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

INCUMPLIMIENTO DEL ESTADO, DE BRINDAR SEGURIDAD, AL SER INCAPAZ DE ERRADICAR DELITOS QUE SE COMETEN EN EL ANONIMATO DE PERFILES FALSOS DE REDES SOCIALES

MELISSA ALEJANDRA ESTRADA MARROQUÍN

GUATEMALA, MAYO DE 2022

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

INCUMPLIMIENTO DEL ESTADO, DE BRINDAR SEGURIDAD, AL SER INCAPAZ DE ERRADICAR DELITOS QUE SE COMETEN EN EL ANONIMATO DE PERFILES FALSOS DE REDES SOCIALES

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

por

MELISSA ALEJANDRA ESTRADA MARROQUÍN

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, mayo de 2022

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

DECANO:	MSc.	Henry Manuel Arriaga Contreras
VOCAL I:	Licda.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic.	Rodolfo Barahona Jácome
VOCAL III:	Lic.	Helmer Rolando Reyes García
VOCAL IV:	Br.	Javier Eduardo Sarmiento Cabrera
VOCAL V:	Br.	Gustavo Adolfo Oroxom Aguilar
SECRETARIA:	Licda.	Evelyn Johanna Chévez Juárez

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Lic.	Magbis Mardoqueo Méndez López
Vocal:	Lic.	Sergio Danilo Conde Cardoza
Secretario:	Lic.	Manuel Roberto García del Cid

Segunda Fase:

Presidente:	Licda.	Sandra Marilena Aquino González
Vocal:	Lic.	Ignacio Blanco Ardón
Secretario:	Licda.	Ileana Noemí Villatoro Fernández

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

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

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

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 29 de mayo de 2020.

Atentamente pase al (a) Profesional, **FRANCISCO JOSE CETINA RAMIREZ**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **MELISSA ALEJANDRA ESTRADA MARROQUÍN**, con carné **201032333**, intitulado **REDES SOCIALES, MADRIGUERA DE DELITOS EN EL ANONIMATO Y LA FALSIFICACIÓN DE PERFILES, QUE CASI SIEMPRE QUEDAN IMPUNE.**

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

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

Fecha de recepción 29 / 05 / 2020. f) **Lic. Francisco José Cetina Ramírez**
Abogado y Notario
Asesor(a)
(Firma y Sello)

Licenciado Francisco José Cetina Ramírez
Abogado y Notario
Colegiado: No. 13776

Guatemala, 28 de julio de 2021

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

JURIDICAS Y SOCIALES
RECIBIDO
27 SET. 2021
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Doctor:
Carlos Ebertito Herrera Recinos
Jefe de Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

Distinguido doctor Herrera:

Atentamente me dirijo a usted para darle cumplimiento a la providencia de fecha 29 de mayo de 2020, por medio de la cual fui nombrado ASESOR de tesis de la bachiller MELISSA ALEJANDRA ESTRADA MARROQUÍN, titulada: "REDES SOCIALES, MADRIGUERA DE DELITOS EN EL ANONIMATO Y LA FALSIFICACIÓN DE PERFILES, QUE CASI SIEMPRE QUEDAN IMPUNE". Analizando con la estudiante la conveniencia de modificar el título, el mismo queda de la siguiente manera: "INCUMPLIMIENTO DEL ESTADO, DE BRINDAR SEGURIDAD, AL SER INCAPAZ DE ERRADICAR DELITOS QUE SE COMETEN EN EL ANONIMATO DE PERFILES FALSOS DE REDES SOCIALES ".

En cumplimiento de esta designación, he brindado la orientación requerida y se ha asesorado el tema con la debida acuciosidad, dando como resultado que: el desarrollo del trabajo de tesis, denota una investigación y estudios completos, su contenido científico y técnico de tesis, cumple con los requisitos del método científico de las ciencias sociales; a través de éste, se hacen observaciones; en cuanto a las técnicas empleadas, éstas tienen como objetivo exponer propuestas que se realizaron para llegar a resolver el problema a través de los pasos establecidos previamente, utilizando la recolección de datos, tales como: libros, diccionarios, la exposición de doctrina en páginas Web y ejerciendo el cronograma de actividades planteado en el plan de investigación.

La metodología y las técnicas de investigación que se han utilizado, se desarrollaron a través de un análisis crítico y descriptivo del contenido de la presente tesis y la realización de síntesis y deducciones para generar la conclusión discursiva; de manera que se utilizó el análisis de diversas leyes, doctrinas y la información de páginas de internet, que se relacionan con el tema investigado; todo ello, con el fin de llegar a la conclusión discursiva de que se deben buscar soluciones al problema señalado.

La redacción utilizada por la estudiante, es la correcta; apegándose a los requisitos de las normas mínimas establecidas en el Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales, y del Examen General Público.

La contribución científica de las ciencias sociales, son las normas, principios, fuentes y doctrinas; en donde la bachiller hace sus propias aportaciones, para comprobar y llegar a

cumplir con los objetivos planteados. La conclusión discursiva, resume los resultados obtenidos y sugerencias; en la cual se da la importancia del estudio sobre algo tan valioso como lo es la solución al problema; dándole la consideración que amerita al ser estudiada, haciendo notar la necesidad de que se controle el problema señalado. La bibliografía consultada se extrajo de fuentes de autores nacionales e internacionales, así como páginas del internet.

En síntesis, el contenido del trabajo de tesis, se ajusta a las exigencias científicas y técnicas que se deben cumplir, de conformidad con la normativa respectiva; la metodología y técnicas de investigación utilizadas, la redacción, la conclusión discursiva, bibliografía utilizada son congruentes con los temas desarrollados dentro de la investigación.

Indico que, no me une parentesco alguno con la bachiller. En tal virtud emito DICTAMEN FAVORABLE al referido trabajo de tesis, a efecto de que continúe con el trámite respectivo, ya que el estudio desarrollado cumple con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis y de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.
Atentamente,

Lic. Francisco José Cetina Ramírez
Colegiado No. 13776

Lic. Francisco José Cetina Ramirez
Abogado y Notario

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 27 de septiembre de 2021.

Atentamente pase a Consejero de Comisión de Estilo, FREDY ROBERTO ORELLANA MARTÍNEZ, para que proceda a revisar el trabajo de tesis del (a) estudiante MELISSA ALEJANDRA ESTRADA MARROQUÍN, con carné número 201032333, intitulado INCUMPLIMIENTO DEL ESTADO, DE BRINDAR SEGURIDAD, AL SER INCAPAZ DE ERRADICAR DELITOS QUE SE COMETEN EN EL ANONIMATO DE PERFILES FALSOS DE REDES SOCIALES
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 Ciencias Jurídica y Sociales y del Examen General Público.

"ID Y ENSED A TODOS"

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

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

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

Guatemala, 30 de octubre de 2021.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
30 OCT. 2021
UNIDAD DE ASESORÍA DE TESIS
Hora:
Firma:

Dr. Carlos Ebertito Herrera Recinos
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala.

De manera atenta le informo que fui consejero de estilo de la tesis titulada: "INCUMPLIMIENTO DEL ESTADO, DE BRINDAR SEGURIDAD, AL SER INCAPAZ DE ERRADICAR DELITOS QUE SE COMETEN EN EL ANONIMATO DE PERFILES FALSOS DE REDES SOCIALES ", realizada por la bachiller: MELISSA ALEJANDRA ESTRADA MARROQUÍN, para obtener el grado académico de licenciada en Ciencias Jurídicas y Sociales.

La alumna cumplió con todas las observaciones, que le sugiriera, por lo que dictamino de manera FAVORABLE, por lo que el trámite de orden de impresión puede continuar.

ID Y ENSEÑAD A TODOS

Lic. Roberto Fredy Orellana Martínez
Consejero de Comisión de Estilo

Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala. Ciudad de Guatemala, cuatro de abril de dos mil veintidos.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante MELISSA ALEJANDRA ESTRADA MARROQUÍN, titulado INCUMPLIMIENTO DEL ESTADO, DE BRINDAR SEGURIDAD, AL SER INCAPAZ DE ERRADICAR DELITOS QUE SE COMETEN EN EL ANONIMATO DE PERFILES FALSOS DE REDES SOCIALES. 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: Por darme la sabiduría necesaria, guiarme a lo largo de mi existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

A MIS PADRES: Fredy Rodolfo Estrada Hernández y Flor de María Marroquín Rodríguez, quienes con su apoyo incondicional fueron mi fortaleza durante todo este proceso, para seguir adelante, aprendiendo a ser perseverante para cumplir mis sueños, a quienes dedico este triunfo.

A MI ABUELA: Marta Julia Hernández Chicas, a quien la recuerdo todos los días de mi vida, por haber sido como una segunda madre, por guiarme en los caminos de Dios y hacer de mi una persona de bien.

A MIS HERMANOS: A quienes a pesar de cualquier circunstancia, estuvieron de alguna u otra manera pendientes en este proceso de estudio, a quienes les dedico también este triunfo.

A MIS AMIGOS: En general por el apoyo brindado y sus buenos deseos en la evolución de este proyecto; cada uno en su propio estilo; así también mi sincero agradecimiento especialmente a Diego Alejandro Vargas Morales, a quien agradezco su apoyo incondicional durante todo este proceso, por ser la fuente de motivación e inspiración en superarme cada día más.

A TODOS MIS FAMILIARES: A mis tíos, tías, primos, sobrinos; por su apoyo incondicional.

A: Guatemala, mi patria; a la que podré contribuir en su desarrollo y prosperidad.

A: La Facultad de Ciencias Jurídicas y Sociales; por abrirme sus puertas y permitirme iniciar los conocimientos, aptitud, carácter y valores para actuar con apego a la ética y a la moral profesional.

PRESENTACIÓN

Dado que, los usuarios de las redes sociales exhíben no solo sus datos de contacto o información profesional como formación, experiencia laboral; se exponen de manera pública las vivencias, gustos, ideología y experiencias del usuario, lo que conlleva a que, un gran número de datos de carácter personal estén a disposición del público. Asimismo, se tratan informes especialmente protegidos, lo que supone un mayor nivel de riesgo para la protección de dichos datos personales y, por ende, del ámbito de la privacidad e intimidad de los usuarios.

Este estudio corresponde a las ramas del derecho: informático, penal y procesal penal. El período en que se desarrolla la investigación es de marzo de 2020 a octubre de 2021. Es de tipo cualitativo. El sujeto de estudio fueron las redes sociales; y, el objeto de estudio, los delitos que se cometen utilizando las redes sociales, convierte a las redes sociales en medio para delinquir.

Concluyendo con el aporte científico de que el Estado, con el fin de que cumpla con la obligación de velar por la la seguridad y la vida de los ciudadanos, tal y como se le encomienda en la Constitución Política de la República, cree mecanismos para enfrentar la prolifereción de delitos informáticos.

HIPÓTESIS

Las redes sociales han permitido grandes avances, principalmente en relación a la comunicación. Sin embargo, en muchas ocasiones, se han convertido en oportunidades para que personas inescrupulosas las utilicen como escondite para cometer delitos que, en su mayoría quedan impune, debido a las limitantes que se presentan al momento de investigar la identidad de quienes cometen estos hechos; siendo esto, motivo de múltiples perfiles falsos que pueden ser creados por una misma persona con fines delictivos. El Estado de Guatemala tiene la obligación de velar por los derechos y garantías de los guatemaltecos, teniendo presente que para dicha protección, debe ser aprobada una serie de normas que permita proteger de mejor manera a los guatemaltecos, en cuanto a la utilización de las redes sociales. Muchos casos de delincuencia informática viene de las cárceles, por lo que se debe limitar el uso de tecnología dentro del sistema penitenciario, ya que esto se convierte en una fuente de oportunidades para cometer delitos, siendo principalmente uno de ellos, la extorsión, aunque no es el único.

COMPROBACIÓN DE LA HIPÓTESIS

Durante la elaboración de esta investigación se lograron comprobar los factores que generan el impacto en los derechos y garantías de los guatemaltecos, en cuanto a la vulneración a los mismos mediante las redes sociales, principalmente considerados como delitos informáticos; siendo estos una tendencia, tomando en cuenta el crecimiento de las redes sociales y su mala utilización por parte de personas inescrupulosas. Teniendo presente que, existe la necesidad de la implementación de procedimientos y estrategias por parte del Estado, que permitan el mejoramiento de las condiciones y aplicación de normas para los guatemaltecos dentro de la utilización de las redes sociales, con la implementación de herramientas indispensables para que el ente investigador, cumpla con su trabajo; formalizando una división que atienda delitos informáticos, con el fin de proteger los derechos y garantías de los guatemaltecos, ya que los delitos informáticos son una tendencia mundial.

Entre los métodos que se emplearon para la validación de la hipótesis formulada, están: el analítico, el deductivo e inductivo y el dialéctico para la elaboración de razonamientos que sustentaron los aspectos científicos y jurídicos. Con lo que se pudo ampliar el conocimiento y perspectiva del tema en estudio. Asimismo, las técnicas de investigación documental, bibliográfica y de campo

ÍNDICE

Pág.

Pág.

CAPÍTULO IV

INTRODUCCIÓN

En esta tesis, se realizó un análisis acerca de cómo las redes sociales se convierten en medios por los cuales se cometen delitos en el anonimato y falsificación de perfiles, que casi siempre quedan impune; teniendo presente la necesidad de la búsqueda del respeto a los derechos y garantías inherentes al ser humano, provistas por la Constitución Política de la República de Guatemala.

Claramente existe la necesidad de que, el Estado proteja los derechos de los guatemaltecos, a través de normas que regulen de mejor manera el uso de las redes; siendo esto de mucha importancia, debido al surgimiento de delitos informáticos que vulneran la integridad de muchos ciudadanos.

Se realizó un estudio acerca de las responsabilidades del Estado, y de la protección de las garantías de los guatemaltecos; principalmente a través del derecho penal, entendiéndose los delitos informáticos y sus principios; para con esto encontrar la manera más clara y efectiva de proteger los derechos de los guatemaltecos.

El objetivo general trazado para este trabajo fue: evidenciar la vulneración de los derechos de los guatemaltecos, a través de las redes sociales, principalmente por medio de perfiles falsos que son utilizados por los delincuentes, con el fin de quedar realizar cualquier acto delincuencial sin ser erradicados.

En cuanto al contenido del trabajo de tesis, se encuentra dividido en cuatro capítulos; en el primero se trató el derecho penal guatemalteco, teniendo presente su origen, naturaleza y la división del mismo; en el segundo se estudiaron las generalidades del

delito informático, en cuanto a su definición, delimitación, organización y clasificación; en el tercero, los principios del delito informático, analizando el principio de legalidad y el principio de reserva legal; y, por último, en el cuarto capítulo, se llevó a cabo un análisis jurídico de las redes sociales y como se convierten en medios utilizados por delincuentes para cometer todo tipo de delitos, quedando impunes detrás de perfiles falsos.

El beneficio que trajo la tecnología es evidente; pero también puede ser madriguera de delitos que quedan impune, en Guatemala, debido a que, el ente investigador no cuenta con herramientas necesarias para poder afrontar este tipo de delitos.

Asimismo, para alcanzar del objetivos trazados, fue necesario implementar el método analítico, para plantear los elementos jurídicos, administrativos y sociales que afectan el desarrollo de los procesos jurídicos, dentro de los procesos penales específicamente, para regular el uso de las redes sociales y evitar delitos informáticos. Cabe mencionar también, los métodos: analítico, sintético, deductivo e inductivo. Asimiasmo, las técnicas documental y las fichas bibliográficas, con las cuales se recolectó información suficiente y de actualidad.

Asimismo, al finalizar esta investigación se podrán tener conceptos claros, respecto a lo que engloba la responsabilidad del Estado ante la provisión de todos los elementos necesarios para proteger a los guatemaltecos y sus derechos básicos dentro de los procesos que busquen sancionar o determinar una acción cometida por delincuentes que utilizan las redes sociales, como herramienta para delinquir libremente.

CAPÍTULO I

1. Derecho penal guatemalteco

Para alcanzar los objetivos de la investigación es necesario iniciar analizando el elemento más básico, como lo es en este caso el derecho penal en Guatemala, ya que este será de mucha importancia para entender la procedencia de los delitos informáticos que se presentan dentro de las redes sociales.

De tal manera es necesario analizarlo para entender la manera correcta en que debe procederse con el fin de erradicar o prevenir este tipo de delitos, siendo muy importante el evitar la impunidad y que las redes sociales se conviertan en una plataforma que permita el abuso de los delincuentes.

De esta manera es necesario establecer conceptos claros y específicos del mismo para de esta manera tener la capacidad de obtener conclusiones de forma objetiva, por lo que se debe entender a fondo el derecho penal, y observar que esta disciplina ha recibido distintas denominaciones.

En Francia, se le llamó *drot pénal y droit criminal,* en tanto que en España y los países del continente americano se le denomina finalmente como derecho penal, asimismo en Alemania se le denominaba como Peinliches Recht, sin embargo, posteriormente se llamaron *Kriminalrcht.*

Asimismo, en Italia se empleó la expresión Diritto Penale, aunque los positivistas prefirieron llamarle *Dirrito Criminale*, para desterrar la palabra pena, y como bien es sabido, estas las reemplazan por la de sanción.

De esta manera, es necesario tener presente que cuando se define el derecho penal en su forma más simple, se encuentran una serie muy amplia de conceptos que tratan de darle una definición clara.

Sin embargo, de acuerdo con autores importantes, es posible decir que toda definición es un silogismo que, si bien plantea correctamente los problemas, los resuelve luego tautológicamente, así pues, las definiciones que se han dado respecto a esta disciplina son diversas, de carácter subjetivo, unas, y de índole objetiva, las otras.

Pertenecen al primer grupo las que ofrecen los autores como Luis Jiménez de Asua en su libro sobre la Ley y el delito, de la misma manera nos menciona a Berner y Brusa: "para quienes la consideran como la ciencia que funda y determina el ejercicio del poder punitivo del Estado". Lo cual muestra claramente la posición del autor.

Se menciona que, el estudio del delincuente y de las medidas asegurativas amplió el concepto de esta rama jurídica, indicando a su vez que Alimena menciona aquél y Mayer habla de estas últimas, incluyendo en su definición los otros medios de lucha contra el crimen. Asimismo, es preciso mencionar que se le pone una coletilla a la definición del derecho penal, "en que sólo habla de pena, para comprender otras medidas que tienen

por fin prevenir los delitos."[1]

De esta manera, se puede considerar también lo siguiente: "Derecho penal es el conjunto de normas y disposiciones jurídicas que regulan el ejercicio del poder sancionador y preventivo del Estado, estableciendo el concepto del delito como presupuesto de la acción estatal, así como la responsabilidad del sujeto activo, y asociando a la infracción de la norma una pena finalista o una medida aseguradora".[2]

Debe tomarse en cuenta que los puntos de vista con respecto al derecho penal pueden variar según las personas o las corrientes de pensamiento desde donde se evalúe esta disciplina. De los cuales se pueden mencionar:

a) El *ius puniendi*: De acuerdo con este punto de vista, es frecuente leer en tratados de derecho que éste se divide en subjetivo y objetivo. El primero consiste en la facultad de hacer o no hacer una cosa; el segundo es Ley, regla o norma que manda, que permite o que prohíbe.

Así como en el derecho penal objetivo, el centro de la preocupación académica gira en torno a la sistematización de las normas jurídico-penales, en el caso del derecho penal subjetivo es la potestad punitiva del Estado.

El derecho penal objetivo es el *ius poenale,* el derecho penal subjetivo es la potestad

[1] Jiménez de Asúa, Luis. **La ley y el delito. Principios de derecho penal**. Pág. 18
[2] **Ibíd**.

punitiva del Estado. Para algunos, el *ius poenale* es una emanación del *ius puniendi* para otros ha sido todo lo contrario. Negar la existencia de un derecho subjetivo de castigar del Estado es cerrarse el camino para entender los fundamentos de todo el sistema del derecho penal.

De este modo, se entiende que durante mucho tiempo y quizá por efecto del gran desarrollo de la teoría del delito se produjo una gran despreocupación por este tema, lo que llevó a decir que constituía un recuerdo histórico, pero pasado el entusiasmo por la teoría del delito, o bien porque reducido el análisis sólo a ella había límites y contradicciones insalvables, los juristas han vuelto a colocar su atención en la pena y en la potestad del Estado de carácter punitivo. En suma, el derecho penal subjetivo o *ius puniendi* se puede definir como: "la potestad penal del Estado de declarar punibles determinados hechos a los que impone penas o medidas de seguridad".[3]

Es entonces expresión del poder único y exclusivo del Estado para ejercer la violencia legítima, de tal manera claramente debe mencionarse que la violencia penal no es sino un aspecto de aquélla.

Ahora bien, de por sí implica un orden jurídico positivo, esto es, que el Estado es una organización surgida de los hombres y para los hombres; por tanto, cuando se plantea el problema del derecho natural, aunque haya autores que así lo hagan o períodos de la historia en que esto fue lo preponderante.

[3] Bustos Ramírez, Juan. **Manual de derecho penal. parte general**. Pág. 39

Es derecho penal subjetivo el *ius puniendi*, que resulta limitado por las propias leyes que los Estados dictan. Esto es así en garantía de la libertad, ya que las actividades estatales han quedado, por lo mismo, concretadas a lo que la ley establece. Originalmente, el poder punitivo del Estado, era considerado como un poder derivado de la soberanía del Estado. En virtud de este poder, el Estado dicta leyes penales, organiza el sistema judicial, condena y ejecuta las sanciones.

El *ius puniendi* aparece, por tanto, como la fuente del derecho penal objetivo, ahora bien, bajo la influencia del liberalismo político y del positivismo jurídico, esta concepción fue, por tanto, abandonada.

El poder del Estado se consideró como fundado en las normas legales, las misma que justifican su pretensión para reprimir a las personas. Así mismo, el derecho a castigar sería un derecho subjetivo basado en la relación existente entre el Estado y el delincuente.

Este criterio, que recuerda a la noción de derechos subjetivos del derecho privado, no es satisfactorio, ya que el poder punitivo del Estado no puede ser explicado como una prerrogativa derivada del conjunto de las disposiciones penales que el mismo Estado dicta.

La noción de derecho penal subjetivo, entendida de esta manera, resulta incorrecta e inútil. Lo cual no se trata de un derecho subjetivo del Estado para castigar, poder que está limitado por sus fundamentos mismos y por la Constitución Política de la República de Guatemala, sobre todo en las disposiciones referentes a la organización del Estado y a

los derechos fundamentales.

b) El *ius poenale*: Desde un punto de vista objetivo, es decir, como sistema normativo, o bien, subjetivo, como potestad del Estado. El derecho penal objetivo se puede definir: "como aquella parte del ordenamiento jurídico que determina las características del hecho delictivo e individualiza al sujeto que lo realizó, al que le impone por su hecho una pena y/o medidas de seguridad".[4]

El derecho penal objetivo tiene pues una finalidad de carácter sistemático, es decir, dar un desarrollo y explicación coherentes y racionales, con pretensión de validez universal, a las reglas jurídicas referidas al delito, al sujeto responsable y a las penas y medidas de seguridad.

De ahí que uno de los aspectos básicos del derecho penal sea el referido a su estructura normativa, esto es, a la naturaleza y carácter de las reglas jurídicas que lo componen.

Por lo tanto, se puede decir también en sentido objetivo, "el derecho penal es un conjunto de normas jurídicas, estatuidas por el órgano constitucionalmente competente; en las que se prevén, de un lado los comportamientos incriminados como delictuosos y, de otro, las sanciones en tanto consecuencias jurídicas de dichas acciones".[5]

---

[4] Bustos Ramírez, **Op. Cit**. Pág. 5
[5] Hurtado Pozo, José. **Nociones básicas de derecho penal**. Pág. 1

"El derecho penal objetivo puede definirse como el conjunto de normas estatales referente a los delitos, las penas y otras medidas preventivas o preparatorias que son su consecuencia. Las normas jurídicas penales son siempre una respuesta a la cuestión ya indicada anteriormente, de la convivencia de los seres humanos y su consecuencia cuando esta convivencia genera actitudes u omisiones lesivas de los bienes jurídicos".[6]

Es necesario tener presente que cuando se menciona la objetividad del derecho penal, se está haciendo alusión directamente a la parte más intrínseca de esta rama del derecho.

1.1. Origen y naturaleza

El derecho penal, se puede definir principalmente como un conjunto dentro de las ciencias jurídicas en general, que estudia y define las normas penales, así como los elementos integrantes de las mismas.

Como también, los conceptos científicos sobre tales normas, la sanción, la responsabilidad y conceptos específicos como el delito, el delincuente y la pena. Se integra así la ciencia del derecho penal.

Claramente el derecho penal como ciencia estudia la teoría del delito, la Teoría de la Ley Penal y la Teoría de la Pena y de las medidas de seguridad, ahora bien, como ordenamiento jurídico, es decir como ley.

---

[6] De León Velasco, Héctor Aníbal. **Resúmenes de derecho penal**. Pág. 9

Por lo tanto, principalmente se menciona que contiene aquellas teorías hechas normas y plasmadas en ley en una parte general, descriptiva de aspectos generales a que se refiere la ley penal.

Y finalmente el derecho penal principalmente contiene una parte especial en donde se definen las conductas delictivas, los tipos penales y la punibilidad que ha de asociarse a ellos.

De tal manera que, para hablar de la naturaleza jurídica del derecho penal, hay que referirse a sus características, las cuales únicamente se enumeran toda vez que serán tratadas en apartado especial y son las que definen la misma, las cuales son:

a) Tiene carácter positivo;
b) Pertenece al derecho público;
c) Valorativo y finalista; y
d) Sancionador.

La división del derecho penal y entender cuáles son las partes del mismo, ya que según la manera cómo se estructuran los códigos penales modernos, se distingue el derecho penal general del derecho penal especial.

El primero está limitado a los ámbitos de la aplicación de la ley penal, define los elementos esenciales del delito y determina los límites y el tipo de las sanciones penales, el derecho penal especial describe los actos delictuosos e indica la pena que debe imponerse al

responsable.

El estudio de la parte general está muy desarrollado y la teoría del delito constituye un ejemplo del refinamiento dogmático alcanzado, ahora en cuanto al derecho penal especial es de lamentar la falta de análisis sistemáticos orientados a integrar o completar los tipos legales mediante la elaboración de principios o de criterios generales.

Si bien, por razones esencialmente prácticas y de técnica legislativa se justifica esta distinción, es de señalar que las disposiciones de la parte general y de la parte especial de los códigos penales modernos se encuentran estrechamente relacionadas, tanto en el plano teórico como en su aplicación concreta.

Se demuestra sencillamente citando los Artículos 11 y 12 del Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, en los que se definen los delitos dolosos y culposos, respectivamente.

Ahora bien, en la segunda disposición, se señala de manera explícita que los hechos culposos son punibles en los casos expresamente determinados por la ley. Lo que significa, a contrario sensu, que no es necesario que se mencione, en cada disposición de la parte especial, la intención; ya que los delitos previstos son reprimidos sólo cuando son dolosos y, excepcionalmente a título de culpa. El derecho penal para su estudio comprende en su parte general:

a) Teoría de ley penal;

b) Teoría del delito; y,

c) Teoría de la pena y las medidas de seguridad.

Asimismo, en su parte especial, contiene:

a) Delitos en particular;

b) Penas y medidas de seguridad aplicables a los casos concretos; y,

c) Las faltas.

1.2. División del derecho penal guatemalteco

Este derecho fundamental precisa de un conjunto de normas jurídicas que disciplinan su aplicación en la práctica, y este nuevo organismo ha recibido el nombre de derecho penal procesal que vive en el cuadro general de las normas para que el otro pueda tener perfecta y exacta cristalización.

La técnica moderna tiende a la perfecta delimitación de ambas ramas jurídicas y hacerlas regir por principios diferentes. Esta exacta delimitación, sin embargo, no es posible en muchos aspectos lograrla. Es necesario entender que éste se divide en diversas ramas o subsecciones, por lo que el derecho penal sustantivo es el derecho penal strictu sensu, llamado también, derecho penal material.

Esto singularmente debido a la gran etapa histórica en que ambos derechos permanecieron unidos, sabido es, en efecto, que los grandes cuerpos legales históricos

disciplinaron conjuntamente ambas ramas jurídicas.

Por lo tanto, esta etapa larga de vida común ha hecho que, aunque en los tiempos modernos se tienda a lograr una perfecta separación, todavía aparezcan en una rama preceptos legales que propiamente pertenecen a la otra. De tal manera, se debe tomar en cuenta las diferentes ramas del derecho penal, dentro de las cuales se encuentran:

a) Disciplinario: Se necesita distinguir el propio derecho penal del llamado derecho penal disciplinario, sobre el que tanto se teoriza en los tiempos modernos, los autores han tratado de perfilar bien las diferencias existentes entre uno y otro, por lo que es posible mencionar que se comenzó hablando, en efecto, del diverso fin que mueve a uno y a otro, pues mientras que en el derecho penal común se tiende al restablecimiento del orden jurídico de carácter general.

En el derecho disciplinario única y exclusivamente se tiende, como su nombre lo indica, a mantener la disciplina, la observancia de las normas específicas que afectan a un determinado sector de personas o instituciones.

Con el paso del tiempo se fueron añadiendo otras notas de mayor alcance, como es la diferente naturaleza de que se componen unas y otras normas, pues mientras las normas del derecho penal común describen tipos delictivos o figuras específicas de conductas delictivas.

De esta forma, se toman claramente a las normas del derecho penal disciplinario que

tienen sólo en cuenta preceptos de carácter general que dejan, amplio campo para la resolución del asunto.

El derecho penal disciplinario puede verse de la siguiente manera: Primero, en la actividad del Estado cuando aplica penas no criminales. Es el derecho disciplinario por excelencia y su distinta naturaleza del derecho penal común.

Continuando con la actividad de determinados organismos cuando sancionan hechos que afectan a su constitución y funcionamiento. Un ejemplo típico de este derecho penal disciplinario son las sanciones académicas para el mantenimiento de la disciplina universitaria.

De esta manera, en el llamado derecho penal corporativo, encaminado a reprimir la infracción de los deberes que tiene una persona con la corporación a que pertenece en el trato directo con esta o con sus compañeros.

Aquí se podría incluir la traición del abogado, la inmoralidad del médico o la brutalidad del deportista, etc. Ahora bien, se podría terminar indicando que en su sentido amplísimo cabe hablar también de un derecho penal disciplinario en esferas aún más íntimas, como ocurre por ejemplo con la familia, en donde podría comprenderse el llamado derecho de corrección paterna.

b) Administrativo: Cabe mencionar que es controvertida la delimitación entre el derecho penal propiamente dicho y del derecho penal administrativo, integrado por el conjunto

de disposiciones que sancionan aquellos hechos que violan las disposiciones dictadas por la administración, por lo que en unos casos resulta clarísima esta distinción; pero en cambio, en otros la línea separatoria no aparece tan perfilada.

Por lo tanto, se formulan por los tratadistas diversas teorías de diferentes alcances para distinguir el injusto penal del injusto de policía, de manera que también se discute si este derecho penal administrativo o de policía.

El cual debe seguir viviendo de la savia que proporciona el derecho penal general o, por el contrario, debe integrar una rama jurídica de naturaleza totalmente distinta regida por sus propios principios.

1.3. Características

Las características que definen al derecho penal, encaminan a esta rama o subsección del derecho en cumplir con su objetivo o finalidad, es necesario entender que el derecho penal es:

a) Sancionador: Al Derecho penal le corresponde castigar los actos delictivos que lesionan o ponen en peligro intereses individuales, sociales y colectivos.
b) preventivo y rehabilitador: Incluye dentro de sus fines la objetiva prevención del delito y la efectiva rehabilitación del delincuente para devolverlo a la sociedad como un ente útil a ella.

De este modo, es necesario entender que las características del derecho penal se encuentran relacionadas intrínsecamente con su naturaleza jurídica, por lo que es posible mencionar que son las siguientes:

a) Positivo: El derecho penal es fundamentalmente jurídico, en el sentido de que el derecho penal vigente es sólo aquel que el Estado legalmente ha promulgado con el carácter de tal. Sobre el derecho penal positivo, se constituye el derecho penal y sólo conectando los problemas con esta positividad es cuando se hace verdadero derecho penal.

De esta manera, para reconocer la enorme influencia del derecho natural y la conveniencia de encuadrar las normas penales en el trasfondo filosófico-cultural del período histórico en que el jurista está llamado a operar.

b) Pertenece al derecho público: Los intereses que tutela, se concentran en la defensa de la colectividad; es sólo el cuidado y protección de la misma, lo que guía en la determinación de los delitos y en el señalamiento y aplicación de las penas.
c) Es de esencia valorativo y finalista: El derecho penal es fundamentalmente imperativo; pero esta imperatividad está subordinada a un orden valorativo, y a que califica los hechos de los hombres con arreglo a una evaluación de ellos y teniendo en cuenta el fin perseguido.
d) Es fundamentalmente sancionador: Se ha discutido mucho la naturaleza sancionadora del derecho penal en razón de que, siendo soberano en la descripción de los tipos delictivos, debía considerársele de naturaleza constitutiva.

Como bien se ha mencionado, es necesario entender los principales conceptos que encierran los delitos informáticos cometidos en las redes sociales, principalmente los conceptos contenidos en el derecho penal.


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

CAPÍTULO II

2. El delito informático

Es claro que el delito informático es un concepto totalmente nuevo en lo que a delitos se refiere y es que claramente es totalmente nuevo teniendo en cuenta que las redes sociales y la explosión del internet se ha dado durante las últimas dos décadas.

Por lo tanto, es necesario analizarlo de mejor manera, ya que una de las formas más comunes en que los delincuentes operan hoy en día, es a través de las redes sociales y el internet, logrando con esto impunidad total a sus actos.

Debe mencionarse que, el delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, prejuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Por lo tanto, se considera que no existe una definición formal y universal de delito informático, pero se han formulado conceptos respondiendo a realidades nacionales concretas: no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas.

Es decir, tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión delitos informáticos esté consignada en los códigos penales, lo cual, en el país, al igual que en otros muchos no han sido objeto de tipificación aún.

Así pues, en 1983, la Organización de Cooperación y Desarrollo Económico inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

De esta manera, en 1992 la Asociación internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el principio de subsidiariedad.

La OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito informático como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.

De la misma manera, los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma.

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

Debe mencionarse que, en esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito.

La informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

Es necesario tener en cuenta que la legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información. En este punto debe hacerse un punto y notar lo siguiente:

No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.

No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen. La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.

Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas. La protección de los sistemas informáticos puede abordarse desde distintas perspectivas: civil, comercial o administrativa. Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

2.1. Definición de delito informático

Es posible decir que, el delito informático o ciberdelincuencia es toda aquella acción, típica, antijurídica culpable, que se da por vías informáticas o que tiene como objetivo destruir dañar ordenadores, medios electrónicos y redes de internet.

Es decir, que debido a que la informática se desarrolla más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la teoría del delito, por lo cual se definen como abusos informáticos, y parte de la criminalidad informática.

De la misma manera se menciona que, los delitos informáticos son "todos aquellos en los cuales el sujeto activo lesiona un bien jurídico, que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo, por medio de utilización indebida de medios informáticos.

De esta manera surgen claramente de las nuevas tecnologías aplicadas y tienen como

objeto de manera expresa de las mismas y por regla general no poseen definiciones de tipo posibles de ser utilizadas en modo alguno por estar referidos a bienes y conceptos inexistentes a la sanción de las leyes penales".[7]

En todo el entorno cibernético, se establece en la sociedad humanitaria que el pensamiento permite descubrir sus verdaderas leyes y las fuerzas motrices del desarrollo de la realidad, en el que se establece que es de carácter virtual y público la naturaleza por sí mismo.

2.2. Delimitación del delito informático

Guatemala debe iniciar a prepararse para el futuro, creando medidas necesarias para poder prevenir una seria de delitos tecnológicos, para que la población pueda guardar información relevante y utilizarla después de una forma segura. El problema no solo es en el área penal si no en todo el ordenamiento jurídico nacional.

a) Delincuencia informática y abuso informático: Son todos comportamientos ilegales y contrarios a la ética que tienen por objeto a los sistemas o elementos informáticos, que concierne a un tratamiento automático de datos y/o transmisión de datos, pudiendo presentar múltiples formas de lesión de varios bienes jurídicos tutelados.
b) Criminalidad informática: Es todo comportamiento criminológico en el cual la computadora está involucrada como material o como objeto de acción para el empleo de actos antijurídicos que puedan ocasionar daños patrimoniales a terceras personas.

[7] Cámpoli, Gabriel Andrés. **Delitos informáticos en la legislación mexicana**. Pág. 144.

2.3. Delitos informáticos reconocidos por la Organización de las Naciones Unidas

Es posible mencionar que existen varios criterios para determinar la clasificación de los delitos informáticos, ya que doctrinariamente no existe una normativa a seguir, el Manual de las Naciones Unidas para la Prevención y Control de Delitos informáticos aporta la siguiente clasificación de delitos informáticos:

a) "Fraudes cometidos mediante la manipulación de computadoras: Manipulación de los datos de entrada; Manipulación de programas; Manipulación de datos de salida; y, Fraude efectuado por manipulación informática.
b) Falsificaciones informáticas: Utilizando sistemas informáticos corno objetos; y, utilizando sistemas informáticos como instrumentos.
c) Daños o modificaciones de programas o datos computarizados: Sabotaje informático; Virus; Gusanos; Bomba lógica o cronológica; Acceso no autorizado a sistemas o servicios; Piratas informáticos o hackers; y, reproducción no autorizada de programas informáticos con protección legal".[8]

2.4. Clasificación

El eje principal de los delitos informáticos se da en la manipulación de los datos de entrada, programas y salidas de computadoras, así como la falsificación de los sistemas informáticos, y el espionaje de información.

[8] López Betancourt, Eduardo. **Delitos en particular**. Pág. 271

Lo que produce en el sujeto pasivo un daño en su patrimonio; por ello se estima que los ilícitos cometidos a través de internet en su mayoría causan una afectación al patrimonio de los pasivos.

a) Delitos patrimoniales: El fraude electrónico causa una gran afectación a los usuarios de la banca, siendo el principal blanco de dichos ataques, los ataques informáticos se generan en contra de los clientes y no en contra de la institución crediticia, lo que obedece a los sistemas de protección que gozan las instituciones bancarias.

Tales ataques se llevan a cabo a través de dos programas que se denominan: Phising y Pharming, el propósito de esos programas es hacerse de los recursos del usuario de la banca, aprovechándose de dos factores básicos que toman en consideración los defraudadores, los cuales son el nivel cultural del usuario y la natural curiosidad del ser humano.

Ante los ataques de los defraudadores cibernéticos se han instrumentado sistemas básicos de protección que debe tener cualquier usuario de internet, entre los cuales destacan: Tener una herramienta de antivirus vigente y actualizado;

a) Poseer herramientas anti intrusas;
b) Tener un firewall personal;
c) Tener autorizados parches de seguridad; y,
d) Controlar las entradas y salidas de las unidades usb y disquetes para evitar las descargas de impresiones fotográficas, entre otras.

b) Delitos pornográficos: La distribución de pornografía por todo el mundo a través de la internet está en aumento. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material ofensivo que se transmita o archive."El fenómeno de la pornografía en internet, se engloba dentro de los denominados delitos computacionales, al suponer una nueva manifestación del delito ofensas al pudor, cuya comisión afecta el bien jurídico de la libertad sexual."[9]

c) Delincuencia organizada: El objeto y necesidad de fundamentar los delitos informáticos vinculados en la participación de algún miembro de la delincuencia organizada, así como los hechos, circunstancias, datos, y demás elementos que se pretenda probar.

La persona o personas que serán investigadas; la identificación del lugar o lugares donde se realizarán; el tipo de comunicación privada a ser intervenida; su duración; y el procedimiento y equipos para la intervención y, en su caso, la identificación de la persona a cuyo cargo está la prestación del servicio a través del cual se realiza la comunicación objeto de la intervención.

El objeto de la intervención de las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

---

[9] Reyna Alfaro, Luis. **Pornografía e internet: aspectos penales**. AR. Revista de derecho informático. Núm. 050. Junio de 2021.

La tecnología y el internet son herramientas que han permitido al hombre desarrollar sus actividades laborales y sociales, al mismo tiempo su uso indebido ha ocasionado daños tanto individuales, empresariales e inclusive instituciones de gobierno.

Es posible mencionar que así mismo en Guatemala, se ha reportado un aumento en delitos informáticos en los últimos años, los más comunes son el fraude, robo de identidad, robo de base de datos, infiltraciones.

En la actualidad Guatemala, dentro de los nueve países con mayores detecciones de códigos maliciosos en Latinoamérica ya que es uno de los países con mayores descargas de copias ilegales de software, por lo que muchos medios de protección son obsoletos por la cantidad de datos que existen en la red de internet.

La legislación en Guatemala, necesita una nueva regulación solo en aquellos aspectos donde se produce un vacío legal; en lo concerniente al Código Penal, no se da en ninguno de los títulos los delitos informáticos cometidos a través de redes sociales.

Por eso, dadas las características de esta problemática solo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

En materia penal se encuentran tipificadas una serie de acciones antijurídicas punibles en el Código Penal guatemalteco en su capítulo VII referente a los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos de acuerdo a lo regulado en los

Artículos; 274 "a" "b" "c" "d" "e" "f" "g", así también cómo en el Artículo 275 y 275 bis.

Los bienes jurídicos tutelados que establece el Código Penal establecen una leve protección de datos, por lo que es necesario proteger la privacidad, acceso a propiedad privada, acceso a la información no autorizada, situándolas como nuevas modalidades de delitos informáticos que operan a través de las redes sociales.

Debe establecerse que, "hechos que generen conductas indebidas deben ser tipificados en la legislación correspondiente. Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a prevenir la utilización abusiva de la información reunida y procesada mediante el uso de computadoras".[10]

Existen actualmente dos iniciativas de ley una por el diputado Francisco Contreras del partido de Acción de Desarrollo Nacional la iniciativa 4055 de Ley De Delitos Informáticos la cual tiene por objeto la protección integral de las personas, sus bienes y derechos, mediante el establecimiento de un marco jurídico relativo a los sistemas que utilicen tecnologías de la información.

Así como la prevención y sanción de los delitos cometidos relativos a fraude informático, daño informático, acceso ilícito, falsificación informática, espionaje informático, violación de la disponibilidad, reproducción de equipos, etc.

---

[10] Velásquez Elizarraras, Juan Carlos. **Instauración de un marco legal internacional de internet**. Pág. 289.

Y, la segunda propuesta, correspondió a la ex diputada Nineth Montenegro, en representación, de ese entonces, de la agrupación política, Encuentro por Guatemala, con la cual se buscaba castigar a las personas que mediante perfiles falsos engañen a menores de edad con fines sexuales, cometan extorsiones o difamaciones; dicha iniciativa podría atentar contra la libertad de expresión, por lo que es un análisis de estudio para los parlamentarios.

Sin embargo, éstos son solo algunos de los problemas que se presentan en cuanto a las redes sociales; teniendo en cuenta que, estos delitos, como bien se menciona, son realizados de manera inescrupulosa, por personas que se ocultan detrás de perfiles no verificados.


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

CAPÍTULO III

3. Principios del delito informático

Como bien se ha podido evidenciar en el capítulo anterior, el delito informático es ya toda una tendencia, por lo tanto, durante este capítulo, será necesario analizar los principios que rigen esta clase de delitos.

Por lo que, es prudente iniciar mencionando que, las conductas criminales por vías informáticas que no pueden considerarse como delito, según la teoría del delito, por lo cual se definen como abusos informáticos, y parte de la criminalidad informática.

La falta de acuerdos globales acerca de qué tipo de conductas debe constituir delitos informáticos, y la ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

Asimismo, la ausencia de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos, la armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

De esta manera, el carácter transnacional de muchos delitos cometidos mediante el uso de computadoras. Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Es destacable que, la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Teniendo en cuenta esto, las ventajas y las necesidades del flujo nacional e internacional de datos, que de modo creciente aumenta aún en países latinoamericanos, conlleva también a la posibilidad progresiva de estos delitos.

Por eso puede señalarse que, la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones de los funcionarios judiciales. Ahora bien, atendiendo a esto se afirma, "que la Teoría del Delito es una teoría de la aplicación de la ley penal, y como tal pretende establecer un orden para el planteamiento y la resolución de los problemas que implica la aplicación de la ley penal.

La misma cumple una doble función mediadora, por un lado, entre la ley y la solución del caso concreto; y, por otro lado, una mediación entre la ley y los hechos que son objeto del juicio".[11]

Tomando en cuenta lo anterior, es posible afirmar que la aplicación de la ley penal principalmente pretende establecer el orden de los elementos para con esto obtener una mejor resolución dentro de los casos que este pretende analizar, por lo tanto, es necesario analizar los principios que lo rigen.

---

[11] Bacigalupo, Enrique. **Lineamientos de la teoría del delito**. Pág. 25.

3.1. El principio de legalidad

De la misma manera, cuando se menciona el principio de legalidad, debe mencionarse que para que se dé un delito tiene que cumplirse cada uno de los tipos o elementos que estén en el código.

Sin embargo, debe tenerse en cuenta que no debe confundirse que el hecho que la acción sea típica ya es un delito ya que este es un indicio, pero nos faltan elementos como la acción antijurídica. Sin embargo, es preciso indicar primero, cuáles son las acciones típicas antijurídicas, y es posible mencionar que si va en contra de la norma son acciones típicas y antijurídicas.

Por lo tanto, hay acciones típicas que no necesariamente son antijurídicas como matar en legítima defensa, es decir está tipificado el delito de homicidio y por ello es típica dicha acción, pero es antijurídica porque fue en legítima defensa.

Es necesario entender que el principio de legalidad, claramente exige como condición esencial, la existencia de un régimen jurídico que formule la descripción del hecho o conducta criminal y de la pena a imponerse, previamente al hecho que califica a ella como criminal, para imputar a una persona como autora del delito.

En cuanto a esto, también es necesario entender que la concreción legislativa de nuevos supuestos de incriminación que supongan nuevos delitos, es un paso importante para llevar a cabo en la legislación guatemalteca.

Si bien, y como ha quedado demostrado en los puntos anteriores, a nivel mundial existen varios pronunciamientos y reformas legislativas tendientes a la protección de bienes jurídicos o intereses como ser el software, la información, la intimidad, etc. Se debe remarcar que dicha nueva normativa, brinda una solución parcial a la problemática que nos ocupa, por ello, ante determinadas situaciones, sería conveniente contemplar situaciones puntuales de violación a los sistemas informáticos, a través de figuras tipo, contempladas en los códigos penales.

Se enumera las consecuencias que derivan de dicho principio que son: "la indelegabilidad de la facultad legislativa penal, el Principio de Reserva penal con sus presupuestos (la tipicidad del hecho punible, la prohibición de la aplicación de la ley penal por analogía y la irretroactividad de la ley penal), y la predeterminación legal de la pena aplicable".[12]

Pero el inconveniente surge de la necesidad de incorporar una serie de delitos informáticos y delitos que se cometan en redes sociales al Código Penal.

3.2. El principio de reserva penal

En cuanto al principio de reserva penal, se encuentra principalmente en la garantía de la legalidad, es decir, que el ámbito de lo punible debe estar determinado exhaustivamente por la ley, y que todo lo que queda al margen de ese ámbito está reservado como esfera de impunidad.

[12] Nuñez, Ricardo. **Manual de derecho penal. Parte general**. Pág. 79

Es necesario tener presente que, en el derecho penal, directamente existe la forma idónea de poder establecer la reserva de forma legal ante un tipo penal preestablecido ante la sociedad. Por lo que claramente este principio se encuentra consagrado en el Ar1ículo 12 de la Constitución Política de la República de Guatemala y consiste en que nadie podrá ser condenado ni privado de sus derechos sin antes haber sido citado, oído y vencido en un proceso judicial.

Asimismo, el Código Procesal Penal lo desarrolla debidamente, ya que el procesado tiene desde la primera actuación judicial hasta la eventual condena una serie de facultades y deberes que le permiten conocer todas las actuaciones judiciales y contar con defensa técnica, a excepción de dos casos.

La ley de narcoactividad que permite reserva de actuaciones en las fases de investigación y preparatoria, y el Artículo 314 del CPP que establece que el Ministerio Público podrá tener en reserva las actuaciones, incluso ante las partes cuando no se hubiere dictado el auto de procesamiento.

Claramente, el debido proceso comprende numerosas instituciones relacionadas, tanto con las partes como con la jurisdicción, que han de preservar la certeza en el proceso en todo momento. Busca, en suma, rodear al proceso de las garantías mínimas de equidad y justicia que respaldan en legitimidad la certeza en derecho de su resultado.

De esta forma, debe mencionarse que a través del debido proceso se precipitan todas las garantías, derechos fundamentales y libertades públicas de las que es titular la persona

en el Estado social y democrático de derecho.

El debido proceso legal es la institución del derecho constitucional procesal que identifica los principios y presupuestos procesales mínimos que debe reunir todo proceso jurisdiccional para asegurar al justiciable la certeza, justicia y legitimidad de su resultado. Debe decirse que está integrada a esta garantía genérica, en cuanto es parte indispensable de un enjuiciamiento equitativo que limite el poder del aparato estatal, la garantía del *ne bis in ídem*.

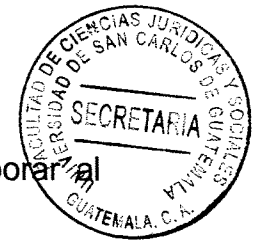
El mismo que tiene un doble significado: procesal, según el cual nadie puede ser enjuiciado dos veces por los mismos hechos, y material, en virtud del cual nadie puede ser sancionado dos veces por una misma conducta.

Asimismo, esta garantía funciona contra quien es objeto de una imputación penal, sin que a ello objete que se formule en sede judicial, que se esté en cualquier fase del proceso o se tenga o no formalmente la calidad de imputado. Constituye, una manifestación privilegiada del derecho a defenderse de una imputación penal.

El imputado tiene el derecho a introducir válidamente al proceso la información que considere adecuada. Él es quien tiene el señorío y el poder de decisión sobre su propia declaración. Sus principales efectos son los siguientes:

a) La no declaración no permite inferencias de culpabilidad;

b) El imputado tiene el derecho de declarar cuantas veces quiera, pues es él quien



controla la oportunidad y contenido de las informaciones que desea incorporar al proceso;

c) Rige solo cuando se obligue al imputado a emitir una declaración que exteriorice un contenido, de ahí que cuando se le obliga a someterse a una confrontación o careo, a una identificación, a una pericia no se viola esta garantía.

Ahora bien, teniendo precisamente en rigor, lo que se protege son las comunicaciones o testimonio del individuo, no la evidencia real o física derivada de la persona del imputado. Las garantías procesales son las seguridades que se otorgan para impedir que el goce efectivo de los derechos fundamentales sea conculcado por el ejercicio del poder estatal, ya sea limitando ese poder o repeliendo el abuso.

De esta manera, en cuanto se trata de un derecho fundamental, destinado a la protección de todos aquellos que acuden al órgano jurisdiccional en defensa de sus derechos e intereses legítimos.

La ley ordinaria no puede impedir la actuación de medios de pruebas sustanciales para la defensa, ni priorizar otros intereses o bienes jurídicos, que no tengan expresa relevancia constitucional o igual nivel.

Asimismo, junto a la pertinencia, el derecho ha incorporado otros dos límites extrínsecos a la actividad probatoria: la utilidad y la licitud.

a) La primera es aquella en que por existir una manifiesta inadecuación de medio a fin, se

puede conjeturar razonablemente que no alcanzará el resultado pretendido.

b) La segunda es aquella que respeta otros derechos fundamentales y no quebranta disposición ordenatoria alguna de la actividad probatoria.

Además, debe mencionarse que, este derecho comprende no solo el poder de lograr la comparecencia compulsoria de testigos y peritos, así como la incorporación de todo documento, informe o dato pertinente al proceso.

Teniendo en cuenta esto, también comprende lograr la información que éstos puedan proporcionar y, en su caso, a posibilitar careos o confrontaciones con testigos de cargo o coimputados.

Ahora bien, lo esencial en este último supuesto es asegurar al oponente la oportunidad de contrainterrogar, de formular directamente preguntas y de obtener respuestas inmediatas.

3.3. Ilícito informático a la luz de la teoría del delito

Cuando se menciona el delito informático debe tenerse en cuenta los elementos que lo componen y permiten el perfeccionamiento del mismo, teniendo en cuenta que estos elementos son los que le dan vida al propio delito, dentro de los cuales se encuentran:

a) Antijuricidad: En el elemento de la antijuridicidad el objetivo es establecer si la conducta prohibida por la legislación es contraria al orden jurídico en general, y por ello al hecho

típico y antijurídico se le denomina injusto.

En virtud de lo mencionado en el párrafo anterior, debe mencionarse que, por el contrario, si el hecho típico está amparado por alguna causa de justificación ya no hay delito. En la conducta-típica, la preocupación natural de la doctrina, es ocuparse de delimitar si la conducta encuadra en el tipo y podría ser particularmente considerada como una conducta prohibida para el derecho penal.

En contrapartida, en la categoría de la antijuridicidad se analiza si esa conducta prohibida se justifica de cara a todo el orden jurídico por las circunstancias materiales que concurrieron en el momento de su realización o si, por el contrario, se constata que el hecho resulta un injusto.

Debe mencionarse que las precisiones anteriores servirán como punto de partida para establecer el terreno en que deben ubicarse los delitos informáticos, puesto que en su mayoría resultan de nueva creación por el legislador y por lo mismo requieren de una atención especial.

Asimismo, esto claramente ya que en algunos casos su descripción legal no corresponde precisamente a las conductas que originalmente se tuvo presentes para sancionar, errores que, en ocasiones por la mala integración de la averiguación previa.

También, debe mencionarse que posteriormente a esto se conducen a un resultado totalmente adverso al no lograrse el enjuiciamiento y dictado de la sentencia

correspondiente.

En la doctrina científica del derecho penal, las causas de justificación son el negativo de la antijuricidad o antijuricidad como elemento positivo del delito, y son aquellas que tienen la virtud de convertir en lícito un acto ilícito.

Es decir, que precisamente cuando en un acto delictivo aparece una causa de justificación de lo injusto, desaparece la antijuricidad del delito y como consecuencia se libera de responsabilidad penal al sujeto activo.

b) Acción u omisión: Es la voluntad de las personas de manifestarse mediante un hacer o mediante un no hacer. Esta es una doble caracterización de la acción, que no quiebra la unidad de la misma, ya que en el no hacer se proyecta al mundo exterior, una manifestación de la voluntad del autor.

En este punto coincidimos en que la gran mayoría de delitos que se cometen mediante sistemas informáticos son delitos de acción positiva, o sea se cometen a través de un hacer.

Casos como el hacking, cracking, phishing, para citar algunos, siempre se perpetran mediante conductas con la voluntad de causar o generar dichos resultados negativos sobre los bienes jurídicos que vulneran. Pero, también se cree que es posible, cometer delito de omisión dentro de la especie de delitos informáticos, aclarando que no se ha visto regulado en forma específica lo que no significa que en algún país efectivamente se

haya regulado de dicha manera, algún delito informático perpetrado por omisión.

c) Tipicidad: La tipicidad es importante aclarar la necesidad actual, tanto nacional como a nivel mundial, de tipificar la mayor cantidad de conductas que puedan configurar delitos informáticos.

En este sentido, se mencionan en forma precedente, los esfuerzos a nivel mundial, de organismos internacionales, como también de los Estados parte de sistemas de integración regional, en lo que respecta a esta preocupación legislativa.

Adoptar políticas conjuntas en lo que hace a seguridad, ya sea en el uso de internet, como así también en el comercio electrónico, o en tráfico de datos, es indispensable para lograr un efecto integrador de los instrumentos de control social, a nivel mundial. Además, también se encuentran actitudes ilícitas que jurídicarnente ya están configuradas como delitos en el ordenamiento penal, pero se estima que la legislación debe perfeccionar debido al vertiginoso desarrollo que viene alcanzando el uso de la tecnología informática.

d) Culpabilidad: La culpabilidad consiste en un juicio sobre el autor mediante el cual se determina si se le puede reprochar el haberse comportado de manera contraria a lo que establece el orden jurídico.

La culpabilidad se conforma de tres elementos: la imputabilidad del sujeto, su conciencia sobre la antijuridicidad de la conducta y la ausencia de causas excluyentes de la culpabilidad. El fortalecimiento de este principio requiere:

a) La culpabilidad debe establecerse mediante sentencia judicial;

b) Que la condena se base en prueba que establezca con certeza el hecho criminal y la culpabilidad;

c) Que la sentencia se base en pruebas jurídicas y legítimas; y,

d) Que la prisión provisional sea una medida cautelar de carácter excepcional para asegurar la presencia del inculpado en el proceso y la realización de la justicia.

CAPÍTULO IV

4. Redes sociales, medios por los cuales se cometen delitos en anonimato, con falsificación de perfiles; que casi siempre quedan en la impunidad

Para concluir con la investigación, tal y como se ha mencionado en los capítulos anteriores, los delitos informáticos se caracterizan por quedar regularmente en el anonimato. Esto, claramente, debe indicarse aunado al hecho de que, estos delitos se cometen en redes sociales de internet en Guatemala y se puede verificar que existen lagunas legales en las leyes tanto sustantivas como adjetivas.

Asimismo, debe decirse que, Guatemala es un país muy vulnerable a recibir ataques en redes sociales ya que no existe regulación alguna por lo que es necesario que los legisladores se capaciten en derecho Informático, para poder establecer nuevos tipos penales que puedan prevenir y sancionar a los actores de dichos delitos.

De la misma manera, debe mencionarse que existen redes sociales que claramente establecen en que tribunal y en qué país debe acudir a un litigio o reclamación de usuarios.

Esta cláusula establece que, renuncia al fuero de su domicilio lo que no es conveniente para el usuario, tratándose de un contrato de adhesión, con ninguna posibilidad que el usuario pueda proponer condiciones favorables para el mismo.

4.1. Los servicios de redes sociales y su naturaleza

Teniendo en cuenta lo anteriormente indicado, para establecer la naturaleza jurídica se analiza la relación obligacional que surge de la prestación del servicio entre la empresa titular del sitio web y el usuario, es claramente un contrato por adhesión.

De esta manera, los contratos por adhesión son aquellos en los cuales el contenido contractual ha sido determinado con prelación, por uno solo de los contratantes, al que se deberá adherir el co-contratante que desee formalizar la relación jurídica obligatoria.

Asimismo, en el contrato de adhesión las cláusulas están dispuestas por uno solo de los futuros contratantes de manera que el otro no puede modificarlos o hacer otra cosa que aceptarlas o rechazarlas.

De acuerdo con wikipedia, de tal manera, el usuario al realizar el proceso de registración en cualquier sitio web que preste este tipo de servicios, tales como facebook, hi5, orkut, debe obligatoriamente aceptar y prestar conformidad a los términos y condiciones del sitio y políticas de privacidad impuestas unilateralmente.

Una red social es una estructura social compuesta por un conjunto de actores y uno o más lazos o relaciones definidos entre ellos. Su estudio se remonta a los años 1930, con la creación de los sociogramas por parte de Jacob Levy Moreno y Helen Hall Jennings, que dieron origen a la sociometría, precursora del análisis de redes sociales y buena parte de la psicología social.

Desde finales de los años 1940, se han estudiado además en profundidad mediante la teoría de grafos. El análisis de redes sociales es un estudio interdisciplinario en el que confluyen las ciencias sociales y del comportamiento, como matemáticas y estadísticas.

Actualmente, las redes sociales representan uno de los mayores paradigmas de la sociología contemporánea y del comportamiento organizacional. La creación de redes sociales en línea ha derivado en redes complejas, que son el objeto de estudio de la ciencia de redes.

Debido a los grandes volúmenes de datos de este tipo de redes, para su estudio se suelen utilizar además herramientas y técnicas de las ciencias de la computación.

Asimismo, "el acto de relacionamiento con el sistema se automatiza, se simplifica de modo que el sujeto que lo celebra no tiene conciencia de sus efectos jurídicos".[13]

Por lo que, es necesario establecer que, no se trata de discriminar ni restarle validez al consentimiento del usuario expresado por medios electrónicos, el cual es perfectamente válido.

Lo anterior permite claramente plantear la problemática típica de los contratos por adhesión llevada al ámbito de internet en relación a la información necesaria que debe tener el usuario a fin de actuar con un debido consentimiento informado en la

[13] Lorenzetti, Ricardo Luis. **La oferta como apariencia y la aceptación basada en la confianza**. Pág. 12

manifestación de su voluntad.

Al analizar de mejor manera la ley de acceso a la información pública protege la información que encuentra en poder de la administración pública, así como el libre acceso a todas instituciones y dependencias del Estado.

Ahora bien, de tal manera, por lo que la protección de información personal en lasas redes sociales cuenta con un nivel de riesgo superior a las páginas web tradicionales principalmente.

Dado que, los usuarios exponen no solo sus datos de contacto o información profesional como formación, experiencia laboral, sino que se pueden exponer de manera pública las vivencias, gustos, ideología y experiencias del usuario, lo que conlleva que el número de datos de carácter personal puestos a disposición del público.

Asimismo, se tratan datos especialmente protegidos, lo que supone un mayor nivel de riesgo para la protección de dichos datos personales y, por ende, del ámbito de la privacidad e intimidad de los usuarios.

De esta forma, debe mencionarse que existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales serán accesibles por cualquier persona y del valor que éstos pueden llegar a alcanzar en el mercado.
En muchos casos, los usuarios hacen completamente públicos datos y características personales que en ningún caso expondrían en la vida cotidiana como ideología,

orientación sexual y religiosa, etc.

El principio básico de esta norma legal consiste en que los datos son propiedad del usuario mientras él mismo no permita su uso a una empresa o a un tercero. La autorización se concede, por ejemplo, al rellenar un formulario de adhesión que permite el acceso a un sitio.

Asimismo, en relación a la propiedad intelectual, la realidad de los delitos que se cometen en redes sociales es una forma fácil de reproducir y distribuir contenidos de internet es uno de los principales medios de crecimiento para los contenidos de propiedad intelectual.

Al tiempo que supone uno de los principales retos en lo que respecta al control y protección de los derechos de autor, en la medida en que los contenidos se encuentran en formato digital y, por tanto, su distribución y comunicación pública es mucho más sencilla que en otro tipo de formato.

Los posibles riesgos que se pueden producir contra la protección de la propiedad intelectual en Internet y en los servicios de redes sociales. Muchos usuarios se ven afectados de los contenidos que son titularidad de terceros y que el usuario decide publicar dentro de la red social sin autorización de los titulares del derecho de propiedad intelectual.

Ahora bien, en estos supuestos el usuario se encuentra violando derechos de autor, y en

consecuencia deberá responder por los daños y perjuicios. Una problemática que se presenta en relación a este punto, es cuando los usuarios deciden darle baja su suscripción o cuenta a la red social, siendo que en ese caso se debería dejar de difundir y publicar los contenidos de su autoría.

A causa de este tipo de situaciones, este año la red social Facebook.com decidió modificar unilateralmente sus términos y condiciones estableciendo que los usuarios cedían y licenciaban de manera irrevocable y perpetua sus contenidos a la empresa norteamericana, argumentando la necesidad de seguir contando con esos contenidos online en caso de que el usuario diera de baja su cuenta.

Asimismo, es preciso tener presente que, esto causó un revuelo en los internautas, que recibieron la noticia con gran descontento, lo que obligó a la empresa a retornar a su política anterior.

La propiedad intelectual en los sitios de redes sociales viene a perjudicar al empresario que se dedica al desarrollo de contenido digital, en vista que es de fácil distribución y cualquier persona que tenga acceso a internet pueda copiar el contenido del creador.

De tal manera, debe destacarse que en la actualidad en Guatemala existen lagunas legales respecto al respeto de los derechos de propiedad Intelectual en los sitios de redes sociales de internet.

Por este motivo, es importante que los usuarios conozcan qué ocurrirá con sus obras una

vez que son publicadas en una red social y que exista alguna forma de supervisión y control de contenidos. Por lo tanto, puede ocurrir que el contenido publicado de un usuario permanezca disponible para el público aun habiendo solicitado la baja de la plataforma o red social, el problema principal que se plantea es la imposibilidad técnica de controlar o supervisar contenidos por parle de los prestadores de servicios de internet.

Ahora bien, en el trabajo de investigación se puede analizar a través de un cuadro comparativo de las medidas que se han tomado a nivel latinoamericano para atender el problema de la criminalidad informática.

Debe analizarse a la comunidad internacional latinoamericana, su forma de abordar el problema y su incidencia en cuanto a falta de consensos sobre delitos informáticos, definición jurídica, conductas delictivas, así como la falta de tratados sobre extradición.

Asimismo, los países y las organizaciones internacionales se han visto en la necesidad de legislar sobre los delitos informáticos y especialmente en redes sociales, debido a los daños y perjuicios que le han causado a la humanidad.

Sin embargo, es cierto existe un esfuerzo por parte de los países para tratar de evitarlos, no existe un criterio unificado de cómo deben ser atacados, así poder tener una legislación internacional coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente.

De tal manera, en materia de estafas electrónicas, defraudaciones y otros actos dolosos

relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

a) Alemania: Este país sancionó en 1986 la Ley contra contempla los siguientes delitos; Espionaje de datos, datos, sabotaje informático, estafa informática, alteración de datos cibernéticos.

b) Austria: La Ley de reforma del Código Penal, sancionada el 22 de diciembre de 1987, en el Artículo 148, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos, además, contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

c) Inglaterra: Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act. Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Ahora bien, es necesario tener presente que, esta ley tiene un apartado que específica la modificación de datos sin autorización. Los virus están incluidos en esa categoría.

El hecho de liberar un virus tiene penas desde un mes a cinco años de cárcel, dependiendo del daño que causen, cual se penaliza el hacking, el phreaking, la ingeniería social, y la distribución de virus para dañar el sistema de cómputo en cuanto a la

tecnología virtual.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error, la pena no superará un mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta cuatro años de prisión.

d) Francia: En enero de 1988, se dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta Ley tipifica en el Artículo 462 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.

Por su parte, el Artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje). Por último,

esta Ley en el Artículo 462-2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

e) España: En el Código Penal de España de 2009, el Artículo 263 establece que, el que causare daños en propiedad ajena. En tanto, el Artículo 264-2 preceptúa, aplicará la pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Este país quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa. Su actual Ley Orgánica de Protección de Datos de Carácter Personal aprobada el 15 de diciembre de 1999, reemplaza una veintena de leyes anteriores de la misma índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreaking, la introducción de virus, etc.

Aplicando principalmente como primer recurso la pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de

funcionarios públicos.

Teniendo en cuenta esto, es posible mencionar que las redes sociales, se han convertido en una madriguera para aquellos que buscan cometer delitos aprovechándose del anonimato y falsificación de perfiles, medio por el cual casi siempre quedan impunes.

4.2 Delitos que se cometen utilizando las redes sociales

De acuerdo con Wikipedia, se toma el siguiente contenido: delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet.

Ante el extendido uso y utilización de las nuevas tecnologías en todas las esferas de la vida (economía, cultura, industria, ciencia, educación, información, comunicación, etc.) y el creciente número de usuarios, consecuencia de la globalización digital de la sociedad, la delincuencia también se ha expandido a esa dimensión. Gracias al anonimato y a la información personal que se guarda en el entorno digital, los delincuentes han ampliado su campo de acción y los delitos y amenazas a la seguridad se han incrementado exponencialmente.

Además de los ataques que tienen como objetivo destruir y dañar activos, sistemas de información y otros sistemas de computadoras, utilizando medios electrónicos o redes de Internet, se producen nuevos delitos contra la identidad, la propiedad y la seguridad de las personas, empresas e instituciones, muchos de ellos como consecuencia del valor

que han adquirido los activos digitales para la *big data* empresarial y sus propietarios bien sean entes jurídicos o personas naturales. Existen también otras conductas criminales que aunque no pueden considerarse como delito, se definen como ciberataques o abusos informáticos y forman parte de la criminalidad informática.

La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, son llevados a cabo utilizando un elemento informático.

Los delitos informáticos son actividades ilícitas o antijurídicas que:

- Se cometen mediante el uso de entornos digitales, redes, *blockchain*, computadoras, sistemas informáticos u otros dispositivos de las nuevas tecnologías de información y comunicación (la informática es el medio o instrumento para realizar un hecho anti jurídico).
- Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos informáticos).

Los ciberdelitos son actitudes contrarias a los intereses de las personas teniendo como instrumento o fin (concepto atípico) a las computadoras.

En la actualidad debe hablarse de ciberdelitos,5 pues este concepto sustantiva las consecuencias que se derivan de la peculiaridad que constituye la red digital como medio de comisión del hecho delictivo, y que ofrece contornos singulares y problemas propios,

como por ejemplo la dificultad de determinar el lugar de comisión de tales hechos ilícitos, indispensable para la determinación de la jurisdicción y competencia penal, para su enjuiciamiento y aplicación de la correspondiente ley penal, los problemas para la localización y obtención de las pruebas de de tales hechos delictivos.

La insuficiente regulación legal de los ilícitos que pueden realizarse a través de la red o de las diligencias procesales de investigación aplicables para el descubrimiento de los mismos .normativa igualmente desbordada por el imparable avance de las innovaciones tecnológicas-, o, en fin, la significativa afectación que la investigación policial en Internet tiene sobre los derechos fundamentales de los ciudadanos.

Por todo ello, la última orientación jurídica es priorizar el enfoque en la seguridad en las redes y los sistemas de información. A tal fin obedece la Directiva de la Unión Europea relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea, también conocida como Directiva NIS.

La directiva anteriormente mencionada impone, por ello, a las entidades gestoras de servicios esenciales, así como a los prestadores de ciertos servicios digitales considerados clave en el funcionamiento de Internet, la obligación de establecer sistemas de gestión de la seguridad de la información en sus organizaciones y de notificar a las autoridades los incidentes que tengan especial gravedad.

Además, obliga a los estados miembros a supervisar el cumplimiento de estas

obligaciones y a velar por que existan equipos de respuesta a incidentes de seguridad con capacidad para proteger a las empresas de la propagación de estos incidentes. Así mismo, impulsa la cooperación entre autoridades nacionales y el intercambio de información como medio para elevar el nivel de seguridad en la Unión Europea frente a las amenazas de carácter transfronterizo.

Mucha información es almacenada en un reducido espacio, con una posibilidad de recuperación inmediata, pero por complejas que sean las medidas de seguridad que se puedan implantar, aun no existe un método infalible de protección.

La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

La Organización de Naciones Unidas reconoce los siguientes tipos de delitos informáticos:

4.2.1 Fraudes cometidos mediante manipulación de computadoras

En este se reúne: la manipulación de datos de entrada (sustraer datos), manipulación de programas (modificar programas del sistema o insertar nuevos programas o rutinas),

manipulación de los datos de salida (fijación de un objeto al funcionamiento de sistemas de información, el caso de los cajeros automáticos) y fraude efectuado por manipulación informática (se sacan pequeñas cantidades de dinero de unas cuentas a otras).

4.2.2 Manipulación de datos de entrada

Como objetivo cuando se altera directamente los datos de una información computarizada. Como instrumento cuando se usan las computadoras como medio de falsificación de documentos.

4.2.3 Daños o modificaciones de programas o datos computarizados

Entran tres formas de delitos: sabotaje informático (eliminar o modificar sin autorización funciones o datos de una computadora con el objeto de obstaculizar el funcionamiento) y acceso no autorizado a servicios y sistemas informáticos (ya sea por curiosidad, espionaje o por sabotaje).

Existen leyes que tienen por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos en las variedades existentes contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías.

Una misma acción dirigida contra un sistema informático puede aparejar la violación de varias leyes penales, algunos autores expresan que el "uso de la informática no supone

más que un *modus operandi* nuevo que no plantea particularidad alguna respecto de las formas tradicionales de comisión".

Una clara dificultad para la persecución de estos ilícitos, ha sido que el ciudadano no considera delincuente al autor de estos delitos, entre los propios victimarios algunas veces existe una reivindicación que subyace a toda su actividad, como es el caso de los *hackers*, quienes cuentan con toda una "filosofía" preparada para respaldar su actividad afirmando que pretenden a un mundo más libre, que disponga de acceso a todas las obras de la inteligencia, y basándose en ese argumento divulgan las claves que tienen en su actividad.

El beneficio que trajo la tecnología es evidente; pero también puede ser reducto de delitos que quedan impune, en Guatemala, debido a que, el ente investigador no cuenta con herramientas necesarias para poder afrontar este tipo de delitos.

4.2.4. Redes sociales: una ventana a los delitos sexuales

"Las denuncias por acoso y divulgación de fotos íntimas registran un considerable aumento en Guatemala, Honduras y El Salvador en los últimos años. El anonimato y el poder de divulgación atribuidos a los perfiles personales en internet posibilitan la alza".[14]

Foto de una mujer atractiva en el perfil de Facebook de un lado y un adolescente

[14] https://nomada.gt/blogs/redes-sociales-una-ventana-a-los-delitos-sexuales/ **Redes sociales: una ventana a los delitos sexuales.** (Consultado del 23 de agosto de 2021).

entusiasmado del otro. Señuelo y credulidad. Anonimato e ilusión. En los últimos años, esos elementos se han convertido en ingredientes de actos que amenazan la libertad sexual de jóvenes. Bajo engaño, pasan a ser víctimas de personas que se esconden tras páginas de redes sociales ficticias.

Casos como ese –puede leerse una historia real ocurrida en Guatemala acá– representan uno de los usos negativos de las Tecnologías de la Información y la Comunicación (TIC) más comunes en los países del triángulo norte centroamericano. Así lo confirman las estadísticas con las que cuentan instituciones policiales de las tres naciones. Y lo certifican sus representantes consultados.

Los expertos los llaman delitos contra libertad sexual. Estos incluyen el acoso, el exhibicionismo, la divulgación de fotos íntimas y la corrupción de menores, entre otros. Según expertos, aunque se trate de actos contra la ley que han existido desde hace tiempo, la popularidad de las redes sociales y el fácil acceso a ellas gracias a la conexión a internet, las ha potencializado en los últimos años.

Solo para citar el caso de Guatemala, las estadísticas de denuncias por acoso en las que internet fue la herramienta utilizada, muestran un alza evidente. En 2015, la PNC registró 245 casos. En 2017 la cifra subió a 366. WhatsApp, Facebook y Twitter son las redes sociales más utilizadas para tal fin.

Las estadísticas sobre denuncias por violación a la intimidad, en que hombres comparten fotos privadas de mujeres, pasaron de 76 en 2015 a 140 en 2017. Casi el doble. En ese

último año, 111 de las 140 denuncias registradas por la PNC, fue el sistema de mensajería whatsApp el medio ocupado. Vía facebook.

De acuerdo a Diego Teos, jefe de delitos informáticos de la PNC de Guatemala, los niños, niñas, adolescentes y mujeres suelen ser las víctimas más recurrentes. Este dato es también válido para los restantes países del triángulo norte centroamericano: El Salvador y Honduras.

Los ejemplos son muchos. Suele pasar, por citar un caso, que una pareja decide grabarse a sí misma sosteniendo relaciones sexuales, bajo consentimiento. Sin embargo, al terminar la relación, uno de ellos –casi siempre el hombre, según las autoridades–, exige a su pareja continuar la relación a cambio de no revelar las imágenes. O decide difundirlas directamente en redes sociales o en sitios web pornográficos a manera de venganza.

En otras ocasiones, la pareja víctima ni siquiera sabía que había sido grabada en tal situación, como se puede leer en este caso que fue judicializado en El Salvador.

También hay denuncias que perfilan a una víctima mujer de clase baja. En este tipo de caso, ellas "son seducidas en redes sociales por hombres que viven en otros países. Les hacen creer que tienen una relación, les manda dinero y, pues sí, también les pide fotos íntimas. Pero cuando ellas ya no quieren seguir en la relación les cobran el dinero que depositaron o, incluso, las amenazan con publicar las fotografías", sostiene Teos, de la PNC de Guatemala.

En otras ocasiones, las redes sociales no son necesariamente la herramienta directa para cometer el delito. Se convierten en una vía de comunicación que sirve para ejecutar un secuestro o en ocasiones, un asesinato. Estas plataformas también sirven para la trata de personas y la explotación sexual.

Se habla, por ejemplo, de delincuentes que, desde un perfil falso, contactan a mujeres u hombres que consideran vulnerables. Una vez ganan su confianza, les ofrecen trabajos como modelos o edecanes, que son únicamente una fachada para explotarlos sexualmente.

En otros casos, personas se hacen pasar por mujeres guapas para atraer a jóvenes hombres. Luego –señala Teos– "existe la posibilidad de que los convenzan a conocerse en persona, con el objetivo de que exista una violación o secuestro" o incluso homicidios, como en este caso ocurrido en Guatemala en el que un par de mujeres jóvenes conocieron a sus asesinos en Facebook.

En conclusión, existen al menos dos características a favor de los delincuentes para utilizar este tipo de herramientas. Por un lado, el anonimato que les permite actuar ante las víctimas desde la sombra y sin generar sospechas. Y por el otro, la capacidad de divulgación mayor de las redes sociales.

En otras palabras: antes de las redes sociales, revelar fotos íntimas de la pareja sexual, generaba un impacto mucho menor. Hoy, las redes sociales vuelven este tipo de sucesos fenómenos virales que pueden sobrepasar fronteras, ensanchando así el sufrimiento y re-

victimizando aún más a la persona ofendida.

4.2.5. Redes sociales: nuevas oportunidades y nuevos peligros

"Dulce es una adolescente de 14 años que como la mayoría de las adolescentes de su generación es asidua a las redes sociales, a navegar por internet y a estar conectada en línea. En una de las tantas ocasiones en las que navegaba por esta, fue contactada a través de un perfil falso, engañada y abusada".[15]

De acuerdo con la cita referida, a nivel global, uno de cada tres usuarios en internet y las redes sociales es una niña o un niño. La mayoría de ellos no conoce los riesgos que puede haber tras estas redes ni sabe cómo protegerse. La brecha digital entre adultos y niños hace difícil que los padres, maestros o tutores puedan tomar medidas de protección en línea y aconsejar a los niños. Detrás de muchos abusos y delitos en línea, hay redes nacionales e internacionales del crimen organizado.

Dulce vive en un ambiente familiar bajo el cuidado de sus dos padres y con una hermana de 17 años de edad. Tanto su papá como su mamá trabajan tiempo completo mientras ella y su hermana estudian. Aunque es un hogar modesto, sus progenitores les han procurado las comodidades necesarias para el desempeño de sus labores y diversión. Entre estas, un computador con acceso a internet, el que podían utilizar en forma relativamente libre, dada la confianza depositada por los papás en sus hijas.

---

[15]https://www.unicef.org/guatemala/historias/redes-sociales-nuevas-oportunidades-y-nuevos-peligros. **Redes sociales: nuevas oportunidades y nuevos peligros.** (Consultado el 24 de agosto de 2021).

En una oportunidad, Dulce se encontraba navegando en internet buscando un trabajo para poder ayudar económicamente en su hogar, cuando encontró lo que podía ser un buen empleo de tiempo parcial.

Según la consulta realizada, "Estaba navegando y cabal, me entró una solicitud de amistad y por lo mismo de volverme más popular y conseguir más amigos la acepté; esa persona me mandó un mensaje diciéndome que me ofrecía un trabajo de dama de compañía y yo le dije que lo iba a pensar y dos días después le dije que si me interesaba; Ella, porque en la web aparecía como una mujer, lo que me daba más confianza, me comentó que me iba a juntar con su jefe, lo que ocurrió una semana después en un restaurante de un centro comercial. El me preguntó mi nombre, edad, donde vivía, si tenía experiencia en cuidar personas y cosas así", manifiesta Dulce.

Luego de esa reunión, el supuesto jefe llevó a Dulce a la casa donde se suponía que estaba la persona que debería cuidar. Allí Dulce fue violada y comprobó de la peor forma posible la magnitud del engaño.

Una semana después la misma "mujer" contactó a Dulce por una red social y le dijo que le habían tomado un video mientras la violaban y que si ella no accedía a tener nuevamente relaciones sexuales con el agresor, subirían ese video a las redes sociales, haciéndolo público y arruinándole la vida, lo que la asustó mucho.

Esta amenaza y abusos se mantuvieron por dos años, hasta que su hermana encontró mensajes en el celular de Dulce y descubrió el hecho. No dudó en contarles a sus padres,

quienes apoyaron a Dulce incondicionalmente.

La perspectiva de Dulce respecto al mundo virtual de la web y redes sociales cambió de forma sustancial debido a esta dura experiencia.

Según la cita realizada, "Si volviera a usar las redes sociales sólo tendría contacto con las personas con las que realmente hablo. Creo que la popularidad no importa, porque de qué te sirve tener tantos amigos en las redes sociales si no hablas con ninguno, sólo por likes, no tiene sentido, sino que tener a los verdaderos amigos que estarán contigo en todo momento" comenta Dulce.

Dora, la mamá de Dulce, dice que debido a los muchos trabajos que les dejan en el colegio, contrató servicios de internet para su hogar y que paradójicamente ella lo vio como una forma de cuidar a sus hijas, ya que así se mantendrían dentro de su hogar, sin la necesidad de ir a otros lugares y correr algún peligro. Nunca se imaginó que el riesgo podía estar adentro.

Continuando con la cita mencionada, UNICEF junto con la Embajada de Suecia y la Embajada Británica promueven que las niñas, niños y adolescentes hagan un uso seguro del internet y redes sociales.

En este sentido, se crearon dos unidades especializadas para la investigación de los delitos de explotación sexual infantil en línea (una en el Ministerio Público y una en la Policía Nacional civil), así como creación de la Fiscalía Especializada de Niñez y

Adolescencia Víctima.

Se está contribuyendo en el aumento de las habilidades técnicas de Jueces, Fiscales, Policías, Peritos y otros funcionarios públicos vinculados a los procesos de investigación criminal, persecución penal, protección y atención a la niñez violentada o explotada sexualmente en línea.

También abogan por la entrega de información para que los padres, maestros, tutores y la sociedad en general, velen por el derecho de las niñas y niños a una navegación segura en línea. Por lo que se realizó un estudio de percepción sobre la prevención de la explotación sexual y el abuso de niñas, niños y adolescentes en línea. De la que partió la estrategia de comunicación para informar a niños, niñas, adolescentes, padres, maestros y autoridades sobre los riesgos de la explotación sexual en línea llamada ¨Me Conecto Sin Clavos¨.

Asimismo, prosiguiendo con la cita, la iniciativa Global #WeProtect para la prevención y protección a la niñez frente a la violencia y explotación sexual en línea, de la cual UNICEF forma parte, ha permitido también el involucramiento de actores gubernamentales, no gubernamentales, sector académico y sector privado en acciones orientadas a la protección de la niñez en línea. cabe resaltar que el gobierno de Guatemala recientemente ha manifestado su compromiso para impulsar dicha iniciativa.

El violador de Dulce fue arrestado y actualmente se encuentra esperando juicio.

4.2.6 Modalidades de estafa en línea

"Con el objetivo de prevenir a los guatemaltecos de ser víctima de estafas en plataformas digitales, el Ministerio Público daio a conocer las modalidades detectadas por medio de investigaciones que realiza la Fiscalía de Distrito Metropolitano, las cuales han sido utilizadas para engañar y estafar a las víctimas en la compra-venta de celulares, objetos diversos y vehículos"[16]

De acuerdo con la cita referida, tomando en cuenta las investigaciones realizadas, estos hechos ilícitos ocurren con personas que anuncian en redes sociales o sitios web, donde ofrecen productos para la venta o buscan comprar mercadería, en ambas modalidades, las víctimas son afectadas en su patrimonio a través de engaños.

Según la consulta realizada, en esta modalidad, el agraviado es quién realiza la publicación en el sitio web para vender un objeto; el sindicado contacta a la víctima vía telefónica, donde acuerdan el precio, la forma de pago y la entrega del objeto; sin embargo, el sindicado realiza el pago del objeto a través del depósito de un cheque de un banco distinto; estos cheques, por lo general, corresponden a una cuenta cancelada, es falsa o con reporte de robo.

Por medio de la investigación se establece que en estos casos el agraviado hace la

[16]https://www.mp.gob.gt/noticia/ministerio-publico-ha-detectado-modalidades-de-estafa-en-linea/. **Ministerio Público ha detectado modalidades de estafa en línea.** (Consultado el 22 de agosto de 2021).

entrega del objeto y no se percata de que el pago no será acreditado a su cuenta bancaria; puesto que, se debe esperar el pago por compensación y hasta que la compensación ocurre, se percata que el cheque depositado no le será pagado porque tiene revocatoria de orden de pago o bien porque el cheque es falso.

Asimismo, se obtuvieron las recomendaciones para evitar caer en estos abusos:

- Utilizar plataformas electrónicas seguras.
- Verificar el perfil del vendedor y/o comprador si la plataforma tiene alguna referencia o calificaciones
- Evitar brindar datos personales, como dirección de residencia, nombres de familiares, números de tarjetas de crédito y/o débito.
- Si es necesario reunirse en lugares públicos, debe hacerse donde haya cámaras de seguridad en el lugar.
- No aceptar pago por medio de cheque, que el pago sea únicamente en efectivo o transferencia electrónica.
- Si se trata de la compra-venta de un vehículo, verificar en PNC y SAT que el mismo se encuentre activo y sin reporte de robo.
- Se debe optar por pagos contra entrega, de preferencia.
- No se debe ingresar a enlaces de mensajes de ofertas que le lleguen por whatsapp.

Es necesario mencionar que, es también responsabilidad de los padres de familia de supervisar las páginas a las cuales se meten sus hijos; puesto que, se han dado hasta suicidios en sitios, en los cuales se les pide hacer juegos diabólicos; donde los perdedores

deben morir; no únicamente dejarlo al Estado y al ente investigador, sino erradicar el problema en casa.

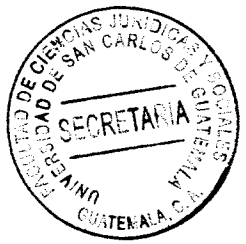
CONCLUSIÓN DISCURSIVA

En el transcurso de la investigación se analizó el derecho penal, en relación a cómo dentro del marco legal guatemalteco, aun no se cuenta con los medios suficientes para proteger los derechos de los ciudadanos; teniendo en cuenta que, hoy en día existe una serie de accesos cibernéticos que les permite, a los delincuentes, realizar actos ilícitos con mayor facilidad y que quedan en la impunidad; debido a que, se pueden ocultar en perfiles falsos, o simplemente cometer delitos a distancia; asimismo, se evidenció la existencia de programas diversos que pueden manipularse y crearse con la tecnología para adecuarlos a fines ilícitos; haciendo de las redes sociales, un medio para cometer delitos en el anonimato y falsificación de perfiles, que casi siempre quedan impune.

Sin embargo, el sistema de justicia resulta ineficiente, al salir de su control el cumplimiento de su deber, de velar y proteger los derechos de los ciudadanos; dejando clara la necesidad de normar, aquellos delitos que se cometen utilizando las redes sociales.

Se deben implementar recursos que verdaderamente protejan los intereses de los guatemaltecos; es claro que, aun cuando existen derechos establecidos, dentro de la Constitución Política de la República de Guatemala, así como en la normativa interna; éstos no son atendidos y el ente encargado de la persecución penal, es insuficiente para poder detener los actos delincuenciales que se presentan en el día a día; ahora, dotados los delincuenres de herramientas que les permite delinquir de una forma fácil; escudándose en el anonimato. Pero se debe considerar, también que, sean los padres de familia los que apoyen erradicando el problema desde los hogares.


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



BIBLIOGRAFÍA

BACIGALUPO, Enrique. **Lineamientos de la teoría del delito**. Tercera ed. Bs. As. Ed. Hammuarabi. 1994

BUSTOS RAMÍREZ, Juan. **Manual de derecho penal. Parte general**. 3ª. ed. Barcelona, España. Ed. Ariel, S.A. 1989

CÁMPOLI, Gabriel Andrés. **Delitos informáticos en la legislación mexicana. Instituto Nacional de Ciencias Penales**. México. 2007

DE LEÓN VELASCO, Héctor Aníbal. **Resúmenes de derecho penal**. Décimo Segunda ed. Guatemala, Guatemala. Ed. Chockmen. 2000

https://nomada.gt/blogs/redes-sociales-una-ventana-a-los-delitos-sexuales/ **Redes sociales: una ventana a los delitos sexuales.** (Consultado del 23 de agosto de 2021).

https://www.unicef.org/guatemala/historias/redes-sociales-nuevas-oportunidades-y-nuevos-peligros. **Redes sociales: nuevas oportunidades y nuevos peligros.** (Consultado el 24 de agosto de 2021).

https://www.mp.gob.gt/noticia/ministerio-publico-ha-detectado-modalidades-de-estafa-en-linea/. **Ministerio Público ha detectado modalidades de estafa en línea.** (Consultado el 22 de agosto de 2021).

HURTADO POZO, José. **Nociones básicas de derecho penal**. Lima, Perú. Ed. Dili. 1987

JIMENEZ DE ASÚA, Luis. **La ley y el delito. Principios de derecho penal**. 3ª. ed. Corregida y actualizada. Buenos Aires, Argentina. Ed. Hermes. 1959

LÓPEZ BETANCOURT, Eduardo. **Delitos en particular**. México. Ed. Porrúa. 2001

LORENZETTI, Ricardo Luis. **La oferta como apariencia y la aceptación basada en la confianza**. Revista de Direito do Consumidor 35/11. Sao Paulo. 2000

NUÑEZ, Ricardo. **Manual de derecho penal. Parte general**. Tercera ed. Córdova, Argentina. Ed. Marcos Lerner. 1987

REYNA ALFARO, Luis. **Pornografía e internet: aspectos penales**. Argentina. AR: Revista de derecho informático.

VELÁZQUEZ ELIZARRARAS, Juan Carlos. **Instauración de un marco legal internacional de internet**. México. 2017

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, 1973.

Código Procesal Penal. Decreto número 51-92 del Congreso de la República de Guatemala, 1952.

Ley del Organismo Judicial. Decreto número 2-89 del Congreso de la República de Guatemala.

Ley Orgánica del Ministerio Público. Decreto número 135-97 del Congreso de la República de Guatemala, 1997.

Iniciativa de Ley de Delitos Informáticos. Número de registro 4055. 2009.