe ser de las personas dentro de una sociedad jurídicamente organizada.

c) Es de carácter positivo

Porque es fundamentalmente jurídico, ya que el derecho penal vigente es solamente aquel que el Estado ha promulgado con ese carácter.

d) Pertenece al Derecho Público

Porque, siendo el Estado el único titular del derecho penal, solamente a él corresponde la facultad de establecer delitos y las penas o medidas de seguridad correspondiente.



e) Valorativo

En palabras del profesor argentino Sebastián Soler, esta cualidad de toda norma es particularmente manifiesta en las leyes penales, ya que carecerían de todo sentido las amenazas penales si no se entendiera que mediante ellas son protegidos ciertos bienes e intereses jurídicamente apreciados. Es decir, que el derecho penal está subordinado a una orden valorativa en cuanto que califica los actos humanos con arreglo a una valoración; valorar la conducta de los hombres es tarea fundamental del juez penal. Dicho en palabras del autor de esta tesis, es valorativo ya que todo actuar antijurídico, trae inmersa una sanción de carácter punitivo y es deber del juez calificar, conforme la tipificación que éste realice, e imponga la pena prevista en la normativa penal.

f) Es finalista

Su fin primordial es resguardar el orden jurídicamente establecido, a través de la protección contra el crimen. Sebastián Soler, hace mención de que la ley regula la conducta que los hombres deberán observar con relación a esas realidades, en función de un fin colectivamente perseguido y de una valoración de esos hechos.

g) Es sancionador

El derecho penal se ha caracterizado, como su nombre lo indica, por castigar, reprimir, imponer una pena con carácter retributivo a la comisión de un delito, y así se hablaba



de su naturaleza sancionadora, en el entendido que la pena era la única consecuencia del delito.

h) Es preventivo y rehabilitador

Es decir, que además de sancionar, debe pretender la prevención del delito y la rehabilitación del delincuente por medio del sistema penitenciario o derecho penal penitenciario.

i) Es fragmentario, subsidiario y de intervención mínima

Esto se debe a que el derecho penal es solamente una parte de los medios de control con el que el Estado cuenta en su lucha contra el delito. Es subsidiario porque se debe utilizar únicamente en caso de que los demás medios de control social no hayan servido para neutralizar las conductas antisociales. Por último, es de carácter mínimo ya que solamente puede actuar en los casos en que se hayan definido previamente en la ley penal tales conductas como delitos, en este último caso estamos frente al principio de legalidad.

Sin embargo, habiendo abordado aspectos generales sobre la ciencia del derecho penal, es necesario abordar el tema de la ley penal, tanto en sus características y formas en las que se manifiesta para el estricto cumplimiento del derecho penal.



A consideración del autor las características del derecho penal están íntimamente relacionadas con el área del derecho informático, debido a que sin estas características no se podrán tipificar las conductas delictivas que se derivan del uso malicioso de la tecnología.

#### **1.4. La ley penal**

El profesor Puig Peña conceptualiza a la ley penal como aquella disposición que por virtud de la cual el Estado crea derecho con carácter de generalidad, estableciendo las penas correspondientes a los delitos que en ella se tipifican. Por otra parte, Palacios Motta explica a la ley penal como el conjunto de normas jurídicas que definen los delitos y las faltas, determinan las responsabilidades o las exenciones y establecen las penas o medidas de seguridad, que corresponden a las figuras delictivas.

##### **1.4.1. Características**

Dentro de las características de la ley penal se pueden mencionar las siguientes:

###### **a) Generalidad**

Se refiere a que la ley penal se dirige a todas las personas, sean naturales o jurídicas, dentro de un Estado, y por tanto es obligación de sus habitantes obedecer.





b) **Obligatoriedad**

La ley penal resulta ser obligatoria, en el sentido de que es de carácter coercitivo, ya que de no cumplirse o transgredirse conlleva una sanción pecuniaria o de prisión.

c) **Igualdad**

Esta característica radica en el cumplimiento estricto de la ley penal por todos los individuos dentro del territorio de la República de Guatemala, sin excepción alguna, evitando la discriminación de raza, color, sexo, religión, nacimiento, posición social, política o económica.

d) **Exclusividad**

Hace referencia a que sólo el Estado a través de su órgano legislativo, crea la ley penal, y en consecuencia establece los delitos, penas y medidas de seguridad para los mismos.

e) **Permanencia**

Consiste en que la ley penal perdura en el tiempo y espacio de su aplicabilidad, sin embargo, ésta deja de tener vigencia hasta que otra ley la abrogue o derogue.

f) Ineludibilidad

Se refiere a que la ley penal no se puede eludir por los habitantes de un Estado, salvo aquellas excepciones de inmunidad y antejuicio que gozan algunos funcionarios públicos y habitantes que establece la misma ley.

g) Imperatividad

En el sentido de que la ley penal contiene prohibiciones que todo habitante de un país debe cumplir y no deja nada a voluntad de las personas, por consiguiente, ordena hacer y prohíbe hacer, sin tomar en cuenta la disposición de las personas, única y exclusivamente debe acatar la ley, ya que de no hacerlo se le impondrá una pena.

h) Es sancionadora

A diferencia de otras disciplinas del derecho, lo que la distingue de otras disciplinas es su norma penal cuya infracción trae consigo una sanción que bien puede ser una pena o medida de seguridad, ya que de no existir una pena estaríamos frente a una ley penal sin pena y por consiguiente dejaría de ser ley penal.

i) Es constitucional

La ley penal al igual que cualquier otra normativa jurídica debe de tener su fundamento en Constitución Política de la República de Guatemala, debido a que, si ésta contradice



a la Constitución o normas Constitucionales, la ley penal sería una ley inconstitucional y como consecuencia no nace a la vida jurídica ante sus habitantes.

Las características de la ley penal dentro del presente estudio nos brindan un mejor panorama para que las normas sancionadoras del derecho informático sean apegadas al marco jurídico guatemalteco dando como resultado una norma vigente y positiva.

#### **1.4.2. Formas**

Para entender ¿Qué es la forma de la ley penal? Debe comprenderse en el sentido del órgano u organismos que erogan la norma jurídica penal, en ese sentido la ley penal puede ser:

##### **a) Ley penal formal**

Es toda norma jurídica de carácter penal que nace a la vida jurídica derivado de un proceso legislativo el cuál se lleva a cabo por el órgano competente para crear leyes, en Guatemala es el Congreso de la República quien creo el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala.



b) Ley penal material

Esta disposición es emitida por un organismo que no está facultado constitucionalmente para emitir leyes, y se emiten para gobernar durante un gobierno de facto por la falta de un organismo legislativo, por tal razón son catalogados como decretos leyes. Sin embargo, también son llamadas así las leyes que tienen contenido penal, pero se encuentran fuera del Código Penal.

**1.4.3. Especies**

Es todo cuerpo normativo, aparte del Código Penal, cuyo contenido es inevitablemente penal, y por consiguiente se han convertido en especies de ley penal. Por ejemplo: Ley de Armas y Municiones, Ley de Femicidio y Otras Formas de Violencia Contra la Mujer, Ley de Régimen Penitenciario, entre otras.

Es de mencionar que existen tres clases de especies de la ley penal:

a) Leyes penales especiales

Estas normas no se encuentran precisamente en el Código Penal, su finalidad es proteger a un colectivo social en específico, o tutelar bienes jurídicos, esto lo convierte en leyes penales especiales. Por Ejemplo: Ley Contra la Delincuencia Organizada, Ley Contra el Lavado de Dinero y Otros Activos, Ley Contra el Financiamiento del Terrorismo, entre otras.



b) **Convenios Internacionales**

Este tipo de norma se lleva a cabo por el convenio entre distintos países, que contienen normas de tipo jurídico penal, y que a raíz de un proceso legislativo se convierten en obligatorias para los habitantes de un país.

c) **Decretos leyes**

Estas normas jurídicas devienen de un órgano externo al legislativo por la razón de que no se encuentra reunido o no existe el Congreso de la República de Guatemala, en ese sentido, es el Organismo Ejecutivo el encargado de dictar las disposiciones jurídicas con carácter de leyes. Estos Decretos surgen, en la mayoría de las situaciones, en un estado de emergencia o en un gobierno de facto, por ejemplo; el Código Civil Decreto Ley 106, Código Procesal Civil y Mercantil Decreto Ley 107, que nacieron a la vida jurídica para garantizar las actividades cotidianas de las personas en el ámbito familiar, bienes, derechos y obligaciones.



## CAPÍTULO II

### 2. Delitos Informáticos

Durante el Siglo XX y principios del Siglo XXI se han desarrollado grandes avances tecnológicos que permiten compartir información en milésimas de segundo, derivado de ello se ha generado lo que se le denomina revolución digital. Dicha revolución surge como consecuencia de la invención de internet y alcanza su auge gracias a la utilización simultánea de sistemas de cómputo y las distintas interfaces de conexión, es decir, utilizar el ordenador como un medio de comunicación por medio del uso de internet, el cual ha facilitado la interrelación entre las personas.

Sin duda alguna el internet es una herramienta que trajo consigo un sinfín de beneficios, pero cabe decir que utilizarla conlleva sus riesgos, debido a que puede ser usada para realizar daño a una persona individual o personas jurídicas públicas y privadas. Con la aparición del internet han surgido diferentes formas de operar para los delincuentes y con ello nuevos delitos, que eminentemente amenazan la integridad, disponibilidad y confidencialidad de las personas, por consiguiente, nos encontramos frente a los delitos informáticos.



Aunado a lo anterior, podemos evidenciar el riesgo en que se encuentran los diferentes derechos de las personas derivado de las nuevas formas de cometer delitos por medio del internet, y ante la falta de una legislación adecuada en Guatemala pueden devenir nuevas formas de transgredir los derechos de las demás personas y cuyas conductas queden impunes.

Ante la falta de tipificación, se hace necesario establecer la importancia de los nuevos actos delictivos que surgen derivado de la interacción de las personas por el uso de las plataformas digitales de video juegos que utilizan la conexión a internet y que son utilizados para delinquir.

## **2.1. Definición**

En términos generales el delito para muchos autores es toda acción u omisión típica, antijurídica, culpable y punible; resaltando los elementos principales del mismo y que de no concurrir alguna de ellas, el delito dejaría de existir.

“Delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin”<sup>4</sup>

---

<sup>4</sup> Lima Malvido, María de la Luz. **Delitos Electrónicos**. Pág. 100



Luego de haber dado los elementos que conforman el delito debemos tomar en cuenta que para la definición de delito informático el verbo rector ante esta conducta es hacer uso de computadoras, medios electrónicos o análogos, mediante un programa de cómputo que permita cometer ilícitos penales.

Dicho lo anterior, podemos definir al delito informático como toda acción u omisión, típica, antijurídica, culpable y punible, que realiza una persona, haciéndose valer por el uso de computadoras, medios electrónicos o análogos; y que, mediante un programa informático, conectados a través de redes locales o internet, comete ilícitos penales, con el fin de obtener beneficios económicos.

Sin embargo, para comprender la diferencia que existe entre un delito común de un delito informático es necesario, no solo atender a los elementos positivos y negativos que este contiene, sino, observar detenidamente las características que hacen único al delito informático, las cuales se describen en párrafos siguientes.

## **2.2. Características**

“Los delitos informáticos presentan las siguientes características principales:

- a) Son conductas criminales de cuello blanco, ya que solo un número determinado de personas, con cierto conocimiento, en este caso técnico, pueden llegar a cometerlo.





- b) Son acciones ocupacionales, en cuanto a muchas veces se realizan cuando el sujeto se haya trabajando.
- c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- d) Provocan serias pérdidas económicas, ya que casi siempre producen beneficios a aquellos que las realizan.
- e) Ofrece posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- f) Son muchos los casos y pocas las denuncias, debido a la misma falta de regulación por parte del derecho.
- g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- h) Presentan grandes dificultades para su comprobación. Esto por su mismo carácter técnico.



i) Tienden a proliferarse cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley."<sup>5</sup>

Atendiendo a las características mencionadas, y la definición dada en el apartado anterior, es permisible indicar que, los delitos informáticos son cometidos con exclusividad por personas que tienen conocimiento en informática, lo cual les da ventaja sobre sus víctimas, facilitando el acceso a información íntima de las personas individuales y colectivas de índole público o privado; y derivado de la ausencia de una ley que tipifique estos ilícitos, es casi imposible, que las pocas denuncias que ocurren a raíz de estos hechos, no puedan tener el seguimiento respectivo, quedando impunes estas conductas criminógenas.

Es importante señalar, que este tipo de conductas, al quedar impunes, tenderán a expandirse y ser más frecuentes de lo habitual; y a falta de la regulación legal será cada vez más difícil de imponer sanciones con el pasar del tiempo. Por ello, es importante que el Estado de Guatemala genere una normativa que prevea cometer y castigar a aquellas personas que cometen delitos informáticos, tomando en cuenta el conocimiento técnico y legal de expertos en esta materia, ya que de no hacerlo será complejo aplicar las sanciones debidas a las personas que se dedican a delinquir mediante plataformas digitales.

---

<sup>5</sup> Téllez Valdez, Julio. **Delitos Informáticos y El Derecho Penal Informático**. Pág. 67.



Por otra parte, para el Estado de Guatemala es un reto controlar el aumento de flujo de datos a nivel nacional e internacional; por consiguiente, la cantidad de casos en criminalidad informática aumenta a medida que el flujo de datos está en constante crecimiento, es por ello que nuestras autoridades se ven afectadas en su infraestructura limitando al Ministerio Público y al Organismo Judicial a dar seguimiento a los casos de delitos informáticos.

Sin embargo, a simple vista pareciera que al estudiar los delitos informáticos se restringe en su definición a cometer delitos por medio de sistemas de cómputo o sistemas digitales de informática, es por ello, que a continuación se desarrollan las diferentes clasificaciones en que se pueden manifestar los delitos informáticos.

### **2.3. Clasificación de los delitos informáticos**

#### **2.3.1. Según el instrumento medio**

“Esta clasificación de delitos se basa en dos criterios:

##### **a) Instrumento o medio**

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo; falsificación de documentos vía computarizada.



b) Como fin u objetivo

En esta categoría encuadramos a las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física, por ejemplo; programación de instrucciones que producen un bloqueo total del sistema, entre las que destacan:

- a. La destrucción de programas por cualquier método;
- b. El daño de la memoria;
- c. El atentado físico contra la máquina o sus accesorios;
- d. El sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados; y
- e. El secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje.”<sup>6</sup>

Ésta primera clasificación observamos que la tecnología electrónica, de cómputo e informática, es esencial para que concurran los delitos informáticos, atacando ya sea a su sistema físico y lógico de almacenamiento de datos; así como, sus diversas formas de programación mediante instrucciones de bloqueo de sistema, por lo que no se considera un riesgo para la información de las personas.

---

<sup>6</sup> Téllez Valdez, Julio. **Ob. Cit.** Pág. 190

### **2.3.2. Atendiendo al bien jurídico**

En "esta clasificación de delitos informáticos se destaca atendiendo al bien jurídico que específicamente trata de tutelar. En ese sentido su clasificación es la siguiente:

#### **1) Delitos contra la Integridad**

En esta categoría podemos encuadrar:

- a) Daño informático
- b) Falsificación informática
- c) Fraude informático

#### **2) Delitos contra la disponibilidad**

Dentro de esta categoría podemos citar el delito de violación a la disponibilidad

#### **3) Delitos contra la confidencialidad**

- a) Espionaje informático
- b) Acceso ilícito
- c) Reproducción de dispositivos de acceso
- d) Intercepción ilícita

#### 4) Delitos de pornografía infantil

Todas las conductas tipificadas como Pornografía Infantil reguladas en el Código Penal, Decreto 17-73 del Congreso de la República, Ley Contra la Violencia Sexual, Explotación y Trata de Personas y cualquier otro cuerpo normativo están orientadas a su realización por medio de un sistema que utilice tecnología de la información.

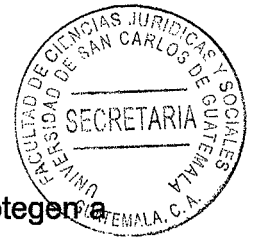
#### 5) Delitos contra la Propiedad Intelectual

Todas aquellas conductas tipificadas como violatorias a los derechos de propiedad intelectual, regulados en la Ley de Propiedad Industrial y Ley de Derechos de Autor y Derechos Conexos, o en cualquier otro cuerpo normativo, siempre y cuando se realicen por medio de un sistema que utilice tecnologías de la información.”<sup>7</sup>

A diferencia de la clasificación anterior vemos como el fin que persigue cada delito es distinto, ya que, en la clasificación según el instrumento medio, las lesiones o daños se dirigen hacia el sistema físico de una computadora o a sus componentes digitales, como sistemas operativos, controladores digitales, programas esenciales de un computador, entre otros que afectan el buen funcionamiento del ordenador.

---

<sup>7</sup> Alvarado, José y Morales, Ronald. **Cibercrimen**. Pág. 17.



Por otra parte, los delitos informáticos que atienden al bien jurídico tutelado protegen a las personas de otras personas que utilizan las tecnologías de informática e información para dañar su integridad, disponibilidad o confidencialidad de información y obtener beneficios económicos.

## **2.4. Sujetos**

Al realizar cualquier tipo de delito siempre encontraremos a la persona que comete el delito y la persona que es víctima del delito; y los delitos informáticos no son la excepción. Sin embargo, hablar de los sujetos en los delitos informáticos, hablamos de cierta clase de personas privilegiadas con conocimientos en sistemas informáticos que los diferencia al resto de delitos tipificados en el Código Penal de Guatemala.

### **2.4.1. Sujeto activo**

En esta categoría, con relación a los delitos informáticos, encontramos a personas que generalmente están dotadas de conocimientos educativos de nivel superior; por consiguiente suelen ser analistas de sistemas, programadores, supervisores, personal técnico y de mantenimiento operativo; es decir, suelen ser aquellas personas que tienen acceso ilimitado y tienen el conocimiento para diseñar seguridad informática, o cuentan con conocimiento de cómo evadir la seguridad de los distintos sistemas operativos e informáticos, así como acceder a bases de datos de forma incalculable para manipular la información de las personas.



#### 2.4.2. Sujeto pasivo

Es también llamado víctima del delito, y es la persona “que sufre cualquier tipo de lesión, mediante el uso de un sistema que utilice tecnologías informáticas.”<sup>8</sup> Es la persona sobre la cual recae el daño causado por la acción u omisión que realiza el sujeto activo, generalmente son las personas que utilizan tecnologías automatizadas de información y que en su mayoría se encuentran conectados por redes de sistemas entre sí.

Para el presente estudio se puede establecer que es el *gamer*, tanto aficionados como a nivel profesional, tomando en cuenta que en la actualidad estas personas utilizan distintas plataformas de videojuegos en internet para poder realizar sus actividades y que en Guatemala, son las personas jóvenes que se encuentran influenciadas por estas tendencias, que en muchos países se considera como una actividad laboral; ya que, prestan sus servicios a grandes marcas para realizar entretenimiento a través de las distintas plataformas de transmisión en directo o *live stream* por internet.

En el transcurso de esta investigación se observan los diferentes rasgos que hacen que los delitos informáticos tengan influencia en nuestro diario vivir. Sin embargo, a pesar que se abordó con anterioridad quien es el sujeto activo y pasivo en la comisión de delitos informáticos, no se han mencionado las características que identifican al sujeto activo en los delitos informáticos, ya que no presentan las mismas características que un delincuente común.

---

<sup>8</sup> *Ibíd.* Págs. 18 y 19.





## 2.5. Características del ciberdelincuente

“Las principales características que presentan los sujetos activos de la conducta delictiva a estudiar son las siguientes:

- a) Poseen antecedentes delictivos.
- b) La mayoría son de sexo masculino.
- c) Son muy individualistas, es decir, que actúan siempre en solitario.
- d) Poseen inteligencia brillante y alta capacidad lógica, con una actitud deportiva que les incita a vulnerar la seguridad de los sistemas, y que suelen ser comunes en aquellas personas denominadas *hackers*.
- e) En su mayoría son personas jóvenes que cuentan con destreza en el manejo de equipo de cómputo e informática, con mucho coraje, temeridad y gran confianza en sí mismos.
- f) Suelen ser personas autodidactas con conocimientos técnicos universitarios, con capacidad de concentración y perseverancia, y por no ser delincuentes típicos, son socialmente aceptados.
- g) Derivado de su espíritu deportivo, aprovechan las falencias en los sistemas de seguridad para encontrar acceso en los diferentes programas de informática; y de encontrarlas, evidencian las deficiencias en las medidas de seguridad que se encuentran vigentes, o en los procesos lógicos de los sistemas.



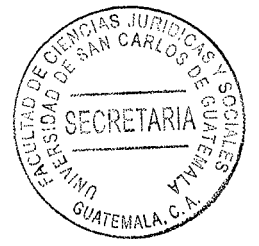
h) Han sido personas que cuentan con gran reconocimiento dentro de las instituciones para las que se encontraban trabajando y se les cataloga de trabajadores motivados y excepcionales en su quehacer.”<sup>9</sup>

Es importante destacar que al referirnos sobre las características del delincuente informático o ciber delincuente, el común denominador de todas ellas es la agilidad, destreza, capacidad de concentración y coeficiente intelectual superior que demuestra el sujeto activo al momento de utilizar los sistemas de cómputo y programas informáticos para obtener un beneficio personal, que en la mayoría de casos suelen ser beneficios económicos.

Sin embargo, a raíz de los problemas y daños que los delincuentes informáticos han ocasionado en algunos Estados, y siendo conscientes que su actuar sobrepasa las fronteras, algunos países han optado por implementar medidas legales que permiten perseguir y castigar los delitos cometidos por estos sujetos, soluciones que se estudian en el siguiente capítulo con el fin de encontrar planteamientos ecuanímenes para que el Estado de Guatemala pueda solventar esta problemática.

---

<sup>9</sup> <https://gestion.pe/tecnologia/siete-caracteristicas-identificar-ciberdelincuente-122640-noticia/>  
Consultado el 08/06/2020





## CAPÍTULO III

### 3. Derecho comparado

Con la aparición de nuevas tecnologías han surgido nuevas formas de cometer delitos sin que el sujeto activo se encuentre en el lugar donde se realiza la acción ilícita. Este problema ha traído consigo consecuencias jurídicas para los distintos países del mundo en cuanto a que muchos de ellos optaron por modificar el derecho penal, debido a que algunos delincuentes hacen uso de los sistemas de cómputo y de aplicaciones digitales, ya sea como medio o método, y así cometer delitos informáticos.

Con la aparición del internet varios delitos se han convertido en crímenes transnacionales y ello ha coadyuvado de cierta forma al crimen organizado; esto derivado del gran impacto de la globalización, la cual ha traído consigo grandes beneficios, así como la proliferación de estas conductas criminógenas.

“El crimen organizado no existe como tipo ideal, sino como un **grado** de actividad criminal o como un punto del **espectro de la legitimidad**.”<sup>10</sup> En esta definición se puede observar, que con el pasar del tiempo, como el crimen organizado y sus diferentes formas de actividades ilícitas se proliferan, rebasando los límites territoriales de un país determinado por ello estamos frente a lo que conocemos como delincuencia transnacional.

---

<sup>10</sup> Resa Nestares, Carlos. **Crimen organizado transnacional: Definiciones, causas y consecuencias.** Pág. 47

“Dentro de la definición de crimen organizado, la gama de actividades que puede ejecutar un determinado grupo de crimen organizado puede ser extensa, variando en cada caso según diversas variables internas y externas a la organización, y combinar uno o más mercados, expandiéndose asimismo por un número más o menos limitado de países, aunque en tiempos recientes existe una fuerte tendencia a la concentración empresarial en cada vez menos grupos de un mayor número de campos de ilegalidad. Su repertorio de actividades incluye el delito de cuello blanco y el económico (En donde se encontrarían los delitos informáticos), pero supera a este último en organización y control, aunque los nexos de unión entre ambos modelos de delincuencia tienden a fusionarse y el terrorismo y el ciberterrorismo pueden llegar a formar parte de sus acciones violentas en ciertas etapas y momentos.”<sup>11</sup>

El crimen organizado, como comúnmente se le conoce, se ha transnacionalizado y consigo atrajo nuevas formas de cometer delitos y como consecuencia nuevos métodos para cometerlos.

A raíz de esto las grandes organizaciones criminales, como las mafias del sureste o suroeste asiático, la mafia italiana, las Yakuza en Japón, las Triadas en China y la mafia rusa, han ido evolucionando y con la aparición de la tecnología encontramos una nueva forma de criminales denominados *crakers* quienes son catalogados como los verdaderos piratas informáticos y que con el uso de su conocimiento en informática

---

<sup>11</sup> Acurio del Pino, Santiago. **Delitos Informáticos: Generalidades.**  
[http://www.oas.org/juridico/spanish/cyb\\_ecu.htm](http://www.oas.org/juridico/spanish/cyb_ecu.htm). Pág. 3



cometen delitos que han causado grandes pérdidas contabilizadas en millones de dólares a bancos y empresas, así como a Estados completos.

Además, este tipo de delincuentes han apoyado al crimen organizado con los crímenes de robo de identidad, clonación de tarjetas de crédito, han prestado su ayuda a empresas legítimas para cometer ilícitos, tales como la vulneración de normativas medio ambientales y laborales; la utilización de redes legítimas para cometer actividades ilícitas, y en cuanto al tráfico de drogas crean empresas de transporte y las gestionan para transportar sus mercancías, así como se ha determinado que utilizan inmobiliarias para el lavado.

Derivado de lo anterior, en los últimos años se ha puesto en discusión en el ámbito internacional un acuerdo en cuanto a la forma de valorar jurídica y políticamente los delitos que se derivan por el mal uso de los sistemas de cómputo y programas informáticos y que sin lugar a dudas, ha dado origen, a que en algunos Estados, se adecue la rama del derecho penal.

Por lo anteriormente descrito, es necesario indagar sobre las soluciones que se han planteado a nivel internacional e identificar las características criminógenas en las que se basan los diferentes países que han optado por tipificar las conductas delictivas derivadas por el uso inadecuado de los sistemas de cómputo y plataformas digitales, cualquiera que sea su índole.



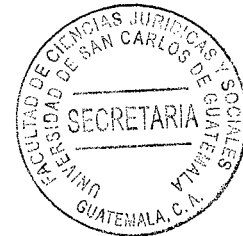
### **3.1. Soluciones planteadas en otros países**

Sin lugar a dudas los delincuentes catalogados como terroristas; así como, grandes organizaciones criminales transnacionales se aprovechan de las nuevas tecnologías con el fin de cometer delitos haciendo uso de las redes de telecomunicaciones y donde han encontrado un lugar adecuado para expandir sus redes criminales, es por ello que el Estado debe detener esta situación haciendo uso de sus organismos, que se encuentran a cargo del control de esta clase de conductas delictivas.

Es preciso mencionar que, algunos países y organizaciones internacionales ante el crecimiento constante de estas conductas delictivas y la necesidad de poder frenar esta nueva forma de delinquir, que a su paso causan grandes daños y perjuicios a la humanidad, han logrado legislar sobre los delitos informáticos.

Por otra parte, aunque ha existido un gran esfuerzo por parte de los Estados y organizaciones internacionales para combatir y erradicar estos delitos, no se ha concretado un criterio de cómo deben ser afrontados, por lo tanto, es necesario la unificación de criterios y con ello obtener una base sustentable para la legislación internacional y así lograr que más países puedan tipificar los delitos informáticos tomando en cuenta los criterios internacionales.

A continuación, se desarrollan aspectos importantes sobre la legislación de diferentes países; así como, los criterios de cada uno de ellos, para comprender qué tipo de conductas delictivas han tipificado para su persecución.



### 3.1.1. Alemania

A partir del 15 de mayo de 1986, Alemania crea la Ley Contra la Criminalidad Económica la cual entra en vigencia el 1 de agosto de 1986, con el fin de regular a la delincuencia informática y en la cual establece los siguientes delitos:

- a) Espionaje de datos.
- b) Estafa informática.
- c) Alteración de datos.
- d) Sabotaje informático.
- e) Utilización abusiva de cheques o tarjetas de crédito.

“En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.”<sup>12</sup>

Por otra parte, al momento de querer tipificar nuevas formas delictivas encaminadas a erradicar los delitos informáticos, el gobierno alemán estudio el origen de la dificultad de aplicar el derecho penal convencional a las conductas dañinas o delitos cometidos por medio de los procesos electrónicos de intercambio de datos y que tienen un rol esencial

---

<sup>12</sup> *Ibíd.* Pág. 35





en la vida humana, así como el estudio de aquellos bienes jurídicos a los que el Estado debe de garantizar su protección para con sus habitantes y que resultan vulnerados por la utilización abusiva de la informática.

Sin embargo, los delitos tipificados en la Ley Contra la Criminalidad Económica, con relación a los delitos informáticos en Alemania, tuvo como dificultad poder encontrar tres aspectos esenciales por los cuales estos delitos no pudieran ser análogos del delito de estafa o acción engañosa, de tal cuenta que la producción del error y disposición patrimonial, en el engaño del computador, así como garantizar las posibilidades de control de este nuevo ámbito legal fueron los desafíos a enfrentar, por lo que la solución radica en que, al momento de tipificar, el daño que se comete en contra del patrimonio se realiza producto de una elaboración de datos que es originada por medio de una realización errónea del programa, por introducción de datos incorrectos o incompletos al programa, mediante el uso no permitido de datos o de una intromisión ilícita al sistema.

Derivado de lo anterior, se logra la tipificación de los delitos informáticos, se evidencia la protección paulatina de algunos bienes jurídicos y con ello se puede determinar que el derecho vigente no es suficiente para garantizar la seguridad jurídica de éstos, ya que se han encontrado nuevas formas de vulnerar los derechos de las personas por el uso malicioso de la informática.

Es de manifestar que la aparición de los delitos informáticos trajo consigo una nueva forma de vulnerar los bienes jurídicos, lo cual además de ser tipificado debe ser castigado con una pena, en el sentido que el acto delictivo consista en almacenamiento



de datos, transmisión de datos, o dañar sistemas informáticos ya sea en su estructura física o en el procesamiento lógico de sistemas.

### **3.1.2. Argentina**

En Argentina se opta por modificar el Código Penal por medio de la Ley 26388 la cuál fue sancionada el 4 de junio de 2008 e incorpora delitos como:

- a) Distribución y tenencia con fines de distribución de pornografía infantil.
- b) Violación de correo electrónico.
- c) Acceso ilegítimo a sistemas informáticos.
- d) Daño informático y distribución de virus.
- e) Daño informático agravado e interrupción de comunicaciones.

El mayor aporte de esta legislación es el introducir la definición de documento electrónico, el cual comprende toda la representación de actos o hechos, que independientemente del soporte utilizado para su elaboración, almacena, archiva o transmite información de forma digital.

También, se introdujeron los términos firma y suscripción lo que debe de entenderse como la creación de la firma digital o bien, firmar digitalmente, además se crean los términos instrumento privado y certificado lo cual debe comprenderse como todo documento digital firmado de forma digital.



Además de los delitos mencionados, se tipifica dentro determinados bienes jurídicos tutelados formas de cometer ilícitos por medio del uso de la informática dentro de los cuales encontramos los siguientes artículos del Código Penal de Argentina, siendo éstos:

Para la protección del bien jurídico de la integridad sexual encontramos el Artículo 128 el cual sanciona con prisión de tres a seis años toda distribución de pornografía infantil por medios digitales u análogos,

En cuanto a los delitos de violación de secretos y de la privacidad se tipifica en los Artículos 153, 153 bis sancionándose con pena de prisión o multa a las personas que abran, accedan, apoderen, supriman, desvíen, intercepten o cambien indebidamente una comunicación electrónica, ya sea por medio de telégrafo, teléfono u otra tecnología y éste no le pertenece.

El Artículo 155 bis del cuerpo legal relacionado sanciona con multa o pena de prisión a las personas que se encuentran en posesión de correspondencia ajena de una comunicación electrónica y, aunque no están destinados a publicidad, se publican indebidamente y éste cause agravio a terceras personas.

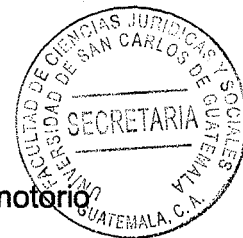
Los Artículos 157, 157 bis de la citada ley, tipifica y castiga a los funcionarios públicos que tienen en su poder documentos o datos que por ordenanza legal deben ser confidenciales y que por cualquier circunstancia dicho funcionario los revele.

El Artículo 173 numeral 16 contiene los delitos relacionados a las estafas y otras defraudaciones, sin embargo, específicamente en la parte conducente se tipifica lo relativo a la estafa o defraudaciones realizadas por medio de la manipulación informática o que produzca alteraciones al debido funcionamiento de un sistema informático e inclusive hace mención de los datos que son transmitidos por medios digitales.

En otro contexto, el Artículo 184 numeral 5 de dicho cuerpo normativo sanciona los daños que se causan al momento de ejecutar programas que causen agravio a datos, documentos, programas o sistemas informáticos de índole público.

Asimismo, el Artículo 197 del Código Penal de Argentina encontramos los delitos contra la seguridad del tránsito y de los medios de transporte y de comunicación, en dicho artículo se regula una sanción con prisión a las personas que interrumpan o entorpezcan una comunicación que se transmita por cualquier vía informática o resista de manera violenta restablecer la comunicación que ha interrumpido.

Por último, en el Artículo 255 de la citada ley se tipifican los delitos relativos en cuanto a la violación de sellos y documentos, por lo que se castiga con pena de prisión la destrucción o alteración de objetos que son destinados como medios de prueba ante autoridad competente. En el mismo sentido se castigará al funcionario público que tenga en su custodia documentos de interés al público, además incurre en este mismo delito, el depositario que destruya o altere documentos que sirvan como prueba o sean de interés público, ya sea por imprudencia o negligencia.

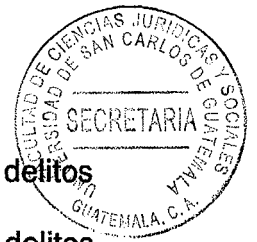


Al abordar la legislación de Argentina, en cuanto a los delitos informáticos, es notorio que optan por implementar una reforma al Código Penal para poder abordar la problemática en cuanto a la criminalidad informática, planteando así una solución, que si bien es cierto no acabará con este fenómeno, sin embargo, abre una ventana a que otros países en América Latina se percaten de esta nueva forma criminal.

### **3.1.3. España**

Es este país los delitos informáticos son introducidos a la legislación a partir del Código Penal de 1995, que es aprobado a través de la Ley Orgánica 10/1995 del 23 de noviembre de 1995 y publicado en la Agencia Estatal Boletín Oficial del Estado -BOE- bajo el número 281, el 24 de noviembre de 1995, en la cual se tipifican los siguientes delitos:

- a) Interceptación del correo electrónico.
- b) Usurpación y cesión de datos reservados de carácter personal.
- c) Fraude informático.
- d) Daños informáticos.
- e) Difusión de mensaje injurioso o calumnioso.
- f) Falsedades documentales.
- g) Revelación de secretos.



El Código Penal español no diversa de la tipificación tradicional en materia de delitos informáticos, sin embargo, destaca el equilibrio jurídico que existe entre los delitos comunes o tradicionales y la nueva corriente de criminalidad informática, además, el gobierno español ha realizado un esfuerzo para evitar la separación de los delitos informáticos del resto de delitos comunes tipificados en el Código Penal, así como la creación de leyes especiales; ya que, de realizarlo de esa forma evidenciaría una mala práctica legislativa, como sucede en algunos países de Latinoamérica.

#### **3.1.4. Estados Unidos**

En Estados Unidos se aborda la problemática de la criminalidad informática desde un punto de vista distinto a otros países, debido a que tratan de erradicar las definiciones y términos de nivel técnico muy elevado y que tienden a confundir a la población con relación a tecnologías digitales. De tal cuenta en 1994 a través del Acta Federal de Abuso Computacional, se modifica el Acta de Fraude y Abuso Computacional de 1986.

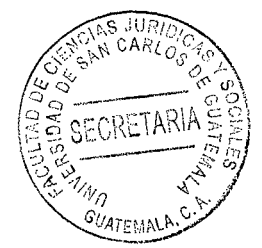
Dicha reforma representa un adelanto en la referida materia porque está ligado a erradicar los actos de transferencia de virus informáticos como un gusano, caballo de Troya, entre otros, así como eliminar la transmisión de programas, información digital, código o comandos que estén destinados a causar agravio a los sistemas de cómputo, al sistema lógico, redes *Wide Area Networks* WAN, *Local Area Networks* LAN, *Global Area Networks* GAN, *Metropolitan Area Networks* MAN y *Personal Area Networks* PAN; información digitalmente almacenada, datos o programas digitales.



Es de mencionar que los legisladores estadounidenses sancionan a este tipo de delincuentes con dos tipos de sanciones, la primera radica en sancionar a los creadores de virus informáticos y cuyo fin es causar daño de manera intencional, el que será sancionado con prisión federal de 10 años más una multa, además, el creador de un virus nunca podrá alegar en su defensa que desconocía que con su actuar podría causar agravio a terceros, o que él simplemente quería hacer llegar un mensaje como muchas veces sucede; y, la segunda, sanciona a las personas, que de forma imprudencial, transmiten los virus informáticos, por lo que se castiga con multa y un año de prisión.

Por otra parte, al momento de crear esta ley se realiza una tipificación innovadora al momento de no definir a los virus informáticos en específico, sino describiendo la acción antijurídica creando una brecha a una nueva etapa de atentados cibernéticos, tecnológicos e informáticos en cualquier medio que se ejecuten.

Por último, cabe destacar que la legislación estadounidense en lo que concierne al concepto de *computer contaminant* o virus, como comúnmente se conoce, no hace referencia únicamente a los gusanos informáticos o troyanos, sino además, enmarca una serie de algoritmos, programas y tecnologías desarrolladas con el fin de causar daños por medio de invasiones digitales a los diferentes programas o base de datos, y que permiten modificar, destruir, copiar o trastornar la operación normal de un ordenador y sus componentes, así como de sistemas o redes informáticas.



### 3.1.5. México

En México no se cuenta con un gran avance en la materia, pero cabe destacar que los delitos informáticos son sancionados con una multa de 100 hasta 600 días, un día de multa equivale a un día de salario mínimo en México, o con pena de prisión de seis meses hasta cuatro años. Sin embargo, han logrado tipificar los delitos relativos a la revelación de secretos, contemplados en los Artículos 211 y 211 bis del Código Penal Federal de México, así como los delitos de acceso ilícito a sistemas y equipos de informática, regulados en los Artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6 del Código Penal Federal de México.

Por otra parte, en los Artículos 112 y 113 de la Ley Federal del Derecho de Autor prohíbe la importación, fabricación, distribución y uso de medios informáticos cuyo fin sea erradicar la protección técnica de los programas de cómputo, así como la transmisión, sin autorización, por medio de las redes electromagnéticas y programas efectuados electrónicamente cuyo contenido sea visual, sonoro, tridimensional o animado.

Indiscutiblemente la falta de regulación y protección de los bienes jurídicos como el patrimonio, la privacidad, la confidencialidad, propiedad intelectual y honor de las personas, en lo que respecta a los delitos informáticos, dió como origen que muchas personas cometan ilícitos por medio de sistemas de cómputo y las plataformas digitales que utilizan conexión a internet, por lo que estas conductas fueron catalogadas por muchos juristas como delitos cibernéticos de nueva generación, siendo esto un



problema social, en el que algunos países de distintas partes del mundo han podido afrontar con una técnica jurídica adecuada.

En ese sentido se han sumado a esta lucha distintas organizaciones internacionales, que, junto al esfuerzo de algunos países del mundo, se pudo lograr la realización diferentes acuerdos y convenios encaminados a erradicar esta problemática.

### **3.2. Convención sobre la cibercriminalidad de la Unión Europea**

El crimen organizado habitualmente se dedica a identificar y valerse de oportunidades para cometer nuevos actos delictivos. En ese sentido, siendo internet una red globalizada y en constante crecimiento donde el comercio a través de la tecnología pudo expandirse hacia nuevas oportunidades; lamentablemente, también ha generado la aparición de otras formas de crear negocios y beneficios ilícitos poniendo en peligro a la comunidad de usuarios de internet.

Durante una convención celebrada el 21 de noviembre de 2001, en la ciudad de Budapest, el Consejo de Europa y distintos países del mundo, entre los cuales se encuentran potencias como Estados Unidos y Japón firmaron el Convenio de Cibercriminalidad de la Unión Europea; cuyos objetivos buscan igualar los regímenes legales en materia penal sustantiva que tienen como finalidad tipificar los crímenes que se cometen en el contexto informático; regular, en lo procedimental, la competencia para que los jueces investiguen y persigan los delitos informáticos; y mediante una normativa activa y positiva facilitar la colaboración internacional.



En cuanto al contenido del Convenio de Cibercriminalidad de la Unión Europea podemos mencionar que se divide en cuatro capítulos en los cuales se ven reflejados los objetivos que se desean alcanzar mediante su suscripción.

El capítulo primero se compone de términos y definiciones necesarias para la comprensión del espíritu de la norma; el capítulo segundo aborda las disposiciones que deben ser empleadas a nivel nacional, haciendo énfasis en distinguir las disposiciones del Convenio sobre Cibercriminalidad a las normas penales sustantivas, así como incluir las disposiciones procesales y jurisdiccionales; dentro del tercer capítulo se hace referencia en cuanto a los principios generales en cuanto a la extradición, cooperación y asistencia internacional, además se encuentran las disposiciones aplicables en caso de que no existan acuerdos, convenios o tratados internacionales.

Por otra parte, en el cuarto capítulo se regulan las disposiciones finales encaminadas a regir la entrada en vigor, la forma en que pueden suscribirse otros países al Convenio de Cibercriminalidad, la aplicación territorial, los objetivos de ratificar el Convenio, reservas, declaraciones y enmiendas.

Sin duda alguna la Convención sobre Delitos Informáticos refleja el trabajo y esfuerzo de la cooperación internacional más relevante para combatir la criminalidad informática y siendo internet un sitio propicio para la ejecución y optimización de conductas delictivas en circunstancias anónimas es deber del Estado de Guatemala, así como de países latinoamericanos, regular las sanciones y procesos de investigación idóneos que puedan hacer frente a los denominados delitos informáticos.



### **3.3. Organización de los Estados Americanos**

Con la invención de internet y su uso hacia la economía mundial se puede apreciar un gran aumento en la productividad, operatividad y reinversión de los negocios en el continente americano. Pequeñas y grandes empresas hacen uso de internet y sus distintas redes de información para coordinar, diligenciar actividades, comunicar datos y realizar investigaciones. Derivado de lo anterior, en el año 2001 se celebró en la Ciudad de Québec la tercer Cumbre de las Américas, en donde los grandes mandos de nuestro continente se comprometieron a resguardar la seguridad y aumentar la conectividad de los países americanos.

A raíz de la realización de la Cumbre de las Américas se han desarrollado diferentes políticas que buscan combatir las amenazas cibernéticas hacia la información que viaja en internet y que puede ser interrumpida o redirigida con el fin de impedir el correcto funcionamiento de un gobierno o los servicios públicos, afectando de esa forma a los ciudadanos en su economía y suministros básicos como redes eléctricas, agua potable, redes de telecomunicación y transporte; servicios que cada vez más necesitan estar conectadas por internet para tener mejor rendimiento e infraestructura.

Dentro de las políticas para combatir y erradicar las amenazas cibernéticas, es relevante mencionar la resolución AG/RES 1939 XXXIII-O/03 denominada, Desarrollo de una Estrategia Interamericana para Combatir las Amenazas Cibernéticas, emitida por la Asamblea General de la Organización de los Estados Americanos, aprobada el



10 de junio de 2003, en la cual se demuestra la vulnerabilidad de la seguridad informática y la amenaza que representa en los sistemas informáticos esenciales de infraestructura y economía mundial, y que para solucionar esta problemática se necesita una ayuda y coordinación mutua integrada por los distintos sectores económicos así como el apoyo de organismos gubernamentales.

La Estrategia Interamericana Integral de Seguridad Cibernética hace conciencia en las funciones y responsabilidades de los encargados de brindar seguridad a las redes y sistemas informáticos con el fin de incentivar el desarrollo de la seguridad informática. Además, se establece un sistema para la protección de redes y datos informáticos que circulan en internet encaminado a garantizar una respuesta inmediata y recuperación satisfactoria ante un ataque informático.

Sin embargo, la recuperación depende de la creación de instituciones públicas y privadas que velen por fomentar la educación en seguridad informática, además, que tengan capacidad de coordinar e instruir a los usuarios y fabricantes de computadoras con la finalidad de asesorar sobre la forma correcta de asegurar sus redes en contra de amenazas y posibles vulnerabilidades.

De lo anterior, se pretende evaluar e identificar procesos y métodos que resguarden la información que viaja diariamente en internet para que así los gobiernos puedan adoptar políticas y normas encaminadas a tipificar los delitos informáticos, protegiendo de esta manera a las personas que utilizan internet, previniendo el manejo ilícito y malicioso de los sistemas de cómputo y redes digitales.

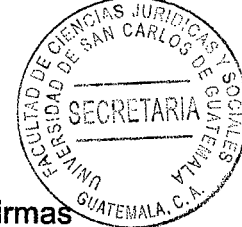


Por último, las políticas desarrolladas por la Organización de los Estados Americanos en la VI Conferencia de Ministros de Defensa de las Américas, celebrada en Ecuador en noviembre de 2004, hacen un llamado a prestar ayuda mutua entre los países miembros de la O.E.A. con el objeto de impulsar normas preventivas que sean capaces de enfrentar amenazas cibernéticas realizadas por grupos delincuenciales y terroristas.

#### **3.4. Situación de los delitos informáticos en Guatemala**

En Guatemala los delitos informáticos se encuentran regulados en el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, a partir del Título VI, de los delitos contra el patrimonio; Capítulo VII, de los delitos contra el derecho de autor, de la propiedad industrial y delitos informáticos; Artículos 274 "A" al 274 "H", en los cuales únicamente se tipifican delitos en contra de acciones que perjudiquen los derechos de autor por el daño causado a registros y datos informáticos contenidos en dispositivos de almacenamiento digital, protegiendo única y exclusivamente el bien jurídico del patrimonio.

Por otra parte, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto 47-2008 del Congreso de la República de Guatemala, se emite por la necesidad de verificar conceptos del mundo digital aplicados al comercio nacional e internacional, con el fin de crear, estimular y fomentar que las operaciones mercantiles sean más rápidas y eficientes con el uso de la tecnología informática. Además, se utiliza como instrumento legal para dar seguridad jurídica a las



contrataciones electrónicas, así como legitimidad al reconocimiento de firmas electrónicas asemejándolas respecto a documentos de papel y firmas manuscritas.

Sin embargo, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto 47-2008 del Congreso de la República de Guatemala, reconoce definiciones aplicables al uso de comunicaciones electrónicas y por consiguiente abre la oportunidad de introducir normas especializadas a proteger las instituciones creadas por esta normativa. Además, el Artículo 3, de la citada ley, produce una laguna legal al establecer que para poder interpretar y aplicar de forma adecuada se deberá regir por el origen internacional y, teniendo en cuenta que el Estado de Guatemala no ha suscrito ningún tratado o convenio internacional en materia informática, la aplicación de esta ley se podrá ver ambigua.

Por otra parte, los diputados Félix Ruano, Francisco Contreras y Mario Mazariegos, crean la iniciativa 4055 de Ley de Delitos Informáticos, la cual tiene por objeto proteger la integridad de las personas, bienes, derechos y obligaciones mediante la creación de disposiciones jurídicas enfocadas a tecnologías informáticas. Además, trata de prevenir y sancionar, entre otros, actos como el *hacking* (Acceso sin autorización), *cracking* (daño o sabotaje), *phishing*, *smishing*, *vishing*, (Invitación de acceso a sitios o sistemas informáticos falsos o fraudulentos), y pornografía infantil, entre otros actos ilícitos informáticos. Por último, encontramos que esta iniciativa solicita que sea creada una fiscalía especializada para el combate y persecución de estos actos criminales.



Durante los últimos 10 años se han logrado grandes descubrimientos y avances tecnológicos y sumado a ello la criminalidad cibernética. De lo anterior, se observa que durante este período en Guatemala no existe voluntad e interés político de crear normas encaminadas a regular y tipificar la tecnología y los delitos que se pueden cometer derivados de su uso malicioso, por lo que combatirlos en un futuro será un reto para los legisladores, el gobierno central y el órgano de justicia. Es por ello, que se recomienda realizar estudios orientados para perfeccionar la iniciativa de Ley 4055 y así obtener una referencia y una solución a la delincuencia cibernética que con el pasar del tiempo se perfecciona a nivel nacional e internacional.



## CAPÍTULO IV

### 4. Propuesta de estructuración de las principales conductas delictivas derivadas del uso inadecuado de las plataformas digitales de video juegos

Los *gamers* existen desde hace tiempo, en la década de los 80's se organizaron los primeros torneos, pero es en la actualidad que viven su mejor momento a través de los *e-sports* (deportes electrónicos), esto gracias al crecimiento del internet, nuevas tecnologías y plataformas digitales. Derivado de ello grandes empresas realizan inversiones millonarias con el objetivo de que más personas adquieran los productos de los video juegos.

“Actualmente, cerca de 300 millones de personas siguen de forma habitual los deportes electrónicos. La final de “League of Legends” alcanzó los 36, más que la final de la NBA o del mundial de Rugby.”<sup>13</sup>

Por otra parte, el Instituto Nacional de Estadística de Guatemala –INE- ha revelado en el último censo realizado en el año 2018, que el 21% de la población, equivalente a 2.62 millones de personas, tienen acceso a una computadora; y el 29%, equivalente a 3.67 millones de guatemaltecos utilizan internet, este último dato consecuencia de la ventaja que tienen los teléfonos celulares o *Smartphone* para acceder a sitios en el ciberespacio.

---

<sup>13</sup> [https://as.com/esports/2016/09/16/portada/1473981525\\_248613.html](https://as.com/esports/2016/09/16/portada/1473981525_248613.html). (Consultada: 25 de septiembre de 2020)





Es evidente que en Guatemala con el pasar del tiempo la tecnología se vuelve indispensable para la vida cotidiana de sus habitantes, ya que a través de ella se pueden hacer gestiones bancarias electrónicas, compras en línea a comercios y restaurantes, ver películas por medio de plataformas multimedia y entretenerse con la variedad de videojuegos.

**“Un *gamer* profesional guatemalteco, Estephan Méndez es un joven guatemalteco que se dedica, de manera profesional, a jugar a *League of Legends*, y ha competido en torneos a nivel latinoamericano. Ahora se esmera en entrenar a *gamers* para destacar en este videojuego y representar a su equipo, *Predators*, en competencias internacionales.**

Méndez, a quien en el mundo de los *e-sports* se le considera un *coach*, es de los cuatro o cinco centroamericanos que se dedican a esta actividad de manera profesional, comenta Prensa Libre.”<sup>14</sup>

**“Guatemala gana primero y segundo lugar en campeonato centroamericano de E-Sports. Francisco Mac PANCHOMAC199026 obtuvo el primer lugar centroamericano en FIFA18, mientras que el equipo Shorys Gaming ganó el segundo lugar en League Of Legends, en el torneo centroamericano Axe Gaming League.**

---

<sup>14</sup> <https://www.prensalibre.com/vida/tecnologia/asi-son-los-gamers-profesionales-y-el-fenomeno-de-los-esports/> (Consultada: 30 de agosto de 2020)



El campeonato regional se realizó el pasado 27 de octubre y reunió a los jugadores más diestros en los videojuegos de más demanda, FIFA 18, League of Legends y Clash Royale, llevándose a cabo en modalidad virtual para que los participantes pudieran enfrentarse cara a cara con sus competidores en esta gran final. Prensa Libre”<sup>15</sup>

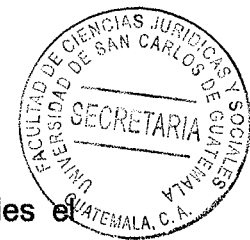
En Guatemala, es una realidad que las personas utilizan los videojuegos como pasatiempo, sin embargo, hay personas que ya se dedican a usarlos como un trabajo e incluso como una carrera profesional, participando en torneos internacionales, los cuales son transmitidos por plataformas de *streaming* como *Twitch.tv*, *Facebook live*, *Periscope*, *YouTube*, entre otras plataformas, a las cuales se han ido sumando cadenas de televisión como ESPN y FoxSport.

Sin embargo, cabe destacar que esto influye a más personas para hacer uso de los videojuegos, esto con el fin de que las empresas desarrolladoras obtengan ganancias las cuales ascienden a más de US\$493,000,000, unos Q2,500,000,000, tan solo en en competiciones de *E-Sports*.

En la actualidad miles de personas son parte de esta nueva corriente tecnológica, tanto niños como adultos mayores buscan entretenimiento a través de los videojuegos ya sea desde un dispositivo móvil *Smartphone*, tabletas digitales o computadoras. Es el caso que, para hacer uso de los videojuegos, los distintos servidores solicitan a sus usuarios

---

<sup>15</sup> <https://www.prensalibre.com/vida/tecnologia/campeonato-centroamericano-esports-gamers/>  
(Consultada: 07 de septiembre de 2020)



datos personales y confidenciales con el fin de crear un avatar para permitirles el acceso a los distintos modos de juegos que las plataformas ofrecen.

Habiendo ingresado los datos éstos quedan registrados, no solo en el servidor, sino también en la red de internet; de tal cuenta que cualquier persona que desee realizar actos criminales y tenga conocimientos en informática puede tener acceso a dicha información utilizando medios ilícitos con el fin de obtener beneficios propios o perjudicar a otras personas.

Por tal motivo quedan expuestos los datos personales de los usuarios, por lo que se considera necesario indagar acerca de las principales características que los denominados delincuentes cibernéticos tienen al momento de cometer delitos para posteriormente ser tipificados ya sea por incorporación al Código Penal o en una ley especial en la materia.

Para el efecto se debe de tomar en cuenta los bienes jurídicos tutelados que se vulneran a raíz de las conductas realizadas por el delincuente cibernético, así como los métodos y herramientas que se utilizan, para posteriormente acoplarlos a una legislación que pueda resolver esta problemática.

#### 4.1. Bienes jurídicos tutelados

Para comprender cuáles son los bienes jurídicos tutelados vulnerados por los delincuentes informáticos, se debe de tomar en cuenta la naturaleza del delito cometido, es decir, si el hecho ilícito violenta derechos como la intimidad, la propiedad privada, propiedad intelectual o industrial, la fe pública, el buen funcionamiento de la administración, la seguridad interior o exterior del Estado.

La empresa *eset Nod32* expertos en la materia, creadores de defensa y seguridad informática se pronuncian de forma general respecto a los delitos informáticos cometidos en plataformas digitales de videojuegos: “La venta de elementos virtuales (incluyendo las monedas virtuales) constituye una parte importante de la economía propia del juego, pero a su vez presenta algunas oportunidades únicas para los delincuentes que generalmente son: robo de bienes, falsificación de elementos, *gold farmers* o granjeo de oro.”<sup>16</sup>

En cuanto al robo de bienes, sucede que el desarrollador del videojuego crea una necesidad de jugar mediante recompensas a sus usuarios que consiste en brindar elementos raros, únicos y de edición limitada, siendo éstos muy escasos por lo que motiva a los jugadores a obtenerlos con dinero real, además, el desarrollador de videojuegos puede cobrar tarifas de suscripción para jugar, por lo que el dinero real se vuelve objeto de lucro para los delincuentes.

---

<sup>16</sup> <https://www.welivesecurity.com/la-es/2014/08/26/videojuegos-blanco-para-crimen/> (Consultada: 27 de octubre de 2020)



Es por esa razón que los usuarios de las plataformas a menudo reciben ataques de bandas de delincuentes, con correos electrónicos de *phishing* o *software* que permiten el robo de contraseñas con el fin de obtener las credenciales personales de las cuentas de los jugadores, de esa forma los *ciber* delincuentes vacían la cuenta del usuario, sin dejar rastro del ilícito cometido.

El Código Penal de Guatemala, Decreto 17-73 del Congreso de la República de Guatemala, tipifica el delito de robo en el Artículo 251 y dentro del bien jurídico tutelado de esos delitos está el patrimonio. Al analizar este delito dentro del cuerpo legal citado destaca que los bienes objeto de robo, son bienes corpóreos, por lo que al aplicar esta norma jurídica en el robo informático no es viable, debido a que, el fin primordial de los *ciber* delincuentes es obtener los bienes que se encuentran en las plataformas digitales, es decir, bienes incorpóreos.

Además, para que los criminales informáticos puedan tener acceso a los bienes de los *gamers* es necesario irrumpir la seguridad informática con el fin de obtener información, por lo que, en este caso, el sujeto activo comete el delito de acceso sin autorización o acceso ilícito, el cuál no se encuentra regulado en Guatemala.

En la legislación guatemalteca se trata de abordar esta problemática en la iniciativa de ley 4055, Ley de Delitos Informáticos Artículo 4 (Acceso sin Autorización). El que, sin plena autorización, acceda, intercepte, interfiera o utilice un sistema o dato informático, de naturaleza privada o pública, y de acceso restringido, será penado con prisión de



dos a seis años. Dentro de esta figura delictiva la intención del delincuente es infringir el sistema informático y hacer uso de la información del usuario.

Debido a que el delito de robo de bienes cuenta con una intención de lucro mediante la transferencia no autorizada de cualquier activo patrimonial en perjuicio de un tercero haciendo uso de herramientas informáticas, se considera que esta acción debe ser regulada dentro del delito de fraude informático.

Dicho delito se encuentra regulado en el Artículo 8 del Convenio sobre Cibercriminalidad, así como en el Artículo 8 de la Iniciativa número 4055, Ley de Delitos informáticos el cual establece: (Fraude informático) Quien para obtener algún beneficio para sí mismo o para un tercero, mediante cualquier artificio tecnológico o manipulación de sistema 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 100 hasta 1000 veces el salario mínimo legal vigente.

En lo que respecta al tema de estudio, en el delito de robo de bienes, se puede observar que en Guatemala los bienes jurídicos que se encuentran en riesgo de ser violentados por parte de los delincuentes informáticos son el patrimonio, la confidencialidad, la integridad, la disponibilidad de datos y los sistemas informáticos.



Por otra parte, se encuentra la falsificación de elementos, que en el mundo virtual de los videojuegos consiste en la duplicidad de elementos o moneda del juego en forma repetitiva y constante aprovechándose de la fragilidad, vulnerabilidad y errores que las plataformas pueden tener derivado de una mala conexión con el servidor, problemas con diferencia horaria, entre otros; con el objetivo de hacerlos pasar como si fueran reales y obtener el beneficio económico que éstos representan.

El riesgo de la falsificación de elementos recae en poder duplicar determinado elemento o moneda virtual tantas veces como sea posible hasta generar excesivas cantidades de dinero y crear pérdidas millonarias a los desarrolladores de videojuegos.

“La falsedad puede configurarse de dos maneras: (1) Mediante la “simulación” (sic.), cuando se representa algo fingiendo o imitando lo que no es, es decir, que estamos ante la situación total de lo verdadero. (2) Mediante la “alteración” (sic.), cuando se modifica o cambia la esencia o forma de algo, es decir, se altera algún elemento del objeto verdadero, caso en el cual estaríamos ante una sustitución parcial de lo verdadero”<sup>17</sup>

El Código Penal de Guatemala, Decreto 17-73 del Congreso de la República de Guatemala, regula en el Artículo 321 el Delito de Falsedad Material y establece: Quien hiciere, en todo o en parte, un documento público falso, o alterare uno verdadero, de modo que pueda resultar perjuicio, será sancionado con prisión de dos a seis años. Por otra parte, en el Artículo 322 del mismo cuerpo legal se encuentra regulado el delito de

---

<sup>17</sup> Alvarado, José y Morales, Ronald. **Ob. Cit.** Pág. 91



falsedad ideológica el cual establece: Quien, con motivo del otorgamiento autorización o formalización de un documento público, insertare o hiciere insertar declaraciones falsas concernientes a un hecho que el documento deba probar, de modo que pueda resultar perjuicio, será sancionado con prisión de dos a seis años.

Al analizar ambos artículos se observa que el objeto principal de la falsedad en el derecho penal guatemalteco es alterar o simular un documento, emitido por funcionario público, es decir, aquellos documentos autorizados por funcionario, empleado o notario público, a quien se le ha otorgado fe pública y cuyo contenido crea certeza probatoria en el mundo de lo jurídico.

Actualmente Guatemala no cuenta con normas adecuadas que tipifiquen la falsificación de datos informáticos, por lo que, la simulación o alteración de elementos o monedas de cambio en las plataformas de videojuegos, así como los datos e información de muchas otras plataformas digitales, queda impune.

Sin embargo, a falta de una norma que regule la falsificación informática y para definir apropiadamente como delito informático, se debe de considerar lo establecido en el Artículo 7 del Convenio sobre la Ciberdelincuencia: Falsificación informática. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias, para tipificar como delito en su derecho interno la introducción, alteración, borrados o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos, con intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las partes





podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

De tal manera que los datos o elementos informáticos deben ser introducidos, alterados, borrados o suprimidos para crear información ilegítima con el fin de que sea utilizada como información auténtica.

De esta forma los datos y elementos informáticos deben llevar un proceso para ser constitutiva de información ya sea legítima o ilegítima, por lo que el bien jurídico tutelado en el delito de falsificación informática es la información; en ese sentido se debe de proteger la integridad de la información, para que ésta no deba de ser alterada ni modificada.

Por último, el término *gold farmer* o granjero de oro, surge debido a que existen usuarios que utilizan las plataformas de videojuegos para generar la moneda del juego para posteriormente venderla en línea a cambio de dinero del mundo real.

De igual forma que la falsificación de elementos amenaza la economía en los videojuegos, debido a que estas conductas generan inflación, también provocan más problemas dentro de las plataformas digitales como en el mundo real por medio del *spam* que contiene avisos publicitarios para la reventa del oro obtenido.



Para poder encuadrar la conducta del granjero de oro dentro de un ordenamiento jurídico es necesario comprender si la consecuencia del mal causado es originada por dolo o culpa.

En ese sentido cuando el daño es causado por premeditación o con clara intención considerando que el daño ocasione perjuicios económicos en el sistema informático, provoque otros perjuicios o se afecte intereses a terceros, estaríamos frente a la figura del delito de daño informático.

Sin embargo, cuando un sistema informático es dañado por un acto de imprudencia, negligencia, impericia o inobservancia de normas básicas de manejo del sistema informático y que provoque perjuicios económicos en el sistema informático y, además, provoque otros perjuicios o afecte intereses a terceros, estaríamos ante la figura de responsabilidad civil por daño al patrimonio el cual es materia de una proceso civil de daños y perjuicios el cual se encuentra regulado en el Código Civil, Decreto Ley 106 y Código Procesal Civil y Mercantil, Decreto Ley 107.

El Código Penal de Guatemala, Decreto 17-73 del Congreso de la República de Guatemala, en el Artículo 278 regula el delito de daño por lo cual establece: Quien, de propósito, destruyere, inutilizare, hiciere desaparecer o de cualquier modo deteriorare, parcial o totalmente, un bien de ajena pertenencia será sancionado con prisión de seis meses a dos años y multa de 1000 a 10,000 mil quetzales.



En los daños de forma culposa observa que la responsabilidad civil derivada del daño se encuentra regulada en el Artículo 1645 del Código Civil, Decreto Ley 106 el cual establece: Toda persona que cause daño o perjuicio a otra, sea intencionalmente, sea por descuido o imprudencia, está obligada a repararlo, salvo que demuestre que el daño o perjuicio se produjo por culpa o negligencia inexcusable de la víctima.

De los artículos citados se puede apreciar que la diferencia que existe entre el delito de daño con el daño civil, según la ley, recae en el dolo, dicho en otras palabras, la premeditación o intención de causar daño.

Cabe resaltar que de los artículos mencionados se desprende que todo acto realizado de forma premeditada, que cause daño, debe encuadrarse dentro del delito de daño, por lo que la víctima tiene el legítimo derecho de iniciar una persecución penal en contra de la persona que le ha causado un daño y, al mismo tiempo del proceso penal o en otro un procedimiento civil, se puede pretender la reparación de los daños causados al detrimento del patrimonio dañado.

Por lo tanto, el delito de daño regulado en el Código Penal de Guatemala, Decreto 17-73 del Congreso de la República de Guatemala, es inaplicable en materia informática, ya que no se encuentra en el apartado de delitos informáticos de dicha normativa.



A criterio del autor, una definición acertada del delito de daño informático se encuentra en la iniciativa de ley número 4055, Ley de Delitos Informáticos de la forma siguiente; Artículo 6. 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 100 a 500 veces el salario mínimo legal vigente

Es de tomarse en cuenta que el daño informático si puede ser un acto doloso o culposo y que existe el derecho de la víctima para exigir una pena en contra del ciber delinciente, así como el resarcimiento de los daños y perjuicios ocasionados al sistema informático, o en el presente caso a la plataforma de videojuegos.

Por tanto, el *gold farmer* o granjero de oro, causa perturbación en la economía del videojuego, ya que su actuar genera inflación, tanto en el juego como en la vida real. De tal cuenta que este delito vulnera los bienes jurídicos de integridad, disponibilidad y confidencialidad patrimonial o activo digital que se encuentre en cualquier sistema informático.

Por último, cabe mencionar que los delitos informáticos por lo general defienden el bien jurídico de la información, asignándole un valor ya sea económico, un valor propio de la persona humana o un valor atendiendo a los sistemas que la procesan o automatizan. Sin embargo, se observa que estos delitos son de índole complejo, debido a que



tienden a proteger de manera simultánea una pluralidad de bienes jurídicos, sin menoscabo de que alguno de ellos se encuentre independientemente tutelado por otro.

Es de considerar que no basta con examinar el daño que causa en la sociedad los delitos que se cometen en las plataformas de videojuegos también se debe estudiar los métodos que emplean los delincuentes informáticos para tratar de cubrir sus crímenes.

#### **4.2. Principales métodos utilizados por los ciber delincuentes para la comisión de delitos.**

“Cuando se piensa en delitos informáticos por lo general se toma en cuenta que éstos son realizados con el fin de destruir sistemas de cómputo completos, es por ello por lo que muchas personas piensan en proteger las unidades centrales de procesamiento y componentes tecnológicos.”<sup>18</sup>

El ser humano como creador y usuario de los sistemas digitales forman parte importante del sistema de información digital que se encuentra en resguardo de los diferentes dispositivos de almacenamiento cibernéticos. De tal cuenta que los delincuentes informáticos han desarrollado técnicas y empleado métodos para acceder a dicha información y así cometer delitos sin ser detectados.

Al analizar el Código Penal de Guatemala, Decreto 17-73 del Congreso de la República de Guatemala, dentro del apartado de delitos informáticos, contenidos en los Artículos

---

<sup>18</sup> Alvarado, José y Morales, Ronald. **Ob. Cit.** Pág. 32



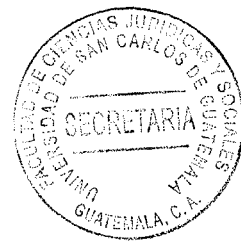
del 274 "A" al 274 "H", así como la iniciativa de ley número 4055, Ley de Delitos Informáticos y el Convenio sobre Cibercriminalidad, se encuentra dentro de su tipificación que el delincuente informático se hace valer de la aplicación de cualquier modo o cualquier medio informático para cometer el ilícito.

De tal cuenta que, cuando la ley se refiere a los diferentes modos o medios para cometer delitos informáticos se debe entender como la variedad de ataques informáticos, virus, armas cibernéticas, simulación o alteración de información, que son utilizados dentro del cibercrimen, especialmente en los bienes jurídicos y delitos estudiados en el apartado anterior de este capítulo.

De los ataques informáticos es de precisar que dentro del cibercrimen los delincuentes constantemente crean nuevas formas o tipos de ataques cibernéticos en contra de los sistemas de información. A raíz de esta problemática la Comisión de las Comunidades Europeas propuso la definición de las distintas amenazas contra los sistemas informáticos, y que son explicadas a continuación:

a) Acceso no autorizado a sistemas de información

Consiste en que el delincuente obtiene acceso no autorizado a un ordenador o red de computadoras mediante uso de información interna hasta la interceptación de contraseñas. Aunque es común, es muy poco probable que este tipo de ataque se realice con intención de realizar algún daño y que medie el fin de copiar, modificar o destruir información.



b) **Perturbación a los sistemas de información**

Este tipo de ataque, también conocido como denegación de servicio DdS, consiste en crear deficiencias o bloquear el suministro de los servicios que internet ofrece. La denegación de servicio tiene por objeto saturar los servidores de internet, o bien, sobrecargar a los proveedores de servicio de internet PSI con mensajes sin sentido de manera automática.

c) **Ejecución de programas informáticos perjudiciales que modifican o destruyen Datos**

Existe diversidad de programas informáticos perjudiciales, por una parte, algunos destinados para dañar ordenadores, mientras otros utilizan a las computadoras para dañar otros elementos de la red a las que se encuentran conectadas. En otros casos, un programa malicioso puede permanecer inhabilitado hasta que se cumpla la condición para el cual fue instalado, por ejemplo; llegar a cierta fecha, causando daños irreparables al modificar y destruir datos.

Otros programas, denominados gusanos, crean réplicas de sí mismo con el fin de inundar un sistema completo y crear daños en la información de la computadora o red local.



Además, los delincuentes informáticos comúnmente utilizan programas informáticos maliciosos denominados **virus** para eliminar información o alterar documentos informáticos con archivos ejecutables que contienen códigos capaces de inhabilitar o deshacer, intencionalmente, los datos digitales de un ordenador.

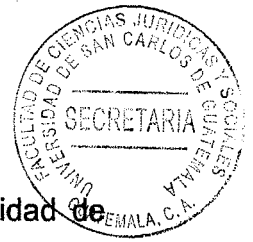
Sin embargo, algunos programas informáticos son creados para la defensa de la soberanía de los Estados en lo que se denomina batallas cibernéticas. A estos programas se les conoce como **armas cibernéticas**, y son utilizados en la defensa, ataque y la desarticulación del crimen organizado que opera a través del ciberespacio, y cuyas consecuencias impactan en la realidad de las personas.

Por último, los datos contenidos en un sistema informático o documentos físicos pueden ser objeto de **alteración o simulación**, en el entendido de que a través de la tecnología los ciberdelincuentes pueden fácilmente optar por métodos para usurpar la identidad de las personas y utilizarla de manera inadecuada, causando daños a terceros.

Entre las formas de alterar o simular información se puede analizar desde dos puntos de vista:

- a) **Objeto:** Surge cuando se modifican datos almacenados en una computadora de forma malintencionada.
- b) **Instrumento:** Consiste en falsificar documentos utilizando sistemas de cómputo o sus componentes tales como fotocopiadoras, escáner o impresoras láser.





Cabe mencionar que dentro de los métodos mencionados existen una diversidad de alternativas a las cuales puede optar un ciberdelincuente al momento de cometer ilícitos en internet. Es por ello que se ha explicado de forma general los distintos modos o medios que son utilizados dentro de las figuras delictivas que pueden ocurrir dentro de la interfaz de las plataformas digitales de videojuegos, y que han sido estudiadas con anterioridad.

Además, estos métodos se encuentran en constante cambio a medida que la tecnología avanza, por lo que no siempre serán los mismos, y mencionar cada uno de ellos de forma específica puede ser desventajoso al momento de querer encuadrar una acción en un tipo penal determinado, es por ello que la misma ley no lo regula de esa manera, a sabiendas de que estos métodos de operación criminal se encuentran en constante evolución.

#### **4.3. Propuesta de regulación de los delitos informáticos para su prevención en Guatemala**

El derecho informático es materia de estudio reciente en la ciencia del derecho y es conocido como un conjunto de leyes, normas y principios aplicables a los hechos y actos derivados del uso de la tecnología informática. Siendo los hechos efectos de un fenómeno aparejado a la informática sin que medie el actuar del ser humano y que provocan consecuencias jurídicas. Por otra parte, los actos son el efecto derivado del



uso de la informática y provocado por el ser humano que trae consigo consecuencias jurídicas.

“Las administraciones públicas se han dado cuenta de hasta qué punto la economía y los ciudadanos dependen del funcionamiento eficaz de las redes de comunicación y varias de ellas han comenzado a revisar sus disposiciones en materia de seguridad.”<sup>19</sup>

La Constitución Política de la República de Guatemala, establece que el Estado se organiza para brindar seguridad y protección a las personas. Por tal motivo, las amenazas cibernéticas que se cometen a través de la tecnología y la falta de regulación de los delitos informáticos en el derecho penal guatemalteco dejan vulnerable la seguridad jurídica de las personas ante esta nueva forma delincencial.

“Según, la Constitución Política de la República de Guatemala, la persona humana debe tener seguridad jurídica, y para lograr la consecución de ésta, el Estado debe tomar las acciones necesarias y precisas. En este caso, debe tomar una acción desde el marco jurídico-penal, para cubrir aquellos espacios generados por el desarrollo de la informática que han quedado afuera de toda regulación y que por lo tanto generan inseguridad jurídica para toda la población que cada vez depende más de la tecnología.”<sup>20</sup>

---

<sup>19</sup> Comisión Europea. **Seguridad de las redes y de la información: Propuesta para un enfoque político europeo.** Pág. 3

<sup>20</sup> Reyes, Hacid. **Seguridad Jurídica.** Pág. 555



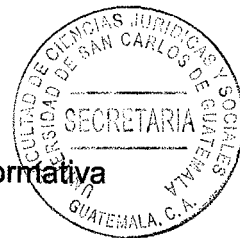
Se ha demostrado que la sociedad, con el pasar del tiempo, evoluciona en cuanto a sus formas de relacionarse, creando nuevos derechos que no se encuentran protegidos por el Código Penal y leyes especiales en la materia, sin embargo, la Constitución Política de la República de Guatemala obliga a resolver la situación de inseguridad con las acciones legales necesarias, optando por mecanismos jurídicos que contengan el mínimo de garantías para la protección de los derechos que se encuentran en peligro de ser vulnerados.

El derecho busca satisfacer las necesidades humanas lo que incluye la seguridad de las personas en el uso de la tecnología y su información almacenada en los dispositivos digitales y ciberespacio.

La tipificación de los delitos informáticos expuestos con anterioridad es de suma importancia, a consecuencia de que, junto a los avances tecnológicos en la sociedad, surgen nuevas conductas delictivas.

Por otra parte, el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala ha quedado obsoleto en la materia de delitos informáticos, ya que, con el pasar del tiempo no se ha puesto a discusión por los legisladores estas nuevas formas de criminalidad por lo que estos delitos tienden a quedar impunes en la sociedad guatemalteca.

De tal cuenta, es necesario que se actualice el derecho penal guatemalteco, a través de reformas al Código Penal, Decreto 17-73 del Congreso de la República de Guatemala,



la ratificación del Convenio sobre Cibercriminalidad o la creación de una normativa especial en la materia.

#### **4.3.1. Incorporación de los delitos informáticos al Código Penal, Decreto 17-73 del Congreso de la República de Guatemala mediante reformas**

La regulación de los delitos informáticos en Guatemala es realmente necesaria, ya que conforme la tecnología avanza surgen nuevas conductas delictivas, tal y como se ha demostrado en el presente estudio, los guatemaltecos quedan expuestos a los delitos informáticos cometidos en las plataformas digitales de videojuegos, esto derivado a que las personas pueden tener acceso a tales plataformas por medio de computadoras, tabletas digitales, *smartphone* o teléfonos celulares.

Por consiguiente, los guatemaltecos quedan expuestos a los ataques cibernéticos o virus que causan una violación a la información, datos, integridad y patrimonio de las personas; y que permitan el acceso no autorizado o perturbación a la información para posteriormente obtener un beneficio económico.

Los delitos informáticos al ser conductas de reciente descubrimiento se van desarrollando y perfeccionando con el pasar del tiempo, por lo que el derecho penal guatemalteco se puede considerar inaplicable para la época actual al no evolucionar juntamente con la tecnología.

El Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, regula los delitos informáticos por primera vez en el año de 1996; reforma y adiciona a ciertos



delitos en el año 2012 y por lo general estos delitos tienden a proteger el **software y hardware** de los sistemas de cómputo, lo cual denota que estos delitos no han sido tomados en cuenta por los legisladores para su discusión, en consecuencia los delitos informáticos que son objeto de este estudio son figuras delictivas que no se encuentran regulados en el Código Penal guatemalteco.

La Constitución Política de la República de Guatemala, en el Artículo 1 organiza al Estado para brindar seguridad a las personas, y como se hizo mención en el apartado anterior, para brindar dicha seguridad debe de optar por las acciones jurídicas viables para resolver la situación de inseguridad causada por los delitos informáticos.

De dicha cuenta, los delitos informáticos regulados en el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, no brindan la seguridad jurídica a la integridad, confidencialidad, integridad y patrimonio de los guatemaltecos.

Es por ello que se recomienda incorporar al Código Penal los delitos informáticos mediante una reforma y atendiendo al estudio de los bienes jurídicos realizado en el apartado 4.1., de la presente investigación, es permisible incorporar los siguientes delitos:

a) Acceso sin autorización

Consiste en el ingreso no autorizado a uno o varios sistemas digitales que contengan información almacenada. Dicho en otras palabras, comete este delito la persona que



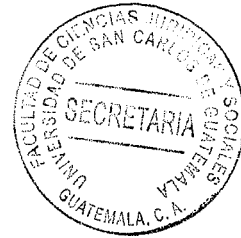
acceda a sistemas informáticos o elementos accesorios, sin previa autorización o excediendo los límites de ésta.

Este tipo de conducta puede cometerse de forma principal o accesoria. Es principal cuando la persona ingresa al sistema informático para conocer el contenido del mismo. En materia informática este sujeto recibe la denominación de *hacker* y comúnmente utilizan sus habilidades para determinar las fallas o vulnerabilidades en los sistemas, así como burlar las medidas de seguridad de los mismos. Y el acceso sin autorización es accesorio cuando la intromisión se realiza para preparar otro tipo de delito.

b) Fraude informático

Consiste en la manipulación de sistemas informáticos para la transferencia no autorizada de los activos patrimoniales en perjuicio de otro, con el fin de obtener beneficios para sí mismo o un tercero.

Algunos estudiosos del derecho consideran que no existe diferencia entre el fraude informático con el fraude o estafa. Sin embargo, se diferencia de la estafa debido a que en ella se ejerce el ardid o engaño en contra de las personas; por otra parte, el fraude informático su objetivo es engañar a los sistemas informáticos con finalidad fraudulenta.



c) Falsificación informática

Este tipo de delito consiste en copiar, alterar o sustituir, de forma ilegítima datos informáticos de los sistemas que hacen uso de tecnologías informáticas generando como consecuencia la falta de veracidad para inducir a los usuarios a brindar información personal o financiera para posteriormente obtener beneficios propios o a terceros.

d) Daño informático

El delito de daño informático procede cuando una persona, sin autorización previa, altera, destruye, inutiliza, suprime, modifica o por cualquier modo o medio, daña un sistema informático o sus componentes.

Si se observa detenidamente, este tipo de delito cuenta con varios verbos que dan sentido a este delito y para su mayor comprensión se procede a explicar:

Existe la alteración cuando ocurre un cambio, modificación o ajuste, no autorizado, de un activo digital. El destruir provoca la inutilización o la supresión permanente de un activo digital. Y el inutilizar, suprimir o modificar, hace referencia a la alteración de un activo digital que provoca que el dueño del sistema informático no pueda utilizarlo de la manera en que está previsto.



Los delitos informáticos del Código Penal carecen de seguridad jurídica para la vida de los guatemaltecos, por lo que, al implementar las conductas mencionadas, se considera que la legislación guatemalteca se vea protegida en cuanto a los bienes jurídicos que se encuentran expuestos en este tema.

Sin embargo, muchos países ya cuentan con una legislación avanzada en materia de delitos informáticos, lo que ha llevado a la creación de normas de carácter internacional, promoviendo convenios y tratados para la erradicación de esta nueva forma delincencial, siendo uno de los más importantes el Convenio Sobre Ciberdelincuencia, celebrado en Budapest en el año 2001.

#### **4.3.2. Ratificación del Convenio sobre Ciberdelincuencia**

Este convenio nace por la necesidad de aplicar una política en común a nivel internacional que procurará la protección de las personas frente a los delitos informáticos y los ciberdelincuentes. Por tal motivo y con la cooperación internacional, el 23 de noviembre del año 2001, los Estados miembros de la Unión Europea junto a su Consejo aprueban la Convención sobre la Ciberdelincuencia, también llamado Convenio de Budapest.

Este convenio regula las conductas ilícitas realizadas comúnmente por los ciberdelincuentes a nivel internacional, las cuales son: el acceso ilegal, interceptación ilegal, interferencia de los datos, interferencia de sistema, uso erróneo de dispositivos, falsificación del ordenador, fraude del ordenador, pornografía infantil. Además, contiene





normas adjetivas para preservar la información almacenada, así como los procedimientos para producir prueba en juicio.

“No obstante que el Convenio de Budapest fue celebrado a nivel del Consejo Europeo, no existe impedimento legal para que otros países, como el caso de Guatemala, puedan adherirse a dicha normativa.”<sup>21</sup>

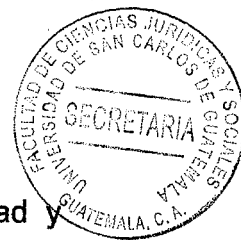
Guatemala no es parte de la Convención sobre Ciberdelincuencia, por lo que sería de suma importancia poder ratificarlo para empezar el combate de la delincuencia informática y las futuras conductas delictivas que puedan aparecer con los avances tecnológicos.

**4.3.3. Creación de un cuerpo normativo especial en materia de delitos Informáticos**

A lo largo de este estudio se ha demostrado que en la actualidad Guatemala no cuenta con una ley que regule los delitos informáticos. Así pues, atendiendo a los avances tecnológicos se puede considerar que la elaboración de una ley especial en materia de delitos informáticos se deben considerar los siguientes aspectos:

---

<sup>21</sup> Alvarado, José y Morales, Ronald. **Ob. Cit.** Pág. 12



- a) Los bienes jurídicos tutelados deben proteger la integridad, disponibilidad y confidencialidad de los usuarios de los sistemas tecnológicos de información y sus componentes con el objetivo de asegurar de manera jurídica el comercio electrónico.

Principalmente deben ir orientados a la protección de la información y el patrimonio de las personas, toda vez que existen plataformas digitales que utilizan información personal para realizar transferencias dinerarias reflejadas en monedas electrónicas.

- b) Debe optar por medidas que contrarresten los ataques informáticos que persiguen causar daño a los datos y patrimonio de los usuarios, tomando en cuenta las leyes nacionales e internacionales.

Además, esta normativa deberá de tener en claro su ámbito de aplicación, ya que en la actualidad muchos tratadistas concuerdan en que es difícil sancionar los actos que se realizan en el ciberespacio debido a que no constituye un espacio territorial o geográfico de aplicación.

“Se trata de un ambiente intangible; no es un mundo de átomos y células, sino digital. Los *bytes* no tienen peso, olor ni color y viajan a la velocidad de la luz”<sup>22</sup>

---

<sup>22</sup> Goodman Mar, *Cibercriminalidad*. Pág. 8



En este tipo de normativas lo que toma relevancia es determinar el lugar donde se crea y donde se producen las consecuencias jurídicas de los hechos o actos delictivos, por tanto, estos lugares constituyen un espacio territorial en el cual si existen normas emanadas por un Estado a través de su órgano legislativo.

Debido a la complejidad para determinar el ámbito de aplicación de la ley se debe de tomar en consideración los siguientes criterios aplicables a delitos informáticos:

- a) Si, el sujeto activo se encuentra dentro del territorio nacional y realiza actos delictivos derivado del uso de herramientas tecnológicas indistintamente del lugar en el cual recaen sus efectos.
- b) Si el sujeto activo se encuentra fuera del territorio nacional y sus acciones delictivas derivadas del uso de las herramientas tecnológicas surten efectos en el territorio nacional.
- c) Cuando el sujeto activo se encuentra fuera del lugar donde surten efectos del delito y de las herramientas tecnológicas que utilizó para realizar tales actos.

En todo caso deberán ser los peritos y expertos en colaboración de los proveedores de internet, con autorización de juez competente, los obligados en determinar el lugar físico donde se originó la acción delictiva.

Estas han sido algunas de las recomendaciones que organismos internacionales como la Organización de los Estados Americanos O.E.A., la División sobre Aplicaciones TIC y Ciberseguridad, de la Unión Internacional de



Telecomunicaciones U.I.T.; aportaron para el combate de los delitos informáticos y que han sido de mucha ayuda al momento de crear leyes ordinarias de distintos países del mundo.

Es evidente que el Código Penal, Decreto 17-73, del Congreso de la República de Guatemala, carece de eficiencia en cuanto a la regulación de delitos informáticos, esto derivado de la falta de equilibrio entre la ley y las nuevas tecnologías, lo que imposibilita una armonía en la realidad de los ciudadanos guatemaltecos que dependen de las plataformas digitales para ejercer sus actividades cotidianas.

De lo anterior, cabe destacar que es necesario e inminente que se tipifiquen los delitos informáticos a fin de otorgar seguridad jurídica a los habitantes de la república de Guatemala de las acciones ilícitas que cometen los ciberdelincuentes.

Por consiguiente, es necesario adicionar los delitos informáticos estudiados en los apartados anteriores, al Código Penal por medio de una reforma; tomar en cuenta la incorporación de la Convención sobre Cibercriminalidad al ordenamiento jurídico de Guatemala; o bien, crear una norma especial en la materia.

Estas medidas deben aplicarse a la brevedad posible, tomando en cuenta las recomendaciones planteadas y la celeridad con que evoluciona la tecnología, con el fin de evitar vacíos legales en el futuro de los ciudadanos.





## CONCLUSIÓN DISCURSIVA

La problemática objeto de estudio radica en la impunidad de los delitos que se comenten por medio de las plataformas digitales de videojuegos por la falta de elementos que permitan la tipificación de estas conductas ilícitas.

Actualmente, son varios los delitos cometidos mediante las plataformas digitales de los videojuegos, entre ellos podemos mencionar los siguientes: robo de bienes, falsificación de elementos y daño informático los que causan agravio a los bienes jurídicos de integridad, disponibilidad, confidencialidad y patrimonio de los usuarios de dichas plataformas.

Además, el atraso legal del derecho penal en materia de delitos informáticos se debe a la falta de interés de los diputados al Congreso de la República de Guatemala, por lo que, es obligación del Estado hacer uso de su poder punitivo y actualizar la legislación mediante reformas al Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, creando una ley especial en la materia o adherirse al Convenio sobre Cibercriminalidad. Sin embargo, la norma que se encamine a regular los delitos informáticos debe encaminarse a la protección de los bienes jurídicos mencionados con anterioridad, así como definir las medidas que contrarresten los ataques informáticos y; el ámbito de aplicación de la ley atendiendo a los criterios expuestos por la División sobre Aplicaciones de Tecnología de la Información y Comunicación TIC y Ciberseguridad, de la Unión Internacional de Telecomunicaciones U.I.T.

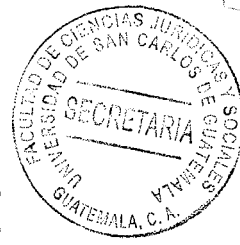




## BIBLIOGRAFÍA

- ACURIO DEL PINO, Santiago. **Delitos Informáticos: Generalidades.**  
<http://www.oas.org/juridico/spanish/cybecu.htm>.
- ALVARADO, Rolando y MORALES, Ronald. **Ciber Crimen.** Guatemala: Ed. Ius Ediciones, 2012.
- AMUCHALEGUI REQUENA, Irma Gabriela. **Derecho Penal. Colección de Textos Jurídicos Universitarios.** México. Ed. Harla, 1999.
- CABANELLAS, Guillermo. **Diccionario de Derecho Usual.** Buenos Aires, Argentina: Ed. Heliasta, 26<sup>a</sup>. ed., 1999.
- Comisión Europea. **Seguridad de las redes y de la información: Propuesta para un enfoque político europeo.** Estocolmo, 2006.
- Es ET NOD 32 <https://www.welivesecurity.com/la-es/2014/08/26/videojuegos-blanco-para-crimen/> (Consultada: 27 de octubre de 2020)
- GOODMAN, Marc. **Cibercriminalidad.** México, Ed. Instituto Nacional de Ciencias Penales, 7<sup>a</sup>. ed., 2003
- [https://as.com/esports/2016/09/16/portada/1473981525\\_248613.html](https://as.com/esports/2016/09/16/portada/1473981525_248613.html).  
(Consultada: 25 de septiembre de 2020)
- <https://gestion.pe/tecnología/siete-caracteristicas-identificar-ciberdelincuente-122640-noticia/> Consultado el 08/06/2020
- JIMÉNEZ DE ASÚA, Luís. **Lecciones de Derecho Penal.** México. Ed. Mexicana, 2<sup>a</sup>. ed., 1997.
- LIMA MALVIDO, María de la Luz. **Delitos Electrónicos.** México. Academia Mexicana de Ciencias Penales. Ed. Porrúa, 1984.
- Prensa Libre <https://www.prensalibre.com/vida/tecnologia/asi-son-los-gamers-profesionales-y-el-fenomeno-de-los-esports/> (Consultada: 30 de agosto de 2020)





Prensa Libre. [https://www.prensalibre.com / vida / tecnología /campeonato-centroamericano-esports-gamers/](https://www.prensalibre.com/vida/tecnologia/campeonato-centroamericano-esports-gamers/) (Consultada: 07 de septiembre de 2020)

RESA NESTARES, Carlos. **Crimen Organizado Transnacional: Definiciones, Causas y Consecuencias.** Argentina. Ed. Astrea, 2005.

REYES, Hacid. **Seguridad Jurídica.** México. Ed. Temis, 1999.

TÉLLEZ VALDÉS, Julio. **Delitos Informáticos y el Derecho Penal Informático.** México. Ed. Mc Graw Hill Interamericana, 3ª. ed., 1996.

**Legislación:**

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

**Código Penal.** Decreto número 17-73 del Congreso de la República de Guatemala.

**Código Civil.** Enrique Peralta Azurdia. Decreto Ley 106. 1963.

**Convenio sobre Ciberdelincuencia.** Consejo de Europa. Budapest. 2001

**Iniciativa 4055,** Ley de delitos informáticos. Guatemala. 2008

**Ley para el reconocimiento de las comunicaciones y firmas electrónicas.** Decreto 47-2008 del Congreso de la República de Guatemala.