

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



**LA IMPORTANCIA DE TIPIFICAR EL PHISHING  
COMO DELITO EN EL CÓDIGO PENAL**

**SERGIO CIFUENTES CHETE**

**GUATEMALA, NOVIEMBRE 2010**

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

**LA IMPORTANCIA DE TIPIFICAR EL PHISHING  
COMO DELITO EN EL CÓDIGO PENAL**

**TESIS**

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

**SERGIO CIFUENTES CHETE**

Previo a conferírsele el grado académico de

**LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES**

**Y los Títulos Profesionales de**

**ABOGADO Y NOTARIO**

Guatemala, noviembre de 2010

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

DECANO:	Lic. Bonerge Amilcar Mejía Orellana
VOCAL I:	Lic. César Landelino Franco López
VOCAL II:	Lic. Gustavo Bonilla
VOCAL III:	Lic. Luis Fernando López Díaz
VOCAL IV:	Br. Mario Estuardo León Alegría
VOCAL V:	Br. Luis Gustavo Ciraiz Estrada
SECRETARIO:	Lic. Avidán Ortiz Orellana

**TRIBUNAL QUE PRACTICÓ**  
**EL EXAMEN TÉCNICO PROFESIONAL**

**Primera Fase:**

PRESIDENTE:	Lic. Ronaldo Sandoval Amado
VOCAL:	Lic. Rafael Morales Solares
SECRETARIO:	Lic. Jaime Ernesto Hernández Zamora

**Segunda Fase:**

PRESIDENTE:	Lic. Juan Ramiro Toledo Álvarez
VOCAL:	Lic. Juan Carlos López Pacheco
SECRETARIO:	Licda. Dora Renee Cruz Navas

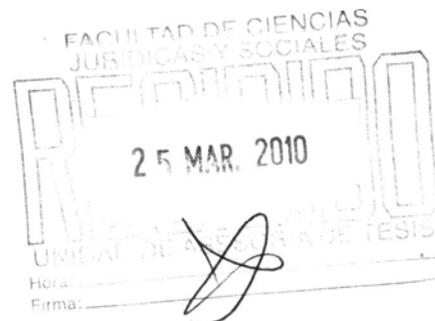
**RAZÓN:** “Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis”. (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del examen general público).”

**LICENCIADO OMAR AUGUSTO CONTRERAS RAMIREZ**  
**ABOGADO Y NOTARIO**  
**COLEGIADO 5982**



Guatemala, 08 de Marzo del 2010

LICENCIADO:  
MARCO TULLIO CASTILLO LUTIN  
JEFE DE LA UNIDAD DE TESIS  
FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES  
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



**Señor Jefe de la Unidad de Asesoría de Tesis:**

Como asesor de tesis del bachiller **SERGIO CIFUENTES CHETE**, con el carné estudiantil número: 9118902; en la elaboración del trabajo de tesis intitulado: **"LA IMPORTANCIA DE TIPIFICAR EL PHISHING COMO DELITO EN EL CODIGO PENAL"**, me complace manifestarle que el presente trabajo de tesis, satisface los siguientes requerimientos:

- **Metodología y técnicas de investigación:** se usó cuidadosamente en todas las etapas del método científico a lo largo de toda la investigación. En el desarrollo capitular, el bachiller **SERGIO CIFUENTES CHETE** se valió del método analítico, para mantener la congruencia y no perder la dirección temática.
- **Contenido científico y técnico:** en la resolución de la problemática objeto de esta investigación, el bachiller **SERGIO CIFUENTES CHETE** hizo uso pertinente de los métodos científicos y técnicas de investigación de acuerdo a la rigidez científica en todas las etapas del proceso de investigación.
- **Las conclusiones y recomendaciones:** fueron redactadas de forma sencilla, que permitirá entender el fondo de la temática desarrollada.
- **Contribución científica:** este trabajo alertan a los usuarios del sistema bancario y a las entidades bancarias y de crédito, del peligro de daño a diversos bienes protegidos, por la utilización inapropiada de la información obtenida mediante la técnica de la pesca de datos y suplantando la identidad de las personas.
- **La redacción:** se advierte en este trabajo de investigación el uso de un lenguaje técnico y una redacción clara que facilitará la comprensión del tema.
- **Bibliografía utilizada:** es de considerable actualidad y de importantes autores.

**LICENCIADO OMAR AUGUSTO CONTRERAS RAMIREZ**

**ABOGADO Y NOTARIO  
COLEGIADO 5982**



En ésta investigación se hace un análisis jurídico penal, para determinar los sujetos responsables de la comisión de los delitos informáticos, proponiendo la tipificación del phishing como delito, que afecta el patrimonio de entidades bancarias y de crédito, al ingresar sin autorización a las cuentas de los clientes.

El bachiller SERGIO CIFUENTES CHETE, durante todo el proceso de la investigación y elaboración del informe final de la investigación, tuvo el empeño de hacer las correcciones y modificaciones que el suscrito estimó oportunamente pertinentes, por lo que:

Emito **DICTAMEN FAVORABLE**, pues el trabajo de tesis de mérito, cumple con los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, para ser discutido en el Examen Público, previo **DICTAMEN** del señor Revisor.

Atentamente,

A large, stylized handwritten signature in black ink, appearing to read 'Omar Augusto Contreras Ramirez'.

**LIC. OMAR AUGUSTO CONTRERAS RAMIREZ  
ASESOR**

*Lic. Omar Augusto Contreras Ramirez  
Abogado y Notario*

UNIVERSIDAD DE SAN CARLOS  
DE GUATEMALA



FACULTAD DE CIENCIAS  
JURÍDICAS Y SOCIALES

Ciudad Universitaria, zona 12  
Guatemala, C. A.



**UNIDAD ASESORÍA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES.** Guatemala, diez de junio de dos mil diez.

Atentamente, pase al (a la) **LICENCIADO (A) RANULFO RAFAEL ROJAS CETINA**, para que proceda a revisar el trabajo de tesis del (de la) estudiante **SERGIO CIFUENTES CHETE**, Intitulado: "LA IMPORTANCIA DE TIPIFICAR EL PHISHING COMO DELITO EN EL CÓDIGO PENAL".

Me permito hacer de su conocimiento que está facultado (a) para realizar las modificaciones de forma y fondo que tengan por objeto mejorar la investigación, asimismo, del título de trabajo de tesis. En el dictamen correspondiente debe hacer constar el contenido del Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, el cual dice: "Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes, 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, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que estimen pertinentes".

  
**LIC. MARCO TULIO CASTILLO LUTÍN**  
**JEFE DE LA UNIDAD ASESORÍA DE TESIS**

cc. Unidad de Tesis  
MTCL/sllh.

# LIC. RANULFO RAFAEL ROJAS CETINA

Abogado y Notario Colegiado 4621

Guatemala, 20 de julio de 2010



**Lic. Marco Tulio Castillo Lutín**  
**Jefe de la Unidad de Asesoría de Tesis**  
**Facultad de Ciencias Jurídicas y Sociales**  
**Universidad de San Carlos de Guatemala**  
**Su Despacho.**



**Señor Jefe de la Unidad de Asesoría de Tesis:**

Como revisor de tesis del bachiller: **SERGIO CIFUENTES CHETE**, con el carné estudiantil número: 9118902; en la elaboración del trabajo de tesis titulado: **“LA IMPORTANCIA DE TIPIFICAR EL PHISHING COMO DELITO EN EL CODIGO PENAL”**, me complace manifestarle que el presente trabajo de tesis, satisface los siguientes requerimientos:

- a) **Contenido científico y técnico:** El bachiller **SERGIO CIFUENTES CHETE** para resolver la problemática empleó apropiadamente en todas las etapas del proceso de esta investigación, los métodos y técnicas científicas; apreciándose en la comprobación de la hipótesis planteada conforme a la proyección científica de la investigación.
- b) **Metodología y técnicas de investigación:** A lo largo del trabajo de investigación se hizo uso estricto de las etapas del método científico; asimismo, mediante el método deductivo se parte de lo general para llegar a lo particular sintetizándose en su aporte personal; de tal cuenta en el desarrollo capitular se exponen tanto las doctrinas existentes sobre el derecho penal y la teoría del delito, seguidamente se hace una reseña de los delitos informáticos, para arribar en el último capítulo lo relativo al delito de phishing, con sus elementos, que constituye la síntesis que se desprendió de análisis de lo que hay legislado y en la doctrina de dicha temática. Cabe hacer notar que también se valió del método analítico en el desarrollo capitular, para mantener la congruencia y no perder la dirección temática.
- c) **La redacción:** El ponente uso un lenguaje altamente técnico y una redacción clara y sencilla que permite la fácil comprensión de la temática.

# LIC. RANULFO RAFAEL ROJAS CETINA

Abogado y Notario Colegiado 4621



- d) **Contribución científica:** Expone los elementos técnicos y jurídico-doctrinarios que permiten el reconocimiento de la autoría de los sujetos activos y pasivos que participan en la comisión de los delitos informáticos, en especial el delito de phishing, que podrían afectar una diversidad de bienes jurídicamente protegidos, por tener acceso no autorizado a cuentas de clientes de instituciones bancarias o de crédito.
- e) **Las conclusiones y recomendaciones:** El trabajo al haber sido desarrollado dentro del rigor de la estructura metodológica formal que abarca las etapas del método y conocimiento científico, lógicamente converge en una serie de valiosas conclusiones y recomendaciones, que podrían ser consideradas por las autoridades invocadas para su implementación a través de normas jurídicas penales que tipifiquen el phishing como delito.
- f) **Bibliografía utilizada:** el material bibliográfico y documental empleado a criterio del suscrito es de considerable actualidad.

Como bien lo establece el título de la tesis, en ésta investigación se hace un análisis jurídico penal, sobre el uso de los medios informáticos para obtener datos de una persona y así suplantar su identidad para cometer delitos que pueden perjudicar varios bienes o derechos tutelados de las personas. Es por ello, que la informática, los recursos electrónicos y herramientas de comunicación como internet, pueden ser medios para cometer delitos. En el presente trabajo de tesis se propone atinadamente la necesidad de tipificar el phishing como delito en nuestro código penal, toda vez que la globalización y la aplicación de la informática en todos los ámbitos sociales, culturales, laborales, comerciales y patrimoniales de las personas, aunado a la falta de legislación penal aplicable a este caso concreto, hacen a los usuarios de internet ser presa fácil de ser suplantada su identidad y pone en peligro su patrimonio.

El bachiller SERGIO CIFUENTES CHETE, durante todo el proceso de la investigación y elaboración del informe final de la investigación, tuvo el empeño de hacer las correcciones y modificaciones que el suscrito estimó oportunamente pertinentes, por lo que: Emito **DICTAMEN FAVORABLE**, pues el trabajo de tesis de mérito, cumple con los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, para ser discutido en el Examen Público.

Atentamente,

LIC. RANULFO RAFAEL ROJAS CETINA  
ABOGADO Y NOTARIO  
COLEGIADO 4621

*Ranulfo Rafael Rojas Cetina*  
ABOGADO Y NOTARIO

13 Avenida 9-80 apartamento 142 zona 2. Guatemala, Ciudad.

Teléfono 22702871

UNIVERSIDAD DE SAN CARLOS  
DE GUATEMALA



FACULTAD DE CIENCIAS  
JURÍDICAS Y SOCIALES

Edificio S-7, Ciudad Universitaria  
Guatemala, C. A.



DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES.

Guatemala, ocho de noviembre del año dos mil diez.

Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante SERGIO CIFUENTES CHETE, Titulado LA IMPORTANCIA DE TIPIFICAR EL PHISHING COMO DELITO EN EL CÓDIGO PENAL. Artículos 31, 33 y 34 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.-

MTCL/sllh.



## DEDICATORIA

- A DIOS: Por brindarme sabiduría, fortaleza y confianza para alcanzar el triunfo que tanto he buscado. Gracias Padre Celestial por permitirme compartir este día contigo y con todos mis seres queridos.
- A MIS PADRES: ZENON CIFUENTES JAYES (†), y ANDREA CHETE CHIROY. Con profundo amor y gratitud por haberme dado vida, por su apoyo y ayuda a lograr tan anhelado triunfo, el cual es el mejor tributo a su cariño y confianza a lo largo de mi vida.
- A MI ESPOSA: DIANA MARISOL LOPEZ MEDINA: Con profundo amor y agradecimiento por su cariño, apoyo, comprensión, paciencia y fe en mí. Gracias por ser cómplice de Dios para darme hijos tan maravillosos.
- A MIS HIJOS: SERGIO ANDRES y SEBASTIAN EDUARDO: Por ser el regalo que Dios hizo en mí; ya que, con sólo existir, lograron dar sentido a mi vida, siendo la motivación y fuerza necesaria que me impulsó a lograr este grado académico.
- A MIS HERMANOS: RAMIRO, SALIN OMERO, CELESTE ANDREA y VILMA YOLANDA; Con amor fraternal.
- A MIS ABUELOS: ALFONSO CHETE LOPEZ (†) y PILAR CHIROY (†). Porque en vida me brindaron tanto cariño y apoyo incondicional, que Dios los tenga en su gloria.

- A MIS TIOS Y PRIMOS: Por su apoyo incondicional y por sus sabios consejos. En especial a LUIS ALFONSO PEREZ CHETE; con mucho cariño, admiración y respeto.
- A MIS SOBRINOS: WILSON RAMIRO, JENNIFER XIOMARA, DENIS GABRIEL, GENESIS MASSIEL, NOA SALIN. Que este triunfo, les permita entender que todas las metas se pueden alcanzar.
- A MIS SUEGROS: JOSE LUIS ROMEO LOPEZ ESCOBEDO y MARIA MEDINA LOPEZ (†), con respeto y cariño.
- A MIS AMIGOS: Por compartir de manera especial mis alegrías, tristezas y logros.
- A MI ASESOR Y REVISOR DE TESIS: OMAR AUGUSTO CONTRERAS RAMIREZ y RANULFO RAFAEL ROJAS CETINA, por su apoyo en la elaboración y presentación de esta tesis.
- EN ESPECIAL A: LOTTY, PATTY y JULY, LOPEZ MEDINA y sus familias, por sus atenciones y su disposición a ayudarme siempre.
- A: Licenciado JORGE MARIO GARCIA PERALTA, por la amistad que nos ha brindado como familia.
- A: RUBEN AVILES y JAIME SALAZAR, por su amistad y disposición a ayudar, gracias.
- A: GABRIEL ERNESTO BARILLAS LOPEZ y JOSE ROLANDO RIVAS LOPEZ, porque me han motivado a la superación.

A: Mis padrinos de graduación, ya que han sido importantes en el desarrollo de mi vida familiar, profesional, académica y laboral.

A: La Universidad de San Carlos de Guatemala, en especial a La Facultad de Ciencias Jurídicas y Sociales, por mi formación profesional.

A: Mi patria Guatemala, que Dios la bendiga siempre.

## ÍNDICE

	Página
Introducción. ....	i
<b>CAPÍTULO I</b>	
1 El derecho penal. ....	01
1.1. Derecho penal Objetivo. ....	01
1.2. Estructura de la norma penal. ....	08
1.3. Leyes incompletas y leyes penales en blanco. . . . .	15
1.4. Los fundamentos y los fines de la pena. ....	23
<b>CAPÍTULO II</b>	
2 El delito y sus elementos. ....	27
2.1. Definición de delito. ....	28
2.2. La teoría del delito. ....	31
2.3. Clasificación de los delitos. ....	36
2.4. Fases de la realización del delito. ....	38
2.5. Sujetos y objeto del delito. ....	42
<b>CAPÍTULO III</b>	
3 Delitos informáticos. ....	45
3.1. Definición del delito informático. ....	45
3.2. Características de los sujetos del delito informático. ....	51
3.3. Bien jurídico protegido. ....	54
3.4. Clasificación de los delitos informáticos. ....	57
3.5. Impacto de los delitos informáticos. ....	62
3.6. Seguridad contra los delitos informáticos. ....	65
3.7. Problemas de persecución. ....	68
<b>CAPÍTULO IV</b>	
4 Importancia de tipificar el phishing como delito en el Código Penal. . .	71
4.1. El delito de phishing. ....	72
4.2. El phishing y el bien jurídico. ....	85
CONCLUSIONES. ....	93
RECOMENDACIONES. ....	95
BIBLIOGRAFÍA. ....	97

## INTRODUCCIÓN

Las nuevas formas de comunicación surgidas a partir de la revolución tecnológica a finales del siglo XX, ha generado formas completamente diferentes de realizar las actividades cotidianas de las personas, tanto en su hogar, su trabajo y su manejo financiero, así como de su relación con el sistema bancario; de igual manera, también ha generado nuevos problemas sociales que el derecho penal debe darle soluciones porque se trata de acciones que atentan contra bienes jurídicos que aún cuando en muchos casos todavía no son tipificados como delitos, son un atentado contra la paz social, lo cual resulta urgente su tipificación. .

A partir de esta realidad, surge la idea de analizar una de esas prácticas que afectan el derecho a la información, especialmente aquella que es sensible como es el caso de los datos personales, la cual en esencia se vulnera para afectar el patrimonio de las personas, por lo que se planteó como problema cuál es la importancia que se tipifique el phishing como delito, puesto que el principal objetivo de esta acción son los clientes de los bancos; de ahí que se propusiera como hipótesis, la cual fue debidamente comprobada, que era importante para los bancos, porque de esa manera lograban garantizarle a sus usuarios la seguridad de que no serían objeto de estafa. Los objetivos se orientaron a establecer los elementos del delito, la tipificación del mismo, así como las distintas denominaciones que tiene la nueva rama jurídica denominada derecho informático.

A partir de haber obtenido la información necesaria se realizó el informe final de tesis que consta de cuatro capítulos; el primero hace referencia al derecho penal, su evolución, los elementos que lo integran y su importancia; en el segundo, se estudia al delito y sus elementos lo cual permitió establecer la manera en que se define un delito, su tipificación, su antijuridicidad, la culpabilidad, así como la importancia de la pena y las medidas de seguridad; en el tercer capítulo se hace un extenso estudio de los delitos informáticos, su origen, sus características, las definiciones que se le han dado y la importancia de la explicación teórica de los mismos para que puedan ser debidamente tipificados en la legislación nacional; mientras que en el cuarto, se explican los elementos del delito de phishing, el bien jurídico que se busca proteger, a los sujetos activos y pasivos, así como la importancia de su tipificación en el código penal guatemalteco.

Que sirva esta investigación para que las instituciones bancarias y de crédito mejoren sus controles de vigilancia e informen a sus clientes del peligro que genera el acceso no autorizado de sus datos personales, ya que de esta forma los usuarios de banca electrónica la utilizarán con la confianza que genera la seguridad que las estas entidades le brindan.

# CAPÍTULO I

## 1. El derecho penal

En la presente tesis se considerará al derecho penal como el conjunto de normas jurídicas que tienen al delito como presupuesto, al cual se le asocian penas y/o medidas de seguridad como consecuencia jurídica.

“El derecho penal es un medio de control social, y este último puede ser comprendido como un conjunto de modelos culturales y de símbolos sociales y también de actos, a través de los cuales dichos símbolos y modelos son determinados y aplicados. Con ellos, se trata de superar las tensiones sociales: generales, de grupo y/o de individuos. Cualquiera que sea el sistema político-económico de una sociedad, el Estado tratará de desmontar los elementos conflictivos potenciales y de aceitar la maquinaria de la circulación social”.<sup>1</sup>

### 1.1. Derecho penal objetivo

El derecho penal como parte del derecho en general, es utilizado para controlar, orientar y planear la vida en común, mediante él, se determinan y definen ciertos comportamientos, los cuales no deben ser realizados o, queridos o no, deben ser ejecutados; a fin de conseguir que los miembros de la comunidad omitan o ejecuten, según el caso, tales actos, se recurre a la amenaza de una sanción.

---

<sup>1</sup> Alegría Hidalgo, Juan Luís, **Derecho penal. Parte general**, pág. 12.

El Estado espera, en primer lugar, orientar los comportamientos de los individuos, motivándolos a realizarlos de cierta manera, para así lograr la aplicación de ciertos esquemas de vida social. Sólo cuando fracasa su tarea de evitar la realización de los actos no deseados, interviene el funcionario judicial para hacer efectiva la sanción penal.

Por eso es que la actividad punitiva constituye uno de los dominios en que el Estado ejerce su poder, con el fin de establecer o conservar las condiciones necesarias para el normal y buen desenvolvimiento de la vida comunitaria. La orientación que dé a su actividad penal, está determinada por las opciones sociopolíticas que haya adoptado en relación a la organización de la comunidad, en general. Por ello, la política criminal del Estado se halla encuadrada y condicionada por su política social general.

Debido a la naturaleza de la intervención penal, siempre ha existido la preocupación de establecer límites al poder estatal. Este esfuerzo se ha orientado a la búsqueda de la justificación de la pena, y a la determinación de un criterio suficientemente claro que permita discernir las acciones que deben ser prohibidas, para la fijación de las condiciones cuya preexistencia permita la imposición de la sanción; y la especificación de los casos en que la actividad punitiva es oportuna, necesaria y positiva. Esta compleja problemática, que afecta los fundamentos mismos del derecho penal, ha tratado de ser resuelta mediante el estudio del fin y naturaleza de la pena. No es otra la finalidad de las denominadas teorías de la pena: absoluta, relativa y mixta, por eso es que, con la finalidad de orientar la conducta de las personas, mediante reglas

generales de carácter penal, se debe determinar, en primer lugar, cuáles son los comportamientos reprimibles; ya que el objetivo del derecho penal es evitar su realización.

“Una conquista del derecho penal liberal es el de haber determinado que sólo deben ser reprimidos penalmente, los actos que ponen en peligro o lesionen bienes que sean fundamentales para la vida en común. De ahí que se considere que toda norma jurídico-penal, tiene que fundamentarse sobre un juicio de valor positivo respecto a tales bienes vitales. Esta concepción, surgió en contra de la tradicional teoría que consideraba a la infracción como un ataque contra los derechos subjetivos de la persona y cuya base era la teoría del contrato social”.<sup>2</sup>

Lo que interesa es no dejar, en la medida de lo posible, en manos de quien detenta el poder, un arbitrio ilimitado en la determinación de los bienes que deben ser penalmente protegidos y de cuales son los comportamientos que deben ser prohibidos. Un concepto material del bien jurídico sería en cierta medida capaz de permitir una crítica de la actividad legislativa penal, porque los bienes jurídicos son tales, no porque el legislador los considere merecedores de protección jurídica, sino porque, son en sí presupuestos indispensables para la vida en común; por ejemplo, la vida, la salud, la libertad de acción, de expresión y de creencia, etc.; se trata, en realidad, de aquellas condiciones fundamentales que constituyen el *mínimum* de derecho natural que es necesario reconocer.

---

<sup>2</sup> **Ibid.**

“El recurrir al criterio de bien jurídico como elemento objetivo para la determinación de las acciones prohibidas, implica, consecuentemente, admitir la concepción de que sólo deben ser reprimidas penalmente las acciones que constituyen un atentado contra tales bienes vitales para la vida comunitaria. En este sentido, sólo las acciones socialmente dañinas son merecedoras de represión penal. Es decir, las que atentan contra un bien jurídico. La presencia evidente e impositiva de esta protección brindada por la ley penal a los bienes jurídicos, ha determinado que la mayor parte de los juristas reconozcan en ella la tarea primaria y fundamental del derecho penal. Sin embargo, no es de olvidar que, conforme lo señalamos al principio, a través del derecho penal el Estado busca, al igual que con el derecho en general, que las personas se comporten de acuerdo a ciertos esquemas sociales; esto es, a forjar y consolidar en ellas cierta conciencia social. El sistema penal tiene la capacidad de inculcar en la población ciertos valores y juicios, los que a su vez se manifestarán en esquemas comunes de conducta moral, que constituyen una barrera contra las tendencias delictivas”.<sup>3</sup>

El derecho penal desarrolla su acción como parte del orden jurídico en general, ya que es un instrumento de la política social del Estado, por lo que tiene un carácter fragmentario y secundario. Es fragmentario, en el sentido de que no tiende a la protección de todo bien jurídico, ni a la defensa de los bienes escogidos frente a cualquier tipo de ataque; y menos aun pretende reprimir toda acción moralmente reprochable. Esta fragmentariedad responde a la necesidad de evitar que el Estado abuse del derecho a castigar, porque sólo debe recurrirse a la fuerza coactiva del ente estatal cuando sea absolutamente necesario; cuando la protección de los bienes

---

<sup>3</sup> **Ibid.**

jurídicos y la consolidación de ciertos esquemas de conducta no sean alcanzables mediante otras previsiones, de allí que se hable de la pena como el último recurso o medida, de no tenerse en cuenta esta regla, se corre el riesgo de producir una hipertrofia del derecho penal, lo que conduce a la creación de situaciones que, precisamente, se busca combatir.

El derecho penal ya no es hoy sólo el derecho de la pena. Se plantea con ello la cuestión de si la denominación derecho penal es, a la vista del nuevo contenido de esta disciplina, lo suficientemente amplia como para dar cabida a una de sus dos integrantes fundamentales, las medidas de seguridad. La respuesta a esta cuestión parece, a primera vista, que ha de ser negativa, porque la expresión derecho penal parece demasiado estrecha para abarcar todo lo que pretende significar hoy.

Como dice Daniel Mezger-Blei: “El derecho penal ha desbordado el marco de su designación literal. La doctrina suele considerar preferible mantener la terminología derecho penal, por mucho que reconozca su actual inexactitud. Sin duda, el argumento de la tradición de que actualmente goza en España y en otros países, como Alemania e Italia, la expresión derecho penal, juega en esta decisión un importante papel. Pero suele argumentarse acudiendo a otros puntos de vista. El de mayor peso es posiblemente el de que la pena sigue siendo la integrante esencial del derecho penal común. En él las medidas de seguridad no ocupan ni en la legislación ni en la ciencia, como tampoco en la práctica, más que un lugar secundario”.<sup>4</sup>

---

<sup>4</sup> **Principios de derecho penal**, pág. 43.

Por eso, en aquellos sectores especiales en que esa relación se invierte, pasando a primer plano la medida de seguridad, como en el derecho de menores, la designación derecho penal debe dejar paso a otras, como la de derecho tutelar de menores.

En defensa de la intitulación derecho penal se alegan otros argumentos, pero su validez puede ser discutida o depende del contenido que se atribuya al derecho penal. Así, el argumento de que el legislador ha elegido el término penal para designar a la rama jurídica que analiza las penas y las medidas de seguridad, tiene en Guatemala, un valor muy elevado, porque el núcleo fundamental de las medidas de seguridad las contiene el Código Penal.

De igual manera, si se analiza la evolución de su denominación, se encuentra que el cambio del concepto derecho criminal al de derecho penal a principios del siglo XIX, no se produce ni por pura casualidad histórica ni por simples pretensiones de fuerza conceptual.

Esta modificación, que a primera vista representa un simple cambio de acento, encierra uno de los cambios valorativos más trascendentales para el derecho penal de la época posterior. En las palabras delito y en la de derecho criminal, se da algo pre jurídico penal, en tanto suena a injusto y a culpabilidad antes de la ley positiva. El término derecho penal alude a la ley, por cuyo solo mandato, se convertirá una determinada conducta desvalorada en delito punible, sometido al poder punitivo del Estado.

Para Maurach, pues, los términos derecho penal aluden a la necesidad de que toda pena se halle prevista por la ley, a diferencia de la expresión derecho criminal, que remite a un concepto pre-jurídico, es decir previo a la ley penal. “Hasta tal punto que, absolutizando los términos del razonamiento, llega a concluir que en este cambio terminológico de derecho criminal a derecho penal se agita el principio rector que ha dominado el derecho penal del siglo XIX y que, tras su provisional desentronización durante la época del totalitarismo, ha ocupado de nuevo el lugar que le corresponde el principio *nulla poena sine lege*”.<sup>5</sup>

Al concepto formal de derecho penal pertenece la problemática de la norma penal. Si el derecho penal se define como conjunto de normas jurídicas penales, importará saber qué naturaleza han de poseer estas normas, **rango jerárquico**, y qué estructura encierran. La primera cuestión enlaza con el problema del principio de legalidad, según el cual sólo la ley es norma jurídica susceptible de tener carácter penal.

“Pero el examen del principio de legalidad encuentra un lugar sistemático más adecuado en el apartado destinado a los límites propios del ejercicio de la facultad punitiva (*ius puniendi*) del Estado, porque ello aclara mejor el significado político-jurídico de ese principio, que desborda ampliamente la problemática del concepto formal de derecho penal y de la norma penal. Estudiarlo ya ahora, sería, sin duda, sobrestimar el aspecto legal del principio de legalidad en perjuicio de su rico contenido político, de imperativo dirigido al legislador”.<sup>6</sup>

---

<sup>5</sup> **Tratado de derecho penal**, pág. 4.

<sup>6</sup> Mir Puig, Santiago. **Introducción a las bases del derecho penal**, pág. 44.

Por consiguiente, de los dos aspectos mencionados de la norma penal, su rango jerárquico y su estructura, sólo el segundo será examinado en este lugar.

## **1.2. Estructura de la norma penal**

En la definición propuesta de derecho penal se parte de normas que asocian consecuencias jurídicas como las penas, las medidas de seguridad y la responsabilidad civil, a presupuestos de delito, estado peligroso y desequilibrio patrimonial, al mismo tiempo que el contenido diferencial de la norma penal, ello describe su estructura, que no es específica de ella sino común a toda norma jurídica formalmente completa; supuesto de hecho o presupuesto, por un lado, y consecuencia jurídica, por otro, constituyen los dos momentos esenciales a la estructura de toda norma de derecho.

“Sería equivocado equiparar precepto y presupuesto, porque el presupuesto no es por sí solo ningún precepto. Pero lo cierto es que, bien entendida, la contraposición de precepto y sanción no se corresponde con la de presupuesto y consecuencia jurídica, sino que responde a una perspectiva distinta. Mientras que este último par de conceptos describe sólo la estructura lógica de la norma, el primero apunta a su esencia imperativa. Presupone, pues, que la norma posee naturaleza imperativa (que es una prohibición o un mandato). Pero aun así resulta incompleto contraponer precepto y sanción, pues en toda norma se expresan dos preceptos distintos, y no sólo uno; el primero, dirigido al ciudadano, le prohíbe u ordena actuar de determinada forma

(norma primaria), y el segundo, que se dirige al juez, le obliga a aplicar la consecuencia jurídica cuando concurra el supuesto de hecho”.<sup>7</sup>

Las normas penales se distinguen de las demás normas jurídicas por el mandato penal de la norma que establece el deber del juez de imponer una pena. Ambos preceptos poseen su sanción; para la norma primaria la prevista en la concreta disposición de que se trate y para la norma secundaria la responsabilidad administrativa y penal prevista en otras disposiciones para los órganos que incumplen el mandato de aplicar aquella sanción legal. Entonces, la distinción precepto-sanción que suele utilizarse para explicar la ley penal, sólo alcanzaría a la norma primaria contenida en ella.

Desde el punto de vista de la estructura lógica sólo es válida la distinción de presupuesto y consecuencia jurídica; la distinción precepto-sanción alude al significado imperativo, más que a la estructura formal, de la norma penal; pero, para que sea válida a ese nivel, debe completarse distinguiendo entre norma primaria y norma secundaria. Ahora bien, adviértase que la estructura lógica representada por la distinción presupuesto-consecuencia, que es la estructura propia de la redacción de las proposiciones jurídico-penales, tiene carácter hipotético: si alguien mata a otro (presupuesto), será castigado (consecuencia). Y esta estructura hipotética es la que corresponde a lo que recibe el nombre de norma secundaria, es decir, la que impone al juez el deber de imponer la sanción. Equivale a decir: si alguien mata a otro, el juez deberá castigarle”.<sup>8</sup>

---

<sup>7</sup> **Ibid.**

<sup>8</sup> **Ibid.**

En otros términos, la redacción de las proposiciones jurídico-penales sólo expresa de forma directa la norma secundaria. La norma primaria, la que prohíbe u ordena una conducta al ciudadano, no se formula directamente por la ley, sino que sólo cabe inferirla indirectamente de la misma. En este sentido pudo decir que el delincuente vulnera la norma concebida como el imperativo dirigido al ciudadano que precede conceptualmente a la ley penal. Las normas pueden ser escritas o no y hallarse previstas fuera del derecho penal, pero lo normal es que se deduzca, implícitamente, de las mismas disposiciones hipotéticas de la ley penal. Según esto, la ley penal expresaría de forma explícita un mandato destinado al juez, por lo que encierra implícitamente una norma dirigida al ciudadano.

Para establecer el delito y la pena, el legislador parte de normas sociales a la hora de decidir qué debe ser castigado, por lo cual tras cada ley penal hay, pues, una norma de comportamiento social o cultural dictada por la sociedad; sin embargo, únicamente la formulada por el legislador crea la obligación de ser respetada, con la sola formulación de la ley penal. Por lo demás, al penalista no le importan más que las normas que se desprendan de las leyes penales. En síntesis, ni son necesarias normas previas a la ley penal, ni cuando existen tienen un significado que no se deduzca ya de la ley penal.

“Un sector de la ciencia penal actual, en parte a partir de la revisión que ha supuesto la doctrina finalista de la acción, vuelve a reclamar la vigencia de las posiciones fundamentales de la teoría de las normas. Que esta formulación sea vista con simpatía desde los principios de la teoría finalista, no puede extrañar, pues la norma, como

imperativo dirigido al ciudadano, aparece adecuada a la esencia final de la acción, dado que un imperativo no es más que solicitud de ordenación de la finalidad en un sentido dado; la naturaleza previa de las normas responde bien al punto de partida metodológico del finalismo, a saber, la vinculación del legislador a estructuras lógico-objetivas pre jurídicas”.<sup>9</sup>

Pero Maurach defiende la teoría de las normas con otros argumentos, al decir que es: “Importante tomar en cuenta la necesidad lógico-jurídica de las normas previas a la ley penal, porque las considera imprescindibles desde la perspectiva de la dogmática jurídico-penal, por la insuficiencia de la sola idea de la lesión de bien jurídico para fundamentar la pena, insuficiencia que se deduce de que la ley no castiga todos los ataques concebibles contra los bienes jurídicos, sino, a menudo, sólo ciertas modalidades de ataque -las más graves- de esos bienes. Así sucede en los delitos contra la propiedad, la cual no se protege penalmente de toda forma de lesión, sino sólo de agresiones especialmente peligrosas”.<sup>10</sup>

La consecuencia de la mencionada insuficiencia de la lesión de bien jurídico para acotar el campo de lo punible sería que para la punición de una lesión de bien jurídico es precisa la existencia previa de una norma que prohíba dicha lesión, lo cual reitera el principio de que no hay delito sin ley anterior que regula el Artículo primero del Código Penal guatemalteco, por eso es que la distinción de ley penal y norma es condición

---

<sup>9</sup> Kuntz, Christian, **La estructura del derecho penal**, pág. 46.

<sup>10</sup> **Ob. Cit**; pág. 6.

necesaria, de que pueda llevarse a cabo satisfactoriamente la delimitación de error de tipo y error de prohibición.

Calliess aborda la cuestión de la estructura de la norma jurídico-penal no como problema en sí mismo, de puro análisis lógico desvinculado de consecuencias ulteriores, sino como base para la solución a la cuestión de la función de la pena, que cree hay que resolver sobre la base de la estructura del derecho penal positivo y no a partir de apriorismos metafísicos".<sup>11</sup>

Esta visión considera que en la proposición jurídico-penal que define el hurto, como en las demás de la parte especial del Código Penal, se hallan presentes distintos sujetos, no aisladamente, sino en una específica conexión. Esta conexión se caracteriza como sigue: mientras que un sujeto activo actúa, en otro sujeto pasivo recae esa actuación y un tercer sujeto, en representación del Estado, está llamado a reaccionar frente a ella con una pena.

Esta conexión entre los sujetos puede describirse como un complejo de expectativas recíprocas, como una red comunicativa en la cual cada sujeto espera no sólo el comportamiento, sino también las expectativas de los otros. Así, el sujeto activo ha de esperar no sólo un determinado comportamiento del tercero como respuesta a su actuar, sino también que el tercero y el sujeto pasivo esperen que se deje determinar en favor de una conducta conforme a derecho. Esta conexión de expectativas tiene lugar, según los delitos, en distintos ámbitos o sistemas sociales: la economía, el Estado o el tráfico diario. Según lo anterior, la estructura de las normas penales es una

---

<sup>11</sup> Calliess, Roberto, **Teoría dogmática del derecho penal**, pág. 15.

estructura basada en la recíproca conexión o comunicación de los tres sujetos; sujeto activo, sujeto pasivo y Estado presentes en ellas.

Calliess prefiere este punto de vista al tradicional por dos razones principales: "1) Porque esa estructura de comunicación intersubjetiva es la misma estructura de toda acción social, de toda "acción comunicativa; 2) porque sólo dicha estructura permite concebir la norma penal no sólo como conducción, sino como regulación".

En la perspectiva de este autor el planteamiento tradicional, que distingue entre supuesto de hecho y consecuencia jurídica, en una relación hipotético-condicional y ve en cada norma un imperativo dirigido a los ciudadanos bajo la amenaza de pena, responde a una dirección ciega, sin control de los resultados y sin que éstos regresen modificando la dirección.

Por eso es que entendida hipotéticamente, condicionalmente, la pena asignada en la proposición jurídico-penal se determina previamente, y sólo es precisa la realización del supuesto de hecho para que automáticamente corresponda la pena. La determinación de la pena es, entonces, la consecuencia última a que conduce la proposición jurídico-penal, y no depende de los resultados que a partir de entonces se consigan con la pena; en este sentido, el esquema tradicional entiende la norma penal como conducción porque la pena se señala previamente, de modo ciego como efecto del delito.

En contraposición a la visión tradicional, se considera que Calliess establece, en cambio, la regulación, que supone tomar en cuenta continuamente los resultados de la dirección, que retroceden orientando a la dirección misma, la cual, a su vez, se adapta a los resultados que va consiguiendo. Ello podrá suceder si la estructura de la proposición jurídica deja de responder al modelo condicional-hipotético, si supuesto de hecho; entonces consecuencia jurídica, para pasar a concebirse como relación comunicativa interdependiente de los tres sujetos, pues tal relación comunicativa se basa en las expectativas de cada uno respecto de los demás y esas expectativas habrán de ir variando según la conducta de los sujetos: así, la pena que el tercero en representación del Estado ha de aplicar, dependerá de los efectos que espere haya de poseer la misma en el sujeto sometido a ella, así como de los resultados que se compruebe vayan produciéndose durante su ejecución.

Como efecto último de la decisión del juez penal, esta visión considera que debe tenerse en cuenta que la norma jurídico-penal sirva a la función de resocialización, la cual sólo puede conseguirse adaptando la pena a los resultados que produce en el condenado.

En cualquier caso, se vislumbra que la estructura de la norma no es una pura cuestión constructiva, de análisis formal, sino que se halla en estrecha relación con el fundamento último del derecho penal. Haber situado en primer plano este aspecto de la problemática de la estructura de la norma jurídico-penal, constituye, sin duda, una aportación de Calliess a la que no cabe renunciar.

### **1.3. Leyes penales incompletas y leyes penales en blanco**

El examen de la estructura de la norma jurídico-penal ha puesto de manifiesto que, desde el punto de vista estático, la misma obedece, como toda norma jurídica, al esquema supuesto de hecho o consecuencia jurídica; sin embargo, por lo general, la expresión completa del contenido de esta estructura no se corresponde con los concretos artículos de las leyes penales, por eso suele destacarse como ejemplo de ello las normas penales en blanco, mas lo cierto es que éstas no ofrecen más que supuestos extremos de lo que es regla en la legislación penal: los artículos legales no acostumbran a coincidir con las normas jurídico-penales completas.

Podría pensarse que la mayor parte de artículos de los Libros I y II del Código Penal, así como los que definen delitos y faltas en las Leyes Especiales, constituyen normas penales completas, por responder a la estructura supuesto de hecho-consecuencia jurídica.

Así, por ejemplo, el Artículo 123 del Código Penal sería considerado como paradigma de norma penal completa: "...quien diere muerte a una persona, supuesto de hecho... al homicida se le impondrá prisión de 15 a 40 años, consecuencia-jurídica. Tal conclusión sería, sin embargo, probablemente inexacta, si por norma completa se entiende aquella que determina exhaustivamente el contenido del presupuesto y de su consecuencia jurídica.

En efecto, un entendimiento literal del Artículo 123, que lo concibiese como norma completa en sí misma, llevaría al absurdo de considerar efectivamente punible todo homicidio, con independencia de que concurriesen causas de justificación o de exclusión de la culpabilidad, y siempre con la pena de reclusión definida en el Código Penal, aunque se hallasen en juego circunstancias modificativas que impusieran el desbordamiento del marco típico de la pena.

Por lo demás, del solo Artículo 123 no se desprende el contenido de la penalidad de 15 a 40 años. Tanto esta penalidad, como los límites del supuesto de hecho y de la concreta sanción aplicable, dependen de preceptos situados en el Libro I del Código Penal, específicamente en el Título III, que regula lo relativo a las causas que eximen de la responsabilidad penal y del Capítulo I del Título IV, de lo relativo a las circunstancias que modifican la responsabilidad penal, siendo estas las circunstancias atenuantes.

En realidad, el Artículo 123 dice más de lo que quiere decir, pues no es cierto que el que matare a otro será castigado siempre con la pena de 15 a 40 años, sino sólo que ello tendrá lugar cuando no concurren causas de justificación ni de exclusión de la culpabilidad, ni tampoco circunstancias modificativas que alteren la pena típica como limitaciones del supuesto de hecho.

Todas estas limitaciones se hallan implícitas en el Artículo 123 porque así lo impone la interpretación sistemática, que obliga a su puesta en relación con otros preceptos del

Código Penal establecidos en el Libro Primero. Por lo que si los preceptos de otros artículos han de completar al Artículo 123, éste no puede considerarse expresión de una norma penal completa.

La doctrina ha advertido el carácter incompleto y complementario de los preceptos previstos en la Parte General, pero suele quedar en el olvido, que tampoco son completos, los preceptos integrados en la Parte Especial. “Así, proposiciones jurídicas incompletas son sólo las que completan o aclaran el supuesto de hecho o la consecuencia jurídica previstos en otras proposiciones jurídicas distintas. No toda disposición de carácter penal alberga una norma completa”.<sup>12</sup>

Por lo anterior se considera que ni las proposiciones contenidas en la Parte Especial ni las que se hallan en la Parte General, encierran por sí solas normas penales completas en cuanto a su contenido, estas son el resultado de la coordinación de ambos tipos de preceptos. A partir de estos elementos, viene a negarse, por esta construcción, el planeamiento tradicional de la relación existente entre tipo y antijuridicidad, ya que se rechaza que la exclusión de la antijuridicidad por obra de las causas de justificación no arrastre consigo la ausencia de tipicidad, puesto que un hecho justificado deja de ser, al mismo tiempo, típico.

“Para la teoría de los elementos negativos del tipo sólo son típicos los hechos: 1) adecuados a un precepto de la Parte Especial (o excepcionalmente a los que definen las formas de imperfecta ejecución, de participación o los actos preparatorios punibles),

---

<sup>12</sup> **Ibid.**

y 2) no amparados por ninguna causa de justificación. Esto se expresa asignando al tipo dos partes, una positiva, coincidente con el concepto de tipo mantenido por la doctrina tradicional y otra negativa, integrada por la ausencia de causas de justificación".<sup>13</sup>

Todo este planteamiento carecería de sentido si el precepto que según la doctrina clásica describe el tipo constituyese una norma penal completa, por lo menos en cuanto a la configuración del supuesto de hecho. La teoría de los elementos negativos del tipo presupone que el tipo completo requiere la puesta en relación de los preceptos que conminan provisionalmente con pena ciertas conductas y los que definen causas de justificación.

La consecuencia más importante de la teoría de los elementos negativos del tipo, es el tratamiento del error sobre los presupuestos de las causas de justificación como error de tipo y no como error de prohibición, como quiere el finalismo.

Pero debe señalarse que el tipo completo propugnado por la teoría de los elementos negativos del tipo no constituye todavía por sí solo el supuesto de hecho de una norma jurídico-penal completa; además de la ausencia de causas de justificación, la aplicación de la consecuencia jurídica asignada al tipo precisa la falta de causas de exclusión de la culpabilidad y de circunstancias modificativas que determinen la superación del marco abstracto de la pena, con lo cual se quiere decir que la teoría de los elementos negativos del tipo no lleva a la búsqueda de la norma completa, sino que es sólo una

---

<sup>13</sup> **Ibid.**

de las consecuencias de que los artículos de la Parte Especial encierren normas incompletas.

La explicación de las razones que tuvo el legislador para elegir la vía de la escisión de las normas jurídico-penales en distintas proposiciones legales, en lugar de hacer corresponder éstas con normas completas, son de economía legislativa, pues si para cada figura de delito se tuviera que aludir a todas las proposiciones complementarias de la Parte General, el Código Penal debería repetir su Libro I tantas veces cuantos delitos contienen el Libro II y las faltas del Libro III, lo que resulta a todas luces absurdo.

Los preceptos que regulan los grados de imperfecta ejecución, las formas de participación y los actos preparatorios punibles son, por ello, doblemente incompletos: por un lado, en cuanto, como todo delito, suponen la remisión a las proposiciones que regulan las causas de exclusión y modificación de la responsabilidad criminal y el contenido de las distintas penas; por otro lado, porque poseen la particularidad de que su propio tipo positivo resulta de la coordinación de los preceptos de los Libros II y III del Código Penal con los que regulan esas figuras en el Libro I del mismo Código.

“La razón de la mencionada especialidad es paralela a la que justifica el carácter incompleto de la gran mayoría de preceptos penales: la economía legislativa, que aconseja reducir a fórmulas generales la posibilidad de extender el elenco de hechos típicos por razón de imperfecta ejecución, de participación o de realización de ciertos

actos preparatorios de cada uno de los actos descritos en la Parte Especial, en lugar de repetirlos para cada caso. La coincidencia de las razones que explican la necesidad de completar todo precepto de la Parte Especial con otros de la Parte General, por una parte, y la de coordinar los preceptos que regulan los grados de imperfecta ejecución, las formas de participación y los actos preparatorios punibles, con los que definen el delito consumado para obtener el propio tipo positivo de dichas figuras, por otra parte, no excluye importantes diferencias en ambos grupos de supuestos”.<sup>14</sup>

Se observa en esta cita que en el primer caso la Parte Especial encierra el precepto principal, al que vienen a completar los de la Parte General, siendo por lo tanto preceptos complementarios.

Si bien el precepto de la Parte Especial es también incompleto, se distingue de los de la Parte General en que es principal respecto a éstos; el precepto del primer libro, no puede considerarse precepto principal, porque no se realiza en ninguna de esas figuras, que precisamente presuponen su no concurrencia, tampoco parece satisfactorio considerar a las fórmulas generales de los artículos especiales del Código Penal como preceptos principales, pues su misma generalidad impide la mínima concreción del supuesto de hecho exigible a un precepto definidor de una específica figura de delito.

Como se puede deducir, la mayor parte de proposiciones jurídico-penales no expresan normas penales completas en cuanto a su contenido, pero normalmente cada uno de

---

<sup>14</sup> Mir Puig. **Ob. Cit**; pág. 58.

los preceptos legales alberga una parte del supuesto de hecho y de la consecuencia jurídica, a completar por otros preceptos. Es excepcional que una disposición legal deje totalmente sin expresar el supuesto de hecho o la consecuencia jurídica. Ello es posible sin que la disposición deje de ostentar la estructura necesaria en toda proposición jurídica, a través de la remisión a otras disposiciones a las que se encarga rellenar el vacío existente en el primer precepto, como es el caso de las denominadas leyes penales en blanco.

“La extensión precisa del concepto de ley penal en blanco varía según los autores. En su origen dicha noción sirvió en Alemania para explicar los casos en que la ley del Imperio (Código Penal del Reich) dejaba la determinación del supuesto de hecho en manos de los Estados o de los municipios. La ley penal en blanco se concibe, por ello, en un principio, como autorización o delegación por parte de un órgano legislativo superior respecto de órganos de inferior jerarquía: la norma resultante es sólo válida, desde el punto de vista de la jerarquía de las fuentes, por virtud de la autorización concedida por la ley penal en blanco”.<sup>15</sup>

Como ejemplos de la ley penal en blanco en el Código Penal, que remite a otras leyes, cabe mencionar los siguientes:

- 1) Leyes penales en blanco en sentido estricto, en donde el complemento se halla en una fuente distinta y de inferior rango: el Artículo 427 dice: conforme... al reglamento respectivo.

---

<sup>15</sup> **Ibid.**

- 2) Leyes penales en blanco cuyo complemento se encuentra en una ley de mismo rango jerárquico pero distinta: el Artículo 274, literal c, remiten a la Ley de Derechos de Autor y Derechos Conexos.
  
- 3) Leyes penales en blanco cuyo complemento está contenido en la misma ley pero en otro Artículo: el Artículo 140 regula que el médico que, abusando de su profesión... será sancionado con las penas señaladas en el Artículo 135.

Se comprende que esta problemática alcanza por igual a todos los casos en que el complemento de la ley en blanco se halla en una norma no penal, aunque sea del mismo rango.

Tal vez por estas razones, de igualdad de tratamiento de los supuestos posibles de complemento situado fuera de la ley en que se halla el precepto penal en blanco, se incluye en este concepto toda norma que sólo fija expresamente la consecuencia jurídica y deja la determinación del contenido del supuesto de hecho a cargo de otras leyes, reglamentos o actos de la administración pública, a lo que se añade que si la remisión tiene lugar a instancia inferior se renuncia a la exclusividad en la precisa fijación de la pena que, como garantía constitucional, corresponde indeclinablemente a la ley.

#### **1.4. Los fundamentos y fines de la pena**

Al estudiarse las funciones de la pena o del sistema penal, se encuentran enfrentadas dos explicaciones sobre la pena; una designada como teoría absoluta de la pena, cuyos defensores sostienen que la pena no tiene un fin específico, sino que es impuesta como retribución o expiación del mal causado; la otra es la denominada teoría relativa de la pena, en donde sus propugnadores afirman que el fin de la pena es evitar la comisión de futuros delitos, mediante la intimidación de terceros prevención especial.

La oposición de estos dos grandes grupos ha tratado de ser superada por los propugnadores de la denominada teoría unitaria, quienes afirman que la pena es retribución y que sus fines deben ser alcanzados dentro de los límites que ésta establece. Se puede sostener que esta posición es la dominante, hoy en día, entre los penalistas.

“Desde este punto de vista, se indica que lo afirmado por Kant, Hegel o Binding, en torno a la pena, es una respuesta a la pregunta sobre la justificación de la pena y sobre su finalidad. Ellos se ocupaban del problema filosófico-moral de si el Estado tiene el derecho de imponer el sufrimiento de la pena, y respondían que su fundamento se encontraba en que el individuo había cometido culpablemente una infracción y no por consideraciones de utilidad social. Es en este sentido que la concepción de estos autores sigue siendo válida para sistemas jurídico-penales como el nuestro”.

Esta postura considera la retribución, esto es a la culpabilidad, como presupuesto esencial para la imposición de la pena, por cuanto que la privación o restricción de derechos impuesta a una persona no considerada culpable, no puede ser calificada como pena, aunque aquella consista en dicha privación o restricción; por lo anterior, el principio no hay pena sin culpabilidad puede constituir una garantía propia del derecho penal democrático.

“Las denominadas teorías relativas de la pena, afirman, como respuesta a la pregunta sobre los fines de la pena, que el fin primario del derecho penal será alcanzado a través de la prevención general o de la prevención especial. Tampoco es de considerar como incompatibles a ambos recursos; bien por el contrario debe reconocerse que es necesario dosificarlos de acuerdo a una política criminal eficaz. Lo que es incorrecto y peligroso para la seguridad jurídica es pensar que el fundamento de la pena es uno de los dos criterios indicados. No se impone una pena porque es necesario intimidar a delincuentes en potencia o porque se estime que es necesario someter a tratamiento al agente. Se le castiga porque culpablemente ha cometido una infracción”.<sup>16</sup>

Una pena que no guarde estas proporciones no será comprendida por la población y será nulo su efecto de prevención general. Esta depende, en general, de la capacidad del sistema para plasmar y reforzar en los individuos la desaprobación moral de las infracciones; es pues, ingenuo pensar cuanto más severas sean las penas, mayor será su efecto de prevención general. Esta se halla más bien en directa relación con la

---

<sup>16</sup> **Ibid.**

oportunidad y la eficacia de la persecución penal, por lo que no es importante la dureza de la pena si no hacerla cumplir.

Las críticas formuladas a la teoría relativa de la prevención general son comprensibles en la medida en que se pretende con ella resolver los problemas referentes a determinar qué acciones deben ser declaradas infracciones, al fundamento de la pena y a sus fines. Pero, desde el momento en que se replantea el problema, tales observaciones carecen de sentido, guardando cierta relevancia la referida a su real eficacia.

“Según la teoría de la prevención especial, la pena se ejerce, en principio, con el fin de beneficiar al delincuente, quien mediante un idóneo tratamiento durante la ejecución de la pena debe ser reconducido al buen camino; reintegrado al medio social al margen del cual se colocó cometiendo la infracción. Es decir, se trata de influir en la personalidad del individuo de manera tal que no vuelva a cometer otro delito, una vez que se reintegre a la vida comunitaria normal”.<sup>17</sup>

Por lo anterior es que, en la legislación y en la doctrina moderna, se acentúa este aspecto de la pena. Los últimos procesos de reforma tienden, precisamente, a hacer de la pena un instrumento de resocialización, sin abandonar su aspecto retributivo y preventivo general.

---

<sup>17</sup> **Ibid.**

La preeminencia que alcanzó la tesis de la prevención especial y la ineficacia de la pena retributiva, en la manera como había sido concebida en los viejos códigos, hicieron que irrumpieran en la legislación y en la doctrina una serie de recursos tendientes a facilitar el tratamiento de delincuentes de acuerdo a su personalidad. Estos recursos son designados con la denominación de medidas de seguridad, y que complementando o suplantado a la pena deben cumplir con la prevención especial, es decir, disminuir o hacer desaparecer las causas que hacen del agente un ser peligroso. Los diversos movimientos propugnadores de un derecho penal de prevención especial, exigen el abandono de la pena y su substitución por medidas de seguridad

Así entonces, esta posición logra encontrar un fundamento adecuado a la responsabilidad mediante la libertad de comportamiento y de responsabilidad, en virtud del cual el hombre cuenta con una libertad para configurar su propio mundo pero a su vez se hace responsable precisamente por ello, de los delitos y las penas que cometa en la órbita del derecho penal.

La conexión entre lo penal y lo social se da porque siempre una modificación en el medio social implica una reacción del sistema penal, generándose con ello, la interpenetración entre sistemas que recíprocamente se perciben como complejidad irreductible pero se toman como dato para su estructuración interna manteniendo su propia complejidad, porque un cambio en las normas morales resulta como consecuencia una modificación del derecho penal y la visión que la sociedad tenga sobre las penas y las medidas de seguridad.

## CAPÍTULO II

### 2. El delito y sus elementos

El concepto del delito es igual a la materialidad resultante del hecho lesivo, sin embargo poco a poco adquiere carácter objetivo y paso a ser la característica de un hecho delictivo y se van configurando los elementos de cada delito. Se va abstrayendo lo que era realidad concreta de ahí se da el paso al tipo penal, tipo como electo genérico de todos los delitos.

Es posible que existan acciones típicas que no son antijurídicas, porque el ordenamiento jurídico establece normas prohibitivas y a veces existen normas permisivas que en casos excepcionales o de conflictos permiten realizar conductas típicas y eso la justifica el carácter de lícita, por ejemplo: legítima defensa.

Normalmente las conductas típicas son antijurídicas, salvo que existan normas permisivas que justifiquen la conducta típica. Todo esto es la valoración del hecho, que al ser una acción típica y antijurídica se le denomina injusto.

Otro elemento del delito es el de la culpabilidad, con la cual se tienen todos los elementos fundamentales del delito, para definir al mismo como toda acción típica, antijurídica y culpable, por lo que deben concurrir todos estos elementos para que haya delito y de aquí emana la responsabilidad penal.

## 2.1. Definición de delito

El concepto substancial o material del delito, establece elementos del delito como presupuestos para que un hecho humano sea considerado como delito, de este concepto se obtienen los elementos constitutivos del delito.

“El concepto nominal o formal define al delito como una conducta humana que se opone a lo que la ley manda o prohíbe bajo la amenaza de una pena. Es la ley la que establece que hechos son delitos, fija caracteres delictuales a un hecho, si en algún momento esta ley es abrogada el delito desaparece. El delito es artificial”.<sup>18</sup>

Entre los elementos primarios constitutivos del delito se encuentra el presupuesto legal o tipo penal, el cual es el contenido eminentemente descriptivo de la norma penal, es la previsión legal que individualiza la conducta humana penalmente relevante.

La definición de delito tiene distintas interpretaciones de acuerdo al enfoque con que se aborde; por ejemplo, el concepto filosófico define al delito como una violación de un derecho fundado sobre la ley moral.

“Para esta concepción el delito consiste en la violación de un deber. La pretensión de validez es socavada porque lo que ayer fue delito deja de serlo con el paso del

---

<sup>18</sup> López Betancourt, Eduardo, **Teoría del delito**, pág. 1.

tiempo y con la abrogación de la ley que lo concibió como delito. Esto ocurrió con el adulterio que era un delito que contravenía el deber de fidelidad, hoy ya no es delito”.<sup>19</sup>

Por aparte, un concepto sociológico considera que el delito es la lesión de los sentimientos altruistas fundamentales de piedad y probidad en la medida en que son poseídos por la comunidad y según sean indispensables para la adaptación del individuo a la sociedad. Aunque esos sentimientos son inherentes al ser humano, no son los únicos.

Por otro lado, el concepto jurídico del delito, considera que el mismo es la infracción de la ley del Estado promulgada para proteger la seguridad ciudadana, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso.

“Para Carrara el delito es un ente jurídico (creación de la ley) y no un fenómeno social (ente de hecho). Es un ente jurídico porque es una contradicción entre el hecho del hombre y la ley. Por eso no se define como acción sino como infracción, lo que supone la antijuridicidad la esencia del delito y no solo su elemento. Al decir acto externo, se refiere a que no son sancionables los actos internos o pensamientos, sólo los actos exteriorizados del hombre. El pensar en matar no es delito, mientras no lo exteriorice”.<sup>20</sup>

---

<sup>19</sup> **Ibid.**

<sup>20</sup> **Ibid.**

Por aparte, un concepto dogmático describe al delito como la acción u omisión voluntaria típicamente antijurídica y culpable, con lo cual numera los elementos constitutivos del delito.

Para esta concepción, el delito es un acto u omisión voluntaria, quedan descartadas las conductas que no son conducidas por la voluntad, como las conductas por fuerza irresistible, acto reflejo o situaciones ajenas a lo patológico.

“El concepto dogmático del delito tiene origen en la Teoría De Las Normas de Karl Binding que dice que el delincuente viola la norma no la ley. La norma es un deber ser: ‘no matarás’. El deber ser guía a lo que es bueno y que es lo malo. La ley es un ser, o sea la ley positiva. Es mas, el delito es una conducta positiva. Con ello se entiende que el delito es un acto típico, todo acto humano para considerarse como delito debe adecuarse al tipo penal. Es decir debe haber tipicidad. Si no hay adecuación no hay delito, o peor aun, si no hay tipo, la conducta no es delito. Por eso, todo lo que no esta prohibido u ordenado, está permitido”.<sup>21</sup>

Mientras desde el causalismo, el delito se basa en la conducta como un elemento primordial del delito, entendida como la acción u omisión que provoca el daño o la puesta en peligro del bien jurídico, siendo la acción que interesa al derecho penal aquella que genera la violación a la norma y la lesión del bien tutelado. Plantea que el delito se integra por tres elementos: la conducta, el nexo causal y el resultado.

---

<sup>21</sup> **Ibid.**

“La teoría causalista ha sido criticada debido a que limita la conducta a la acción que produce meramente un resultado, sin contemplar otros factores que pueden estar involucrados, como la intención y la prevención”.<sup>22</sup>

Para los finalistas, la esencia de la conducta delictiva se presenta en la medida en que se convierte en el ejercicio final, porque la finalidad obedece a la capacidad del hombre de prever, dentro de límites razonables, las consecuencias de su comportamiento; por lo que la intención se convierte en un elemento indispensable. El sujeto activo, al ejecutar la conducta, tuvo la oportunidad de planearla y estar consciente del resultado que obtendrá.

“Esta teoría ha sido criticada respecto a los delitos culposos, ya que pueden presentarse resultados típicos no dolosos”.<sup>23</sup>

Por último desde una visión normativa, el delito el dolo y la culpa constituyen un elemento de reprochabilidad social ante la conducta cometida, entendiendo por reprochabilidad la reacción ante el delito cometido.

## **2.2. La teoría del delito**

La teoría del delito se fundamenta en aspectos teóricos que le permiten desarrollarse plenamente en el campo práctico, al determinar con precisión si existen o no elementos

---

<sup>22</sup> Calderón Ramos, Eduardo, **Estado de necesidad como excluyente de responsabilidad**, pág. 76.

<sup>23</sup> **Ibid.**

constitutivos del tipo penal en los comportamientos humanos gestados en la sociedad. Por ello, la teoría del delito es la parte medular del derecho penal. Adentrarse en ella, constituye el mecanismo mas adecuado para familiarizarse con el ilícito, renglón fundamental del universo jurídico.

Se puede decir que la teoría del delito es una concepción científica que trata de sistematizar presupuestos generales de la responsabilidad que radica en el delito y la sanción. Estudia las características generales que configuran al delito.

Al respecto, Zaffaroni señala que: "La teoría del delito atiende al cumplimiento de un cometido esencialmente práctico, consistente en la facilitación de la averiguación de la presencia o ausencia del delito en cada caso concreto".<sup>24</sup>

Esta es una teoría de interpretación jurídica sobre los presupuestos generales de la responsabilidad de una persona. Son los elementos de análisis sobre la responsabilidad penal y por tanto los elementos generales del delito, de esto se desprende que la misma sea una concepción científica que trata de sistematizar presupuestos generales de la responsabilidad que radica en el delito y la sanción, para lo cual estudia las características generales de todos los delitos.

Uno de los temas que ha sido objeto de las más enconadas controversias dentro de la teoría del delito, es sin duda alguna el de la culpabilidad, por lo que el mismo ha sufrido no pocas modificaciones en su concepción, pasando desde una tesis

---

<sup>24</sup> Zaffaroni, Eugenio Raúl, **Manual de derecho penal. Parte general**, pág. 333.

psicológica que entiende a la culpabilidad como relación psíquica, sin contemplar el aspecto valorativo, hasta llegar a una tesis eminentemente normativa, en donde la culpabilidad, entendida como juicio de reproche, supone la posibilidad de comprensión de la antijuridicidad de la conducta.

Desde luego, cabe advertir que ciertos sectores de la doctrina han desarrollado otras definiciones de culpabilidad que no necesariamente siguen las pautas establecidas para su tradicional análisis, y en determinados casos, incluso pretendiendo formularlo desde una óptica diferente, o al menos desde una perspectiva orientada hacia criterios que no suelen ser tan conocidos; aunque dichas posturas no han alcanzado apoyo mayoritario, resulta de interés mencionar algunas de ellas ya que mantienen importantes críticas del concepto comúnmente aceptado.

Una primera teoría que está fuera de la definición clásica de la culpabilidad, es la del fin de la pena, la cual sostiene que aquella puede apoyarse como un puro criterio político, a partir de la finalidad de la pena, lo que significa que si no hay posibilidad de evitar el injusto, carece de sentido sancionarlo.

“Para Zaffaroni el principal obstáculo a esta tesis radica en que invierte el planteamiento general de la cuestión, según el cual debe conocerse si hay delito para saber si se debe aplicar una pena y no a la inversa”.<sup>25</sup>

---

<sup>25</sup> **Ibid.**

Otra teoría es la de la llamada de la atribuibilidad, según la cual debe distinguirse entre lo que es exigencia conforme a un término medio, que fundaría una responsabilidad por el hecho y la exigencia conforme a pautas individualizadas, que darían lugar a la culpabilidad como juicio de reproche individualizado, en donde culpabilidad y responsabilidad serían así, dos estadios de una más general atribuibilidad del injusto.

Por otra parte, se encuentran las teorías que ubican el dolo y la culpa en la culpabilidad, por lo que se les denomina causalitas, las que no siempre exigieron que el dolo culpable tuviera una efectiva consciencia de la antijuridicidad, sino que al lado y fuera del dolo ubicaron el requisito de la posibilidad de comprensión de la antijuridicidad, entendido como conocimiento potencial o posibilidad de conocimiento.

“Esta tesitura era más coherente y se mantiene cuando el dolo se elimina de la culpabilidad para trasladarlo al tipo, constituyendo la llamada teoría estricta de la culpabilidad (que aparece actualmente como la de mayor aceptación)”.<sup>26</sup>

Frente a esta teoría y como respuesta a la misma, surge la denominada teoría limitada o restringida de la culpabilidad, como complementación de quienes siguen la teoría de los elementos negativos del tipo, según la cual las causas de justificación son causas de atipicidad, siendo que la tipicidad comprende como elementos negativos, las ausencias de causas de justificación.

---

<sup>26</sup> Octavio de Toledo, Ernesto y Susana Huerta Tocildo, **Teoría del delito**, pág. 56.

“Así pues, de acuerdo con dicha posición, la consciencia de la antijuridicidad pertenece a la culpabilidad, pero cuando depende del conocimiento de la falta de situación de justificación se ubica en la tipicidad (dolo), mientras que en la primera (teoría estricta) la posibilidad de comprensión del injusto (conocimiento potencial) se halla en la culpabilidad, permaneciendo ajeno al dolo, sea que éste se encuentre en el tipo (estructura finalista) o en la culpabilidad (estructura causalista)”.<sup>27</sup>

Por otra parte, se encuentra la postura finalista, la cual plantea que además de la causalidad entre comportamiento y resultado, hay que examinar en el tipo el contenido de la voluntad, si el autor quiso el resultado y sólo entonces, habrá tipo doloso; si no fue ése el caso, habrá a lo sumo un hecho imprudente.

La culpabilidad además de constituir un elemento positivo, para la construcción técnica de la infracción, tiene como característica fundamental ser el elemento subjetivo del delito, refiriéndose pues a la voluntad del agente para la realización del acto delictivo. La culpabilidad radica pues, en la manifestación de voluntad del sujeto activo de la infracción penal que puede tornarse dolosa o bien culposa, dependiendo de la intención deliberada de cometer el delito, o bien de la comisión del delito por negligencia, imprudencia o impericia.

---

<sup>27</sup> **Ibid.**

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

El derecho penal, en cada figura tipifica delito, tutela determinados bienes que considera dignos de ser protegidos, siendo su principal interés tutelar la vida de las personas; así, el legislador crea los delitos de homicidio, aborto y participación en el suicidio, homicidios en razón del parentesco o relación con lo cual pretende proteger la vida humana.

Todo delito tiene un bien jurídicamente protegido. En razón a esto, el Código Penal clasifica los delitos en orden al objeto o bien jurídico tutelado. Cada título del mismo agrupa a los delitos, atendiendo el bien jurídico tutelado, por lo que a partir de lo mismo pueden ser clasificados.

Según la forma de la conducta del agente o la manifestación de la voluntad, los delitos pueden ser de acción y de omisión; los primeros se cometen mediante un comportamiento positivo al violar una ley prohibitiva, son aquellos en los cuales las condiciones de donde deriva su resultado, reconocen como causa determinante un hecho positivo del sujeto; mientras que en los segundos, el objeto prohibido es una abstención del agente, consiste en la no ejecución de algo ordenado por la ley; en estos delitos, las condiciones de que deriva su resultado reconocen, como causa determinante, la falta de observancia de parte del sujeto de un precepto obligatorio. Los delitos de omisión violan una ley dispositiva, en tanto los de acción infringen una prohibitiva.

Los delitos de omisión se dividen en: simple omisión y de comisión por omisión, también llamados delitos de omisión impropia; consistiendo los primeros en la falta de una actividad jurídicamente ordenada, con independencia del resultado material que produzcan; es decir, se sancionan por la omisión misma.

Los delitos de comisión por omisión o impropios, son aquellos en los que el agente decide actuar y por esa inacción se produce el resultado material, consisten en la aparición de un resultado delictivo de carácter positivo por inactividad, formula que se concreta en la producción de un cambio en el mundo exterior mediante la omisión de algo que el derecho ordenaba hacer. Ejemplo de este tipo de delito es: “La madre que, con deliberado propósito de dar muerte a su hijo recién nacido, no lo amamanta, produciéndose el resultado letal. La madre no ejecuta acto alguno, antes bien, deja de realizar lo debido”.<sup>28</sup>

En los delitos de simple omisión, hay una violación jurídica y un resultado puramente formal, mientras en los de comisión por omisión, además de la violación jurídica se produce un resultado material; en los primeros se viola una ley dispositiva, en los de comisión por omisión se infringen una dispositiva y una prohibitiva.

Los delitos, por los resultados, se clasifican en formales o delitos de simple actividad y materiales, que son delitos de resultado material; Los formales son aquellos en los que se agota el tipo penal en movimiento corporal o en la omisión del agente, no siendo

---

<sup>28</sup> **Ibid.**

necesario para su integración que se produzca alguna alteración en la estructura o funcionamiento del objeto material, son delitos de mera conducta; los autores ejemplifican el delito formal con el falso testimonio, la portación de arma prohibida, y la posesión ilícita de enervantes; los delitos materiales son aquellos en los cuales para su integración se requiere la destrucción o alteración de la estructura o del funcionamiento del objeto material, tal el caso del homicidio o el delito de daño en propiedad ajena.

Por su duración los delitos se dividen en instantáneos, instantáneos con efectos permanentes, continuados y permanentes; en el primer caso, la acción que lo consuma se perfecciona en un solo momento, su carácter no se lo dan los efectos que él causa sino la naturaleza de la acción a la que la ley acuerda el carácter de consumatoria, puede realizarse mediante una acción compuesta de varios actos o movimientos; para la calificación se atiende a la unidad de la acción, si con ella se consuma el delito no importando que a su vez, esa acción se descomponga en actividades múltiples; el momento consumativo expresado en la ley da la nota al delito instantáneo, en este caso, existe una acción y una lesión jurídica, el evento consumativo típico se produce en un solo instante, como el homicidio y el robo.

#### **2.4. Fases de la realización del delito**

El delito tiene distintas fases o momentos, los cuales son: el *lter criminis*, la fase interna, la intermedia y la externa, cada una de las cuales tiene un significado primordial para la doctrina y la legislación, puesto que de manera individual

representan un proceso con diferentes características, mientras que conjuntamente expresan una realidad conductual importante para determinar la responsabilidad penal y la pena.

El primer elemento o Iter Criminis, se refiere a la vida del delito desde que nace en la mente de su autor hasta la consumación, está constituido por una serie de etapas desde que se concibe la idea de realizar un ilícito hasta que el criminal logra conseguir lo que se ha propuesto, dichas etapas pueden tener o no repercusiones jurídico penales y se dividen en fase interna y fase externa de aquél.

La fase interna esta conformada por las llamadas voliciones criminales que no son mas que las ideas delictivas nacidas en la mente del sujeto activo, que mientras no se manifiesten o exterioricen de manera objetiva no implica responsabilidad penal, ya que la mera resolución de delinquir no constituye nunca un delito.

La fase intermedia comprende actos que no causan daño objetivo y que se expresan en la determinación de cometer un delito, o sea en la resolución manifestada que se expresa en forma de conspiración, instigación y amenazas. Estas aunque no causen daño pueden causar alteraciones públicas.

“A esta fase también pertenecen el delito putativo y la apología del delito. El delito putativo es un acto en el cual el autor cree, por error, que está cometiendo un hecho punible y delictivo. Uno cree que el adulterio es delito, cae en esta conducta y se

estima autor de un delito. No se sanciona porque se sigue el Principio de Legalidad. La apología del delito es el apoyo público a la comisión de un delito o a una persona condenada”.<sup>29</sup>

La fase externa comienza cuando el sujeto activo exterioriza la conducta tramada durante la fase interna, en este momento principia a poner en peligro o a atacar un bien jurídico protegido a través de una resolución criminal manifiesta, por eso el Código Penal reconoce expresamente dos formas de resolución criminal, una individual y la otra colectiva. En el Artículo 17, regula a la primera a través de la proposición, lo cual sucede cuando el que ha resuelto cometer un delito invita a otra o a otras personas a ejecutarlo; mientras que en ese mismo artículo se regula la colectiva denominada conspiración, en donde dos o más personas se conciertan para cometer un delito.

Es en esta fase en que el delito cobra vida, y está compuesta por los actos preparatorios y los de ejecución; los primeros sirven para proveerse de instrumentos adecuados y medios para cometer un delito.

“Para los clásicos, los actos preparatorios no son punibles porque no siempre reflejan la intención del autor. Porque una persona puede comprar un arma para uso diverso. Las positivistas dicen que son punibles si estos actos son realizados por personas que ya cometieron delitos. El Código Penal boliviano no los sanciona. Por excepción, sin embargo, si sanciona, siempre y cuando el conseguir medios e instrumentos refleje

---

<sup>29</sup> López Díaz, Claudia. **Introducción a la Imputación Objetiva**, pág. 89.

inequívocamente la comisión de un delito, pero los sanciona como delito especial, no como acto preparatorio”.<sup>30</sup>

Los actos de ejecución son actos externos que caen en el tipo penal punible. Pertenecen a estos actos la tentativa, el delito frustrado, el delito imposible y el delito consumado.

La tentativa, es el inicio de ejecución de un delito, pero este se ha interrumpido por causa ajena a la voluntad del agente; los elementos que la integran son:

- a) El principio de ejecución, acto material que tiende directamente a la perpetración de la infracción penal.
- b) La intención de cometer el delito, que debe ser confesada por el autor o probada por el protagonista del evento criminal.

El delito frustrado ocurre cuando el agente realiza todos los actos de ejecución, pero el delito no aparece en sus consecuencias materiales; tal es el caso que sucede cuando al sujeto activo le da a alguien a beber un veneno, pero luego evita los efectos del mismo a partir de darle a la víctima un antídoto.

Mientras que el delito imposible, sucede cuando se realizan acciones, pero que por la falta de medios, de objetivo o inadecuado uso de los medios el delito no llega a

---

<sup>30</sup> **Ibid.**

consumarse, siendo un ejemplo de este ilícito dar azúcar creyendo que era veneno, lo cual es uso inadecuado de la substancia; tratar de hacer abortar a una mujer no embarazada, que implica la falta de objeto material sobre el cual recaer la acción delictiva.

En el delito consumado, el sujeto activo realiza la acción típicamente antijurídica que planeó ejecutar, estos delitos son descritos en la Parte Especial del Código Penal.

## **2.5. Sujetos y objeto del delito**

Todo delito requiere el comportamiento de un hombre, por lo que el sujeto de la acción y, por tanto, sujeto activo del delito, sólo podrá serlo el hombre individual. Nadie discute, en la actualidad, el que no puedan ser sujeto activo de delitos los animales o las cosas inanimadas.

Por aparte se encuentra el sujeto pasivo, quien es la persona, física o jurídica, única o plural, titular del bien jurídico protegido.

Puede serlo toda persona con capacidad para ser titular de derechos o intereses: tanto los imputables como los inimputables, la persona física como la jurídica y el propio Estado.

“Conviene no confundir el sujeto pasivo del delito con el sujeto pasivo de la acción, sujeto de la acción, sobre el que recae directamente la conducta típica (coinciden materialmente sujeto pasivo y sujeto sobre el que recae la acción, por ejemplo, en el delito de lesiones; no coinciden, en cambio, en una estafa en triángulo: el sujeto sobre el que recae la acción es la persona engañada, la que sufre el error, y el sujeto pasivo del delito es el titular del patrimonio). Del sujeto pasivo también debe diferenciarse la figura del perjudicado, que es la persona física o jurídica que sufre un daño, patrimonial o de otra clase, a causa de la comisión de un delito”.<sup>31</sup>

El objeto material del delito es una persona, quien es el sujeto sobre el que recae la acción o bien una cosa sobre la que incide directamente la acción descrita en el tipo. Este concepto no debe confundirse con el concepto de objeto jurídico, porque el primero es sobre quien recae la acción, mientras que el segundo es un factor valioso para la vida en sociedad que se estima merecedor de protección penal, es el bien tutelado, elemento esencial en torno al cual gira el tipo del injusto

---

<sup>31</sup> Córdoba Angulo, Miguel, **El principio de culpabilidad**, pág. 103.



## **CAPÍTULO III**

### **3. Delitos informáticos**

A nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, así como la importancia que tiene su progreso para el desarrollo de un país.

Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc., son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

Sin embargo, junto al avance de la tecnología informática y su influencia, en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos.

#### **3.1. Definición del delito informático**

Se puede definir el delito informático como toda acción u omisión culpable realizada por un ser humano en el entorno informático y está sancionado con una pena.

“Los delitos informáticos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y

culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".<sup>32</sup>

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho.

A nivel internacional se considera que no existe una definición propia del delito informático; sin embargo, muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo 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 nuestro país, al igual que en otros muchos, no ha sido objeto de tipificación aún”.<sup>33</sup>

---

<sup>32</sup> Estrada Garavilla, Miguel, **Delitos informáticos**, pág. 4.

<sup>33</sup> **Ibid.**

El delito informático también se define como: "Aquel que se da con la ayuda de la informática o de técnicas anexas como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el Título 1 de la Constitución Española".<sup>34</sup>

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

Este tipo de delito se puede encontrar en forma típica y atípica, entendiendo por la primera a las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y por las segundas las actitudes ilícitas en que se tienen a las computadoras como instrumento o fin.

Este tipo de acciones tienen como características principales que son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos técnicos pueden llegar a cometerlas; son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando; también son de oportunidad, ya que se aprovecha una ocasión creada o

---

<sup>34</sup> **Ibid.**

altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

Los delitos de esta naturaleza provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que las realizan; asimismo, ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

“Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos informáticos, delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora, delincuencia relacionada con el ordenador. En síntesis, 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. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente 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 y los funcionarios judiciales”.<sup>35</sup>

---

<sup>35</sup> Mir Puig, Santiago. **Delincuencia informática**, pág. 22.

En este orden de ideas, en el presente trabajo se entenderán como delitos informáticos todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, en los que se haga uso indebido de cualquier medio informático.

Existe un consenso general entre los diversos estudiosos de la materia, en considerar que el nacimiento de la criminalidad informática se encuentra íntimamente asociada al desarrollo tecnológico informático.

Las computadoras han sido utilizadas para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato, lo cual ha obligado al surgimiento de medidas legislativo penales en los estados industriales donde hay conciencia de que en los últimos años, ha estado presente el fenómeno delictivo informático.

Un primer problema está en delimitar el campo de acción de la llamada criminalidad informática; en primer lugar existe una confusión terminológica y conceptual presente, en todos los campos de la informática, especialmente en relación con sus aspectos criminales, es por eso que, es menester desenmarañar el intrincado debate doctrinario acerca del real contenido de lo que se ha dado en llamar los delitos informáticos.

Desde esta perspectiva, debe reinar la claridad más absoluta respecto de las materias, acciones y omisiones sobre las que debe recaer la seguridad social que aporta el aparato punitivo del estado. La mayúscula trascendencia inherente a los delitos informáticos merece que toda persona que opere en el mundo del derecho se detenga

a meditar sobre el lugar conceptual del espacio de lo jurídico-criminal en que tales agresiones se suceden.

En ese orden de ideas, se señala que: “En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información”.<sup>36</sup>

Es por eso que resulta extremadamente complejo buscar un concepto técnico que comprenda todas las conductas ilícitas vinculadas a los medios o procedimientos informáticos, tanto por la diversidad de supuestos, como de los bienes jurídicos afectados.

---

<sup>36</sup> Acurio Del Pino, Santiago, **Delitos informáticos**, pág. 9.

Ahora bien, dicho lo anterior, es necesario establecer que además dentro de este fenómeno existe una pluralidad de acepciones y conceptos sobre delincuencia informática, criminalidad informática, lo que ha constituido en un tema de debate también dentro de la doctrina.

### **3.2. Características de los sujetos del delito informático**

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas.

De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo.

Los sujetos activos o personas que cometen los delitos informáticos, son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en

el uso de los sistemas informatizados, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de habilidades no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos; sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como delitos de cuello blanco.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes; además, si bien los acuerdos de cooperación

internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

Para el caso de las características del sujeto pasivo, se debe establecer que este, víctima del delito, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos los objetos del delito pueden ser individuos, instituciones crediticias, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito informático, es sumamente importante ya que mediante él se pueden conocer los diferentes ilícitos que cometen los delincuentes informáticos con objeto de prever las acciones antes mencionadas, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

“Ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae

como consecuencia que las estadísticas sobre este tipo de conductas se mantengan bajo la llamada cifra oculta o cifra negra”.<sup>37</sup>

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro.

Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento; en el mismo sentido, se puede decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración e impartición de justicia para atender e investigar estas conductas ilícitas, se avanza mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

### **3.3. Bien jurídico protegido**

Dentro de los delitos informáticos, se puede decir que la tendencia es que la protección a los bienes jurídicos, se haga desde la perspectiva de los delitos tradicionales, con

---

<sup>37</sup> **Ibid.**

una reinterpretación de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos.

Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos reinterpretados o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

“De otro lado otra vertiente doctrinaria supone que la emergente sociedad de la información hace totalmente necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible. Esto por cuanto la información no puede ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tienen un valor intrínseco compartido, que es su valoración económica, es por tanto que ella la información y otros intangibles son objetos de propiedad, la cual esta constitucionalmente protegida”.<sup>38</sup>

El bien jurídico protegido en los delitos informáticos en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

---

<sup>38</sup> **Ibid**; pág. 20.

“El patrimonio, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da lugar.

La reserva, la intimidad y confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.

La seguridad o fiabilidad del tráfico jurídico, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.

El derecho de propiedad, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático”.<sup>39</sup>

El bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde está se almacena o transfiere; por lo que se puede decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos.

---

<sup>39</sup> **Ibidem**; pág. 21.

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

Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen las leyes penales nacionales.

En un primer término, debe considerarse que en 1983, la Organización para la Cooperación y el Desarrollo que involucra a los gobiernos de los países europeos y Estados Unidos de América, inició un estudio de la posibilidad 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.

Esta decisión se llevó a cabo debido a las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución.

Sobre la base de las posturas y de las deliberaciones en la Organización para la Cooperación y el Desarrollo, surgió un análisis y una valoración jurídica de los derechos nacionales aplicables así como de las propuestas de reforma, las

conclusiones desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

“De esta forma, se reseñaron las normas legislativas vigentes y las propuestas de reforma en diversos Estados y se recomendó una lista mínima que clasificaba los delitos, surgiendo, entre otros, el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido, espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales, y el acceso o empleo no autorizado de sistemas de computadoras”.<sup>40</sup>

Las directrices que contenían la clasificación de los delitos informáticos, elaborada para que sirviera a los legisladores nacionales para incluirlos en el derecho penal de cada país, incluyen una lista mínima acerca de determinados casos de uso indebido de computadoras, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Existen muchos tipos de delitos informáticos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es inimaginable, el único límite existente viene

---

<sup>40</sup> Estrada, **Ob. Cit**; pág.11.

dado por la conjugación de la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas.

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios: “Como instrumento o medio y como fin u objetivo. Como instrumento o medio: en esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo: a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.); b) Variación de los activos y pasivos en la situación contable de las empresas; c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.); d) Lectura, sustracción o copiado de información confidencial; e) Modificación de datos tanto en la entrada como en la salida; f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas; g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa; h) Uso no autorizado de programas de computo; i) Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas; j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos; k) Obtención de información residual impresa en papel luego de la ejecución de trabajos; l) Acceso a áreas informatizadas en forma no autorizada y m) Intervención en las líneas de comunicación de datos o teleproceso”.<sup>41</sup>

En la categoría de fin u objetivo, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como

---

<sup>41</sup> **Derecho Informático**, pág. 103.

por ejemplo: a) Programación de instrucciones que producen un bloqueo total al sistema; b) Destrucción de programas por cualquier método; c) Daño a los dispositivos de almacenamiento; d) Atentado físico contra la máquina o sus accesorios; e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados y f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)”.<sup>42</sup>

María De La Luz Lima, presenta una clasificación, de lo que ella llama delitos electrónicos, diciendo que existen tres categorías, a saber: “a) Los que utilizan la tecnología electrónica como método: conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito; b) Los que utilizan la tecnología electrónica como medio: conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo y c) Los que utilizan la tecnología electrónica como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla”.<sup>43</sup>

En lo que se refiere a delitos informáticos, se pueden encontrar tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:” a) Acceso no autorizado: es el primer paso de cualquier delito, lo cual se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente

---

<sup>42</sup> **Ibid.**

<sup>43</sup> **Delitos electrónicos**, pág. 100.

mantenerse conectado; b) Actos dañinos o circulación de material dañino, una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos; tal comportamiento casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet); c) Interceptación no autorizada: en este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él".<sup>44</sup>

Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado este tipo de comportamiento ilícito cometidos a través de las computadoras.

La justificación y los detalles característicos de la criminalidad informática, se encuentran precisamente en su carácter de informática, es decir la especificidad, cuyas notas características las aporta el computador junto con sus funciones propias más importantes, el procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para tales fines.

Cualquier conducta que no opere sobre la base de estas funciones, aunque pueda resultar delictiva o merecedora de sanción penal en su caso, no poseerá ya la

---

<sup>44</sup> Hance, Olivier, **Leyes y negocios en Internet**, pág. 89.

especificidad y debe ser, por tanto, apartada del estudio de la delincuencia vinculada a la informática o tecnologías de la información.

En este sentido, es irrelevante que el computador sea instrumento u objetivo de la conducta, y que ésta esté criminalizada o merezca serlo por consideraciones de política criminal.

### **3.5. Impacto de los delitos informáticos**

A medida que se va ampliando la Internet, asimismo va aumentando el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o piratería informática, el fraude, el sabotaje informático, la trata de niños con fines pornográficos y el acecho.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables enlaces o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en paraísos informáticos, o sea, en países que carecen de leyes o experiencia para seguirles la pista.

“Según datos recientes del servicio secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito”.<sup>45</sup>

Otros delincuentes de la informática pueden sabotear las computadoras para ganar ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión. Los malhechores manipulan los datos o las operaciones, ya sea directamente o mediante los llamados gusanos o virus, que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro.

Algunos virus dirigidos contra computadoras elegidas al azar; que originalmente pasaron de una computadora a otra por medio de disquetes infectados; también se están propagando últimamente por las redes, con frecuencia camuflados en mensajes electrónicos o en programas descargados de la red.

“En 1990, se supo por primera vez en Europa de un caso en que se usó a un virus para sonsacar dinero, cuando la comunidad de investigación médica se vio amenazada con

---

<sup>45</sup> Amoroso Fernández, Yarina, **La informática como objeto de derecho**, pág. 43.

un virus que iría destruyendo datos paulatinamente si no se pagaba un rescate por la cura".<sup>46</sup>

Además de las incursiones por las páginas particulares de la red, los delincuentes pueden abrir sus propios sitios para estafar a los clientes o vender mercancías y servicios prohibidos, como armas, drogas, medicamentos sin receta ni regulación y pornografía.

La proliferación de los delitos informáticos ha hecho que las personas sean cada vez más escépticas a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general.

También se observa el grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global.

Asimismo se advierte que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal para trabajar en éstas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral.

---

<sup>46</sup> **Ibid.**

La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

### **3.6. Seguridad contra los delitos informáticos**

Aunque los consumidores tienden a agrupar sus intereses juntos por debajo del término de la seguridad general, hay realmente varias partes de la seguridad que confunden. La seguridad significa guardar algo seguro.

“Para guardar objetos seguros, es necesario lo siguiente:

La autenticación (promesa de identidad), es decir la prevención de suplantaciones, que se garantice que quien firma un mensaje es realmente quien dice ser.

La autorización (se da permiso a una persona o grupo de personas de poder realizar ciertas funciones, al resto se le niega el permiso y se les sanciona si las realizan).

La privacidad o confidencialidad, es el más obvio de los aspectos y se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos.

La integridad de datos, La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.

La disponibilidad de la información, se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Controles de acceso, esto es quien tiene autorización y quien no para acceder a una pieza de información determinada".<sup>47</sup>

La importancia de lo que se está asegurando y el riesgo potencial involucra en dejar uno de estos requerimientos o tener que forzar niveles más altos de seguridad; por lo que la comprensión de los elementos de seguridad y como ellos trabajan en el mundo físico, puede ayudar para explicar cómo estos requerimientos se encuentran en el mundo de la red y dónde se sitúan las dificultades.

Existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que se debe hacer es diseñar una política de seguridad. En ella, definir quiénes tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas, y preocuparse de hacerlas cambiar periódicamente.

---

<sup>47</sup> **Ibid.**

Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Una de las maneras drásticas de no tener invasores es la de poner murallas, siendo los mecanismos más usados para la protección de la red interna de otras externas son los filtros o cortafuegos.

La lista de filtros se aplican secuencialmente, de forma que la primera regla que el paquete cumpla será marcar la acción a realizar para descartarla o dejarla pasar, debido a que la aplicación de las listas de filtros se puede hacer en el momento de entrada del paquete o bien en el de salida o en ambos.

De igual manera, el cifrado con clave pública permite generar firmas digitales que hacen posible certificar la procedencia de un mensaje, en otras palabras, asegurar que proviene de quien dice, de esta forma se puede evitar que alguien suplante a un usuario y envíe mensajes falsos a otro usuario, por la imposibilidad de falsificar la firma.

La firma digital garantiza la integridad del mensaje, es decir, que no ha sido alterado durante la transmisión, se puede aplicar a un mensaje completo o puede ser algo añadido al mensaje; las firmas son especialmente útiles cuando la información debe atravesar redes sobre las que no se tiene control directo y, en consecuencia, no existe posibilidad de verificar de otra forma la procedencia de los mensajes.

Existen varios métodos para hacer uso de la firma digital, uno de ellos es el siguiente: quien envía el mensaje lo codifica con su clave privada. Para descifrarlo, sólo puede

hacerse con la clave pública correspondiente a dicha persona o institución. Si efectivamente con dicha clave se descifra es señal de que quien dice que envió el mensaje, realmente lo hizo.

### **3.7. Problemas de persecución**

Los delitos informáticos son difícilmente descubiertos o perseguidos, ya que los sujetos activos actúan sigilosamente y poseen herramientas capaces de borrar todo rastro de intrusión o la consumación del delito; pero a pesar de eso existen dos problemas principales que dificultan su persecución: 1) Lo relacionado con la concepción tradicional de tiempo y espacio y 2) El anonimato del sujeto activo.

Con relación a la concepción tradicional del tiempo y del espacio, el escenario en donde se producen los delitos informáticos es el ciberespacio, un lugar donde no existen fronteras territoriales, lo que hace difícil la persecución de estos delitos y su enjuiciamiento, ya que existe la posibilidad de preparar y cometer acciones delictivas informáticas en perjuicio de terceros en tiempo y espacio lejanos.

Debido a los adelantos de las telecomunicaciones y la telemática, hace que las distancias reales o fronteras entre países no existan como ya se ha dicho, ya que una persona puede realizar un acto delictivo en un lugar distinto del lugar de los hechos.

Por otro lado, la posibilidad de realizar programas de efecto retardado como las llamadas bombas lógicas, las cuales no desatan su poder destructivo, hasta tiempo después de que el autor material de la infracción este a buen recaudo; o que con determinadas ordenes, rutinas y subrutinas de algunos programas se puede preparar la comisión de una infracción como la del fraude informático y en el momento que esto sucede el hechor se encuentra realizando una tarea completamente incompatible con el acto delictivo cometido.

El sujeto activo de esta clase de infracciones puede ser totalmente anónimo y usar este anonimato como forma de evadir su responsabilidad, ya que este no necesariamente puede usar su propio sistema informático, sino que se puede valer de un tercero, como por ejemplo en el caso del envión de correo no deseado o spam, en el cual se puede usar a una computadora que está bajo el control del spammer y que le permite usarla como una estación de trabajo de su propia red de computadoras, las cuales pertenecen a usuarios desaprensivos que no tienen al día sus medidas de seguridad y que son fácil presa de los hackers y crackers para cometer este tipo de infracciones.



## CAPÍTULO IV

### **4. La importancia de tipificar el phishing como delito en el Código Penal.**

A partir de establecer los elementos doctrinarios que explican al delito en general y las características que ha de tener cualquier delito informático, es importante abordar los aspectos centrales del delito de phishing, para determinar en cual de los bienes jurídicos tutelados debe incorporarse dentro de la Parte General del Código Penal o si se debe crear un apartado totalmente nuevo.

Debe tenerse en cuenta que un delito es antes que nada una acción o conducta humana, en donde debe darse el acto que, al realizarse, encuadra dentro del tipo o conducta prohibida.

Si bien es cierto, la doctrina ha definido al delito de phishing, sin embargo, en el Código Penal no se ha tipificado el mismo, por lo que no se ha teorizado sobre sus aspectos o elementos centrales, los sujetos ni el bien jurídico tutelado. Por lo que se trata de establecer en un primer momento estos aspectos y discutir con los doctrinarios lo que se dice de los mismos y luego plantear la manera en que debe quedar tipificado en la ley penal.

#### 4.1. El delito de phishing.

La aparición de esta palabra anglosajona, recientemente en el ámbito de la seguridad de la información, en el mundo de habla hispana define la duplicación de un original de una página web, normalmente de bancos, con fines delictivos.

El phishing, consiste en el envío masivo de mensajes electrónicos con falsos remitentes que aconsejan a los usuarios que rellenen y confirmen los datos y contraseñas para poder acceder a sus cuentas bancarias.

“El término phishing puede ser la contracción de password harvesting fishing (cosecha y pesca de contraseñas) y, a pesar de que este término data de mediados de los años 90 en Estados Unidos, es ahora cuando empieza a oírse en castellano. No existe de momento una definición al español pero hay algunos términos que podrían servir como posibles sustitutos: correo electrónico fraudulento, ciberestafa o fraude por Internet. La Fundación del Español Urgente aconseja que se mantenga este término en inglés escrito en cursiva o entre comillas y se aclare su significado (entre paréntesis), siempre que sea posible, con alguno de los términos ya citados”<sup>48</sup>.

---

<sup>48</sup> Oficina nacional de tecnologías de información (onti). (2006). Recomendaciones para evitar ser víctima del “*phishing*”. Coordinación de emergencias en redes teleinformáticas de Argentina. Versión 1.0. Agosto, 2006. [http://www.arcert.gov.ar/webs/tips/recomendaciones\\_phishing.pdf](http://www.arcert.gov.ar/webs/tips/recomendaciones_phishing.pdf). Consultada el 10 de marzo de 2010.

Como consecuencia de los altos niveles de fraude mediante phishing en los Estados Unidos de América, se considera esta modalidad criminal como robo de identidad automatizada.

Este delito informático combina el poder de la red Internet con la candidez y/o codicia de la naturaleza humana para defraudar a millones de personas y por lo tanto millones de dólares.

Casi cualquier persona en el mundo con una dirección electrónica habrá recibido a la fecha algún tipo de correo electrónico con propósitos fraudulentos. Estos mensajes de correo utilizan el formato y apariencia típica de una institución legítima que la hacen parecer confiable para que los usuarios proporcionen su clave de acceso y contraseñas de sus cuentas bancarias. El problema en estos casos es que no se está comunicando con una organización legítima real. La información obtenida engañosamente podrá ser utilizada para acceder a las cuentas bancarias del usuario, realizar transacciones sin autorización y además crear nuevas cuentas.

La palabra phishing proviene del inglés fishing, cuyo significado en español es pescando, y hace alusión directa a la idea de captar incautos en la red o en los correos electrónicos. Consiste en adquirir los datos personales, tales como cuentas bancarias y contraseñas, mediante engaño, haciéndole creer a su propietario, que se encuentra en comunicación con su entidad bancaria u otra compañía. El procedimiento inicia cuando un usuario recibe por email, un correo que supuestamente pertenece al banco con el que opera. El correo cuenta con el logo e imagen del mismo. En dicha nota, se

explica que por su seguridad, se realizan cambios en el sistema de ebanking, y como tal, debe contestar dicho email, confirmando el número de cuenta y contraseña para que se compruebe la funcionalidad del mismo; el usuario, reconoce el logo de la entidad, y ni siquiera duda de que pueda ser enviada por ajenos al banco. Cuando el mismo, contesta el email con los datos sensibles, se consuma el engaño, que culmina con el fraude, a través del vaciamiento de sus cuentas bancarias, gracias a la obtención de los datos necesarios para ello”.<sup>49</sup>

Otro modus operandi, que enviste de mayor destreza a los correos electrónicos de esta clase y por consecuente, con mayor credibilidad por parte del incauto, consiste en otorgarle al usuario un hipervínculo hacia la página Web de la entidad bancaria. Cuando el ciudadano lo acciona, ingresa a una página en Internet, que simula ser del banco dónde opera, y le solicita ingrese sus datos y contraseña para abrir la sesión de comprobación de funcionamiento del nuevo sistema más seguro; de esta manera, los delincuentes, están haciéndose de los datos necesarios para acceder al contenido de las cuentas bancarias y vaciarlos.

Con la proliferación de nuevas técnicas de robo de identidades, fraudes, en las cuales se involucran a entidades bancarias y crediticias, las declaraciones de las mismas, no se hicieron esperar.

---

<sup>49</sup> **Ibid.**

En la actualidad, ningún banco envía correos electrónicos o solicita datos referentes a cuentas bancarias a sus clientes, por medios tecnológicos de comunicación, porque los mismos son sujeto de ataque de mal vivientes.

Las entidades bancarias, les comunican a sus usuarios de estas medidas, también lo han publicado en distintos medios masivos de difusión. A su vez, recomiendan a los involucrados, a no contestar ni seguir las instrucciones de algún correo electrónico referente a sus compañías, por más seguro y veraz que el mismo parezca. Lo mismo para la utilización de las nuevas tecnologías de la información y comunicación.

Actualmente, mientras la sociedad de la información avanza impulsada por las nuevas y emergentes oportunidades tecnológicas, las entidades bancarias, las entidades crediticias y otras, han optado por el camino inverso: renegar del uso de mismas, en pos de salvaguardar la integridad del patrimonio de sus clientes, debido al aumento periódico de las modalidades de fraude que se aprovechan de los agujeros de seguridad existentes en este ámbito.

El acto de phishing se basa del engaño para obtener un beneficio sobre los bienes patrimoniales de las personas. Siendo entonces un delito contra el patrimonio, lo lógico es que se configure como un ilícito de estafa ordinario, y como tal se encuentra regulado en el actual código penal guatemalteco; sin embargo, debido al objeto de la estafa, el medio electrónico utilizado por la misma y que estos se configuran como delitos informáticos, porque para configurar el engaño y posterior perjuicio propio o

ajeno, se utilizan mecanismos de ingeniería social, consistentes en subterfugios sobre medios informáticos a través del phishing, acompañadas de la transferencia no consentida de cualquier activo patrimonial.

Aún así, parecería que no queda del todo claro, si el acto se corresponde a la figura de estafa mediante phishing. Advertencias como estas, han sido tenidas en cuenta, a tal punto, que se deben prever modificaciones al Código Penal de manera que se penalice efectivamente y sin distinciones, la figura del phishing.

“Desde el punto de vista de algunos doctrinarios, el phishing no es otra cosa que un delito de estafa, matizado con algunos ingredientes distintos, como por ejemplo, la utilización de medios informáticos y telemáticos para ejecutarlo. Sí es cierto, que el objeto de la acción recae sobre la sociedad de la información, referida a aquella que se sirve de las tecnologías de la información y comunicación; sin embargo, hablar de un puñado de personas que no pertenezcan a esta categorización, es prácticamente imposible, ya que, de alguna forma o de otra, las tecnologías y las comunicaciones telemáticas se han expandido a todos los ámbitos cotidianos, a tal punto de existir una dependencia cuasi total. Este es un aspecto propio de la globalización, por ello, hablar de sociedad de la información, como referirse a la sociedad en términos generales, no presenta diferencias en los hechos”.<sup>50</sup>

---

<sup>50</sup> García Noguera, N. *Phishing*: Un peligro para la banca online. Abogados Portaley Nuevas Tecnologías S.L. 04/04/2005. <http://www.delitosinformaticos.com/propiedadintelectual/phishing.shtml>, pág. 12. Consultada el 10 de marzo de 2010.

Lo que ha sucedido respecto a la figura del phishing, es que, la corriente impulsora de crear nuevas figuras delictivas, proviene en este caso, no de la población en sí, sino de las instituciones bancarias; en efecto, las mismas que han promocionado el sistema de banca en línea y también el comercio electrónico como una nueva mina de oro para sus ingresos, ven amenazadas sus estrategias debido al actuar de grupos organizados de delincuencia informática.

Quizá, uno puede preguntarse, cómo pueden los bancos y cajas verse afectados, cuando el delito de phishing ataca directamente a los usuarios y no a sus entidades, a lo que la respuesta es, debido a un traslado de pérdidas. En general, sucede algo muy parecido con las víctimas de fraudes mediante tarjetas de créditos a través de Internet: Cuando el usuario comunica que ha sido víctima del uso indiscriminado de su tarjeta mediante compras a través de la Web, por lo general, las compañías terminan haciéndose cargo de la pérdida. Y en este caso, sucede algo parecido: Las entidades bancarias terminan por asumir el riesgo hecho realidad, debido a que, más allá de la pesca de un incauto, lo que ha sucedido es una falla o fracaso de la política preventiva y de seguridad de la compañía. Ello se le suma la reticencia de los usuarios de utilizar un nuevo sistema, que aparenta ser más vulnerable que manipular dinero metálico. Por esta razón, la histeria general ante una nueva amenaza para las personas, ha sido trasladada a la sociedad, con el objeto de que sea ésta la que se preocupe en demasía, y exija así, soluciones rápidas a problemas nuevos que podrían alterar el orden social.

Este dinamismo, acompañado con la exigencia de nuevas actuaciones hacia los poderes, forman parte de lo que hoy se vive a pleno como es la sociedad de riesgos; la misma se sumerge hoy en los conflictos personales y patrimoniales, y por ende, le encomienda al Estado una solución inmediata. Éste a su vez, debe prevenir el advenimiento de los riesgos, a través de la ampliación casi constante de la normativa aplicable. Una vez más, esta sensación de inseguridad frente a nuevos flagelos, presiona para soluciones inmediatas, a las cuales el Estado, en vez de encontrarlas mediante el actuar efectivo, prefiere llenar el ojo de la población a través de nuevos enunciados legislativos.

Debe recordarse, que esta situación, no es otra cosa, que una consecuencia de la pasividad y dependencia de los individuos frente a la transferencia de otros sectores, cuya consecuencia inmediata, típica de una sociedad de riesgo, son los efectos secundarios de la misma.

Así, una aceptación sin más de todo lo que es ofrecido, trae consecuencias como la baja calidad de las prestaciones, debido a la implementación de software y tecnología no preparada y estable para cumplir con las necesidades de la población, que posteriormente se ve inmersa en su propia trampa, al ser víctima de los mismos errores que nunca frenó.

“Esta sociedad pasiva de riesgos, permite un redescubrimiento del derecho penal, asistiéndose a una nueva desmarginalización de la víctima, que ahora cobra mayor

relevancia, forzando al ordenamiento a desvincularse poco a poco del tradicional derecho penal patrimonial, para expresarle mayor trascendencia a los nuevos riesgos de una sociedad que exige una expansión, que no se vincula con el derecho penal nuclear”.<sup>51</sup>

Sin embargo, también es cierto, en relación a los delitos informáticos, que éstos son muy fáciles de llevar a cabo, por dos razones: primero, debido a las grandes vulnerabilidades de los propios sistemas de seguridad, que permiten con el mínimo esfuerzo de los malvivientes, hacerse de sus objetivos; y en segundo lugar, por la sensación de lo abstracto en relación a quién es víctima de un fraude informático, ya que ni siquiera puede identificar si lo sucedido ha sido realizado por una persona, máquina o sistema.

Es lo que Reyna denomina la invisibilidad del delito, y a lo que expresa: “Esta invisibilidad del delito, como bien sostiene Herrera Moreno, tendría su razón de ser en la relatividad del espacio y tiempo informático, a través de la cual, en un jugueteón parpadeo cibernético, el delincuente se inviste con los más absolutos atributos de intemporalidad y ubicuidad. A ello se le suma el hecho, de que para el perpetrador, más que nunca, le resulta más fácil escudarse bajo las tecnologías para hacerse del patrimonio de la víctima, que atracarla a la misma por la calle y a punta de pistola. Evidentemente ello y la nueva sensación de impotencia, han desatado esta sensación generalizada de inseguridad ante lo desconocido, de manera tal que se exigen

---

<sup>51</sup> **Ibid.**

respuestas, que solo el derecho penal (aparentemente) las podría ofrecer, expandiendo su manto de tutela”.<sup>52</sup>

Respecto a si existe o no una adecuada gestión del derecho penal, relacionado con los delitos telemáticos, en este caso, el phishing, podría decirse que existe relación positiva con ello. Un ejemplo que se expresa a continuación, puede ilustrar la idea: para que se puedan configurar determinadas condiciones que lleven a la concreción de la estafa a través de la modalidad de phishing, primero deben darse determinadas situaciones, como ser, la obtención de un contacto, ya sea correo electrónico, teléfono celular u otro, de la posible víctima.

En muchos de los casos de fraude informático, se hace evidente, de que algo previo ha fallado, y efectivamente, se comprueba, que los ficheros de bases de datos de las posibles víctimas, han sido consultados sin consentimiento de sus titulares, permitiendo así la extracción por un tercero de datos vinculantes.

“Respecto a la teoría del derecho penal del enemigo y su relación con el phishing, se podría decir que, este siglo en el cual vivimos, conocido como el siglo de la globalización, ha forjado la figura del enemigo, como aquel que se aleja del derecho penal de los ciudadanos para vivir fuera de la legalidad, pero de manera ya irreversible. Solo pensar en las organizaciones criminales, se puede entender el concepto claramente. En estas asociaciones profesionales delictivas, encajan perfectamente los

---

<sup>52</sup> OC- Red.es. (2005). Jornada Riesgos Penales de la banca online: Sistemas de prevención del fraude online. 16/12/2005. [http://www.red.es/prensa/notas/diciembre\\_05/cata\\_uoc.pps](http://www.red.es/prensa/notas/diciembre_05/cata_uoc.pps) Consultada el 10 de marzo de 2010.

ejecutores de delitos tecnológicos, como es la modalidad de phishing. No se trata de un simple hecho aislado, de un aficionado por hacerse de una suma de dinero y desaparecer en el anonimato, sino de verdaderas redes profesionales de individuos que viven de la previa planificación meticulosa de los futuros golpes a dar, y estratégicamente eligen el cuando y el quién. Así, este derecho penal de la guerra, tratará de anticiparse al accionar de la cyberdelincuencia, aumentando las penas, e incluso ahogando las garantías procesales penales correspondientes”.<sup>53</sup>

Cabe destacar, que la tecnología siempre ha estado muy ligada a la perpetración de los actos terroristas. En efecto, a través de las páginas Webs de contenido pornográfico, se escondían mensajes ocultos en las imágenes, los cuales supuestamente se vinculaban a los preparativos de los actos que se llevarían a cabo. El método utilizado era el de la Steganografía, del griego estegano -secreto, escondido- y grafos -escritura, pintura-, lo cual permitió abrir un paraguas a los defensores del derecho penal del enemigo, para incluir entre los objetivos a atacar, las organizaciones delictivas detrás de los ilícitos telemáticos.

Los intentos más recientes de phishing han tomado como objetivo a clientes de bancos y servicios de pago en línea. Aunque la mayoría de veces, el mensaje es enviado por phishers de forma indiscriminada con la esperanza de encontrar a un cliente de dicho banco o servicio, estudios recientes muestran que los phishers en un principio son capaces de establecer con qué banco una posible víctima tiene relación, y de ese modo enviar un correo electrónico o e-mail, falseado apropiadamente, a la posible

---

<sup>53</sup> **Ibid.**

víctima. En términos generales, esta variante hacia objetivos específicos en el phishing se ha denominado spear phishing, literalmente phishing con lanza.

Los sitios de Internet con fines sociales también se han convertido en objetivos para los phishers, dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad.

“Algunos experimentos han otorgado una tasa de éxito de un 70% en ataques phishing en redes sociales. A finales del 2006 un gusano informático se apropió de algunas páginas del sitio web MySpace logrando re direccionar los enlaces de modo que apuntaran a una página web diseñada para robar información de ingreso de los usuarios. Un ejemplo para disfrazar enlaces es el de utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar el nombre de usuario y contraseña (contrario a los estándares). Por ejemplo, el enlace <http://www.google.com@members.tripod.com/> puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando realmente el enlace envía al navegador a la página de members.tripod.com (y al intentar entrar con el nombre de usuario de www.google.com, si no existe tal usuario, la página abrirá normalmente). Este método ha sido erradicado desde entonces en los navegadores de Mozilla Firefox e Internet Explorer”.<sup>54</sup>

La mayoría de los métodos de phishing utilizan alguna forma técnica de engaño en el diseño para mostrar que un enlace en un correo electrónico, esto cuando se utiliza la

---

<sup>54</sup> **Ibid.**

internet, parezca una copia de la organización por la cual se hace pasar el impostor; mientras otros intentos de phishing utilizan comandos en Java Scripts para alterar la barra de direcciones. Esto se hace poniendo una imagen de la página de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la dirección legítima.

En otro método popular de phishing, el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la dirección y los certificados de seguridad parecen correctos. En este método de ataque, conocido como Cross Site Scripting, los usuarios reciben un mensaje diciendo que tienen que verificar sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

“Otro problema con las URL es el relacionado con el manejo de Nombre de dominio internacionalizado (IDN) en los navegadores, puesto que puede ser que direcciones que resulten idénticas a la vista puedan conducir a diferentes sitios (por ejemplo *dominio.com* se ve similar a *d\_mini\_.com*, aunque en el segundo las letras "o" hayan sido reemplazadas por la correspondiente letra griega *ómicron*, " "). Al usar esta técnica es posible dirigir a los usuarios a páginas web con malas intenciones. A pesar

de la publicidad que se ha dado acerca de este defecto, conocido como IDN spoofing o ataques homógrafos, ningún ataque conocido de phishing lo ha utilizado”.<sup>55</sup>

URL es por sus siglas en idioma inglés, Uniform Resource Locator, Localizador Uniforme de Recursos, o sea, la forma de organizar la información en la web. Una URL es una dirección que permite acceder a un archivo o recurso como páginas html, php, asp, o archivos gif, jpg, etc. Se trata de una cadena de caracteres que identifica cada recurso disponible en la WWW. Las URL fueron usadas por primera vez por Tim Berners-Lee en 1991 con el fin de poder crear enlaces entre distintas páginas en la WWW. Desde 1994 el término URL se incorpora a un concepto más general, el URI, pero igualmente se sigue utilizando URL.

IDN, Internationalized Domain Name, es el acrónimo procedente del inglés cuyo significado es Nombre de Dominio Internacionalizado. Se trata del estándar que utilizan todos los registradores para permitir codificar caracteres internacionales en el DNS y así disponer de dominios con caracteres especiales.

Finalmente otro método de los phishers es el uso de los teléfonos fijos o móviles, llamando al usuario del teléfono y solicitándole enviar un fax o mensaje con los supuestos datos de actualización, en donde luego se los capturan.

---

<sup>55</sup> **Ibid.**

## 4.2. Phishing y bien jurídico

El origen del bien jurídico está en la pretensión de elaborar un concepto del delito previo al que forma el legislador, que condicione sus decisiones, pretensión característica de una concepción liberal del Estado, que concibe este como un instrumento que el individuo crea para preservar los bienes que la colectividad en su conjunto crea de suma conveniencia proteger.

En otras palabras, el bien jurídico es la elevación a la categoría del bien tutelado o protegido por el derecho, mediante una sanción para cualquier conducta que lesione o amenace con lesionar este bien protegido, de esta reflexión se puede decir que el bien jurídico obtiene este carácter con la vigencia de una norma que lo contenga en su ámbito de protección, mas si esta norma no existiera o caduca, este no deja de existir pero si de tener el carácter de jurídico.

Esta característica proteccionista que brinda la normatividad para con los bienes jurídicos, se hace notar con mayor incidencia en el derecho penal, ya que es en esta rama del derecho en que la norma se orienta directamente a la supresión de cualquier acto contrario a mantener la protección del bien jurídico, por ejemplo el delito de espionaje informático busca sancionar los actos que difunden en forma irregular la información privilegiada industrial o comercial a través de medios electrónicos.

En la actualidad la conceptualización del bien jurídico, no ha variado en su aspecto sustancial de valoración de bien a una categoría superior, la de bien tutelado por la ley, en cuanto a ciertos criterios como el origen, o como el área del derecho que deba contenerlos, por lo que encaja perfectamente en la intención de tipificar al phishing o suplantación de identidad.

El derecho penal tiene su razón de ser en un Estado social porque es el sistema que garantiza la protección de la sociedad a través de la tutela de sus bienes jurídicos en su calidad de intereses muy importantes para el sistema social y por ello protegibles por este derecho, incluyendo las nuevas amenazas vinculadas a la era digital que se vive actualmente.

“Un Estado social y democrático de Derecho debe amparar sólo las condiciones de la vida social en la medida en que éstas perturben las posibilidades de participación de los individuos en el sistema social. Por tanto los bienes jurídicos serán jurídico-penales sólo si revisten una importancia fundamental, o sea cuando las condiciones sociales a proteger sirvan de base a la posibilidad de participación de los individuos en la sociedad. En un Estado democrático cabe destacar la importancia de la participación de los individuos de vivir en sociedad confiando en el respeto de la propia esfera de libertad individual por parte de los demás, como ocurre los que hacemos parte de la sociedad de la información”.<sup>56</sup>

---

<sup>56</sup> Luque Guerrero, J.M. (2005). Muleros las otras victimas del *phishing*. Comisión de seguridad en la Red. Asociación de Internautas. <http://seguridad.internautas.org/html/1/511.html>, pág. 23. Consultada el 10 de marzo de 2010.

El bien jurídico nace de una necesidad de protección de ciertos y cambiantes bienes inmanentes a las personas como tales, como es y ha sido el uso de las tecnologías de la información y la comunicación; esta protección es catalizada por el legislador al recogerlas en el texto penal, porque si no se afecta un bien que la sociedad considera necesario proteger, se puede incluir en otras leyes como la mercantil, para que la acción y la voluntad de las personas se encuadre legalmente.

Aquellos bienes jurídicos cuya tutela sólo y únicamente puede ser la tutela penal, son los denominados bienes jurídicos penales; al determinar cuales son los bienes jurídicos que merecen tutela penal, siempre se tendrá en cuenta el principio de tener al derecho penal como ultima ratio o última opción para la protección de un bien jurídico ya que este afecta otros bienes jurídicos a fin de proteger otros de mayor valor social.

De otro lado es claro que no aparece otro factor que se revele como más apto para cumplir con la función limitadora de la acción punitiva, sólo los bienes jurídicos de mayor importancia para la convivencia social y cuya protección por otras ramas del derecho hagan insuficiente la prevención que cualquier transgresión que los afecten, lo cual en el presente se evidencia con los denominados delitos informáticos, puesto que la impunidad de estos afecta el desarrollo de la informática en todos sus niveles.

Para algunos el delito informático es sólo la comisión de delitos mediante el uso de los computadores, pues consideran que en realidad no existe un bien jurídico protegido en el delito informático, porque en realidad no existe como tal dicha conducta, pero, en

esta tesis, se considera que estos ilícitos son más que una nueva forma de ejecución de conductas que afecta bienes jurídicos que ya gozan de protección por el derecho penal, porque son formas autónomas debido a la nueva realidad digital de las comunicaciones y las transacciones bancarias.

La concepción que no acepta que son nuevos delitos, se halla en gran parte de la academia que no quiere aceptar este concepto, así como en los abogados de tendencia clásica o los clásicos per se; otros opinan, como en esta tesis, que estos delitos tienen un contenido propio, afectando así un nuevo bien jurídico vinculado con la Información, diferenciando los delitos computacionales y los delitos informáticos propiamente dichos; finalmente una tercera corriente considera que los delitos informáticos deben ser observados desde un punto de vista triple; estos se inclinan más hacia las ciencias forenses informáticas, por considerarlos como fin en sí mismo, pues el computador puede ser objeto de la ofensa, al manipular o dañar la información que este pudiera contener; como medio, a partir de ser una herramienta del delito, cuando el sujeto activo usa el ordenador para facilitar la comisión de un delito tradicional y como objeto de prueba, a partir que las computadoras guardan pruebas incidentales de la comisión de ciertos actos delictivos a través de ellos.

“El bien jurídico ha sido y será la valoración que se haga de las conductas necesarias para una vida pacífica, recogidas por el legislador en un determinado momento histórico –social; es a razón de que a nuestro entender el bien jurídico en esencia no desaparece, solo cambia en cuanto al ámbito de protección que lo sujeta, el desarrollo

de esta institución jurídica pasa por momentos totalmente distintos, ya que los mismos son producto de las necesidades propias del desarrollo de la sociedad, hay que tener en claro que estos no se originan al crear una norma, su existir es previo a la misma; esto es, en un primer momento, el primer paso para la protección de un bien de suma importancia para el conjunto social, la selección de estas necesidades valoradas socialmente y luego positivizadas sea en las páginas de una constitución o de algún convenio internacional, será el segundo paso de nuestra construcción, para una vez terminado la nueva categoría de bienes a protegerse, determinar cuales son verdaderamente materia de protección penal”.<sup>57</sup>

Al protegerse la información, dará más confianza su uso a través de las tecnologías de la información y la comunicación. El nuevo bien jurídico tutelado de la información, es el fruto de una elección política dictada por criterios de oportunidad o necesidad; la protección de nuevos bienes está a veces guiado por criterios emocionales, episódicos y fluctuantes según la presión de ciertos factores de poder como son los medios de comunicación u orden de autoridad legítima como podría ser una ley penal.

A partir de establecer la importancia de la definición del bien jurídico, que busca la protección de la información, se puede considerar la tipificación del phishing o suplantación de identidad, con una redacción que quede de la siguiente manera:

El que diseñe, desarrolle, trafique, venda, ejecute, programe y/o envíe páginas electrónicas o web site, ventanas emergentes, **pop up**, correo electrónico, mensajería

---

<sup>57</sup> **Ibid.**

instantánea o comunicaciones telefónicas, con el fin de inducir, convencer, a hacer creer a los consumidores a divulgar información personal o financiera sobre su cuenta, incluyendo nombre de usuario y contraseña, información sobre tarjetas de crédito, débito, **e-cash**, o acceso a la cuenta bancaria electrónica, **e-bank**, entre otros, incurrirá en prisión de tres a seis años de prisión, siempre que no constituya conducta de mayor gravedad y al pago de una multa equivalente al 100% de lo defraudado.

Al tipificarlo de esta manera, los elementos estructurales del delito son los siguientes:

Sujeto Activo:        Calificado e indeterminado

Sujeto Pasivo:        Preferiblemente personas que manejan una cuenta bancaria a través de Internet

Objeto Jurídico:     La información confidencial como son contraseñas o información detallada sobre tarjetas de crédito u otra información de tipo bancario.

Objeto Material:     La conducta va dirigida a la protección de los sistemas informáticos o de telecomunicaciones que se usan para apoderarse de la información.

Conducta: Se consuma cuando se conjugan los verbos rectores diseñe, desarrolle, trafique, ejecute, programe, llame o envíe.

Esta tipificación permite diferenciar al delito de phishing, de cualquier otro delito informático, siendo fundamental el hecho de que se afecte la confidencialidad de las personas a quienes se estafa o pretende estafar, puesto que se han evidenciado casos donde la persona ha proporcionado todos los datos, pero logra avisar a tiempo a la entidad bancaria, la cual bloquea la ejecución de las acciones digitales necesarias para llevar a cabo el fraude.

Se trata, entonces, de que el Estado guatemalteco dote de herramientas legales al Ministerio Público para que pueda perseguir penalmente a todas aquellas personas que buscan sustraer el patrimonio de los usuarios del sistema bancario, especialmente porque bajo el principio de que no hay pena sin ley anterior, estos pueden quedar en libertad al demostrar que su acción no se encuadra en ninguno de los delitos vinculados a la computación, a los programas informáticos o a Internet que actualmente se encuentran tipificados en el Código Penal. Tomando en cuenta que en el capítulo VII, del Título VI del Libro Segundo del Código Penal se encuentran contenidos los delitos contra Los Derechos de Autor, la Propiedad Industrial y Delitos Informáticos, siendo necesario crear la figura típica propuesta, tomando en cuenta que el derecho penal es cambiante.

Es de recordar que una de las principales obligaciones del Estado guatemalteco es brindarle seguridad jurídica a sus habitantes, lo cual en el caso de los usuarios del sistema bancario, se puede manifestar de varias maneras, tales como evitar la quiebra fraudulenta de bancos o en el caso de la presente tesis, que los usuarios sean estafados por la suplantación de la identidad de la empresa bancaria, pierdan su capital, el cual pueden ser los ahorros de toda la vida, sin tener posibilidades de ser resarcidos por la entidad bancaria ni que el Estado garantice la persecución penal de los sujetos activos porque no existe un delito tipificado con estas características.

## CONCLUSIONES

1. Aunque es importante para las sociedades el desarrollo y mundialización de las tecnologías de la información y la comunicación, la mayoría de países, entre ellos Guatemala, no se han preparado para enfrentar los efectos negativos que conlleva esta nueva realidad, especialmente con lo relacionado a la protección del consumidor y usuario de los servicios digitales como Internet.
2. Aún cuando la doctrina ha desarrollado extensos análisis sobre las características y particularidades de cada uno de los delitos informáticos que se cometen continuamente a través de Internet o por medio de computadoras, las legislaciones de la mayoría de los países de centroamérica, incluyendo a Guatemala, no han legislado de manera específica cada uno de ellos.
3. Los delitos informáticos implican actividades criminales que se puedan encuadrar en figuras tradicionales, tales como robos, hurtos, fraudes y otras, el uso de las técnicas informáticas han creado nuevas posibilidades de la aplicación indebida de las computadoras lo que ha creado la necesidad de una nueva regulación por parte del derecho penal.

4. La tipificación de los delitos informáticos en Guatemala ha sido llevada de manera lenta y parcialmente, en la mayoría de los casos respondiendo a las presiones de grupos de interés, con lo cual han logrado que en el país se legisle en contra de los delitos contra el derecho de autor y la propiedad intelectual, pero no han regulado todos los delitos informáticos.
  
5. El principal problema que enfrenta el sistema bancario guatemalteco para ampliar la cobertura de sus servicios en línea, es la desconfianza del público acerca de la seguridad de estas transacciones, pues muchas personas han sido estafadas a través de actos ilícitos como la clonación de tarjetas de crédito, prefiriendo por esto seguir realizando sus transacciones directas en el banco.

## RECOMENDACIONES

1. La Junta Monetaria de Guatemala, a través de la Superintendencia de Bancos, debe generar una campaña informativa hacia la población guatemalteca, sobre todas las formas que utilizan los estafadores a través de Internet y medios electrónicos para cometer actos ilícitos, con lo cual mantendrán informados a los consumidores para evitar que sean víctimas de estos delitos.
2. El Colegio de Abogados y Notarios de Guatemala, a través de su comisión de formación permanente, debe someter a discusión de los abogados los distintos delitos informáticos definidos por la doctrina, para que determinen la forma en que los mismos deben ser tipificados en el Código Penal, sin dejar de lado ninguno de los conocidos, ni aquellos que se considere están surgiendo.
3. El Congreso de la República de Guatemala, debe elaborar a partir del bien jurídico que se pretende proteger la nueva terminología necesaria para que se encuadren debidamente los delitos, el bien jurídico tutelado, el sujeto activo y el pasivo, que permita evitar confusiones con otros delitos ya tipificados; promoviendo para el efecto la creación de la norma penal respectiva.

4. El Congreso de la República de Guatemala, conjuntamente con los expertos guatemaltecos en derecho informático, debe llevar a cabo una discusión sobre la forma más adecuada para lograr la tipificación de los delitos informáticos, para presentarlos en un sólo capítulo del Código Penal, y dar al Ministerio Público una herramienta legal para perseguir a los sujetos activos de estos delitos.
  
5. Urge tipificar en el Código Penal el delito de phishing, como un mecanismo para lograr que la población tenga más confianza para usar los servicios en línea que ofrece el sistema bancario guatemalteco, logrando con ello la seguridad jurídica de las transacciones a través de Internet que pueden hacer los usuarios de los bancos.

## BIBLIOGRAFÍA

- ACURIO DEL PINO, Santiago, **Delitos informáticos**; México: Ed. Porrúa, S.A. 2007.
- ALEGRIA HIDALGO, Juan Luís, **Derecho penal. Parte general**; Perú: Ed. Píxel Impresiones, 2007.
- AMOROSO FERNÁNDEZ, Yarina, **La informática como objeto de derecho**; Cuba: Ed. Unión Nacional de Juristas de Cuba, 1991.
- CALDERÓN RAMOS, Eduardo, **Estado de necesidad como excluyente de responsabilidad**; Perú: Ed. Cajamarca, 2003.
- CALLIESS, Roberto, **Teoría dogmática del derecho penal**; Venezuela: Ed. Universal, 1987.
- CORDOBA ANGULO, Miguel, **El principio de culpabilidad**; Argentina: Ed. Temas Jurídicos, 1993.
- DE LA LUZ LIMA, María, **Delitos electrónicos**; España: Ed. Tecnos, 2001.
- ESTRADA GARAVILLA, Miguel, **Delitos informáticos**; México: Ed. Universidad Abierta, 1997.
- HANCE, Olivier, **Leyes y negocios en Internet**; México: Ed. Clásica, 2004.
- [http://www.arcert.gov.ar/webs/tips/recomendaciones\\_phishing.pdf](http://www.arcert.gov.ar/webs/tips/recomendaciones_phishing.pdf) Oficina nacional de tecnologías de información (onti). (2006). Recomendaciones para evitar ser víctima del “*phishing*”. Coordinación de emergencias en redes teleinformáticas de Argentina. Versión 1.0. Agosto, 2006.
- <http://www.delitosinformaticos.com/propiedadintelectual/phishing.shtml>, GARCÍA NOGUERA, N. Phishing: Un peligro para la banca online. Abogados Portaley Nuevas Tecnologías S.L. 04/04/2005.
- [http://www.red.es/prensa/notas/diciembre\\_05/cata\\_uoc.pps](http://www.red.es/prensa/notas/diciembre_05/cata_uoc.pps) OC- Red.es. Jornada Riesgos Penales de la banca online: Sistemas de prevención del fraude online. 16/12/2005.
- <http://www.seguridad.internautas.org/html/1/511.html> LUQUE GUERRERO, J. M. Muleros las otras víctimas del phishing. Comisión de Seguridad en la Red. Asociación de Internautas.
- KUNTZ, Christian, **La estructura del derecho penal**; Nicaragua: Ed. Nueva Sociedad, 2004.

LÓPEZ BETANCOURT, Eduardo, **Teoría del delito**; México: Ed. Porrúa, 1994.

LÓPEZ DÍAZ, Claudia. **Introducción a la Imputación Objetiva**; Bogotá: Ed. Universidad Externado de Colombia, 1996.

MAURACH, Klaus Peter, **Tratado de derecho penal**; México: Ed. Academia Mexicana de Ciencias Penales y editorial Porrúa ,1984.

MEZGER-BLEI, Daniel, **Principios de derecho penal**; México: Ed. McGraw Hill, 2002.

MIR PUIG, Santiago. **Introducción a las bases del derecho penal**; Buenos Aires: Ed. Euros Editores S.R.L. 2003.

MIR PUIG, Santiago, **Delincuencia informática**; Barcelona: Ed. Promociones y Publicaciones Universitarias, 1992.

OCTAVIO DE TOLEDO, Ernesto y Susana Huerta Tocildo, **Teoría del delito**; México: Ed. UNAM. 1996.

TÉLLEZ VALDÉS, Julio, **Derecho Informático**; 2ª. ed.; México: Mc Graw Hill, 1996.

ZAFFARONI, Eugenio Raúl, **Manual de derecho penal. Parte general**; México: Ed. Cárdenas, 1991.

### **Legislación:**

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

**Código Penal**. Congreso de la República de Guatemala. Decreto número 17-73, 1973.

**Código Procesal Penal**. Congreso de la República de Guatemala. Decreto número 51-92, 1992.