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

TIPIFICACIÓN DEL DELITO INFORMÁTICO DE ROBO DE IDENTIDAD

MIGUEL ALEXANDER BERMEJO GARCÍA

GUATEMALA, SEPTIEMBRE DE 2011

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

TIPIFICACIÓN DEL DELITO INFORMÁTICO DE ROBO DE IDENTIDAD

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

MIGUEL ALEXANDER BERMEJO GARCÍA

Previo a conferírsele el Grado Académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, septiembre de 2011

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.	Mario Ismael Aguilar Elizardi.
VOCAL III:	Lic.	Luis Fernando López Díaz.
VOCAL IV:	Br.	Modesto José Eduardo Salazar Diéguez.
VOCAL V:	Br.	Pablo José Calderón Gálvez.
SECRETARIO:	Lic.	Avidán Ortiz Orellana.

TRIBUNAL QUE PRACTICÓ

EL EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente: Lic. Mario René Monzón Vásquez.
Vocal: Licda. Mirza Eugenia Irungaray López.
Secretaria: Licda. Marisol Morales Chew.

Segunda Fase:

Presidente: Lic. Héctor René Granados Figueroa.
Vocal: Lic. Carlos Humberto de León Velasco.
Secretario: Lic. Rodolfo Giovani Celis López.

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).

LIC. MANUEL ARTURO ESCOBAR MARTÍNEZ
6ta calle 4-17, zona 1 Edificio Tikal
Tel. 22510365 – 58655438
Colegiado 4,269

Guatemala, 22 de noviembre de 2010

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

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
25 NOV 2010
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Licenciado Marco Tulio Castillo

Como asesor de Tesis del Bachiller **MIGUEL ALEXANDER BERMEJO GARCÍA,** en la elaboración del trabajo intitulado: **"Tipificación del delito informático de robo de identidad"**, me permito manifestarle que dicho trabajo contiene:

a) Se desarrolla a lo largo del trabajo una explicación de los delitos informáticos, puntualizando en a cuanto breves antecedentes, características, elementos principales y su clasificación, misma explicación permite dar razón al proyecto de tesis. Así mismo se realiza una propuesta de la tipificación del delito informático de robo de identidad, argumentando en el trabajo la necesidad que existe en nuestro ordenamiento jurídico para que se tipifique este delito, a raíz del crecimiento del crecimiento tecnológico y la globalización.

b) El estudiante **MIGUEL ALEXANDER BERMEJO GARCÍA** para la realización del trabajo utilizó el método científico, a que el mismo le concedió la producción de conocimientos y criterios válidos, aplicando de igual manera el método histórico, que le permitió el desarrollo de la reseña histórica de los antecedentes tanto del Derecho Penal y de los delitos informáticos, así mismo se apoyó en extensa bibliografía como antecedente, como fuente de doctrina; permitiéndole así realizar un estudio completo y adecuado de los delitos informáticos.

c) Estudié y analicé el contenido del tema propuesto por el estudiante, el cual reúne los requisitos de actualidad no solo en el aspecto académico sino en el aspecto normativo

del Decreto 33-96 del Congreso de la República, Reformas al Decreto número 17-73 Código Penal, por cuanto en el desarrollo del trabajo trata adecuadamente la necesidad de llevar a cabo la tipificación del delito informático de robo de identidad, con la finalidad de dar mayor certeza jurídica a las personas que ingresan sus datos personales en la Red. Así mismo evidencia la importancia de tipificar el delito informático de robo de identidad para otorgar seguridad jurídica y protección de los datos personales.

d) Es importante mencionar que el presente trabajo concluye en demostrar que todas las personas tienen derecho a la protección de los datos personales en todos los ámbitos y evidencia como recomendación, la necesidad de reformar la legislación penal, para adaptarla al desarrollo social, económico y tecnológico y a la natural evolución del derecho penal con relación a los delitos informáticos.

He guiado personalmente al sustentante durante todas las etapas del proceso de investigación científica, aplicando los métodos y técnicas apropiadas para resolver la problemática esbozada, con lo cual compruebe la hipótesis planteada conforme a la proyección científica de la investigación.

El trabajo de tesis en cuestión, refiere los requisitos legales prescritos y exigidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, razón por la cual emito **DICTAMEN FAVORABLE**, a efecto de que el mismo pueda continuar con el tramite correspondiente, para su posterior evaluación por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Deferentemente,

Lic. Manuel Arturo Escobar Martínez

Asesor

Colegiado 4,269

Lic. Manuel Arturo Escobar Martínez
ABOGADO Y NOTARIO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

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

UNIDAD ASESORÍA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, once de enero de dos mil once.

Atentamente, pase al (a la) LICENCIADO (A) GUILLERMO ROLANDO DÍAZ RIVERA, para que proceda a revisar el trabajo de tesis del (de la) estudiante MIGUEL ALEXANDER BERMEJO GARCÍA, Intitulado: "TIPIFICACIÓN DEL DELITO INFORMÁTICO DE ROBO DE IDENTIDAD".

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. CARLOS MANEL CASTRO MONROY
JEFE DE ~~LA UNIDAD ASESORÍA~~ DE TESIS

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

cc.Unidad de Tesis
CMCM/sllh.

LIC. GUILLERMO ROLANDO DÍAZ RIVERA
COLEGIADO 3,738
BUFETE JURÍDICO
LICENCIADO GUILLERMO ROLANDO DÍAZ RIVERA
6ta Avenida 0-60, zona 4 Centro Comercial Zona 4
Oficina 403 "A" Cuarto Nivel Ciudad de Guatemala.
TELÉFONO: 4531-7217

Guatemala, 25 de enero de 2011

Licenciado:
Carlos Manuel Castro Monroy
Jefe de la Unidad de Tesis
Facultad de Ciencias Jurídicas y Sociales.
Universidad de San Carlos de Guatemala.
Su Despacho:

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
25 ENE. 2011
UNIDAD DE ASESORIA DE TESIS
Hora:
Fecha:

Licenciado Castro Monroy

Como revisor del trabajo de Tesis del Bachiller **MIGUEL ALEXANDER BERMEJO GARCÍA,** en la elaboración del trabajo intitulado: **"Tipificación del delito informático de robo de identidad"**, dejo constancia y hago de su conocimiento lo siguiente:

a) El sustentante realizó un análisis exhaustivo de la doctrina y legislación pertinente relacionada con la tipificación de la existencia de los delitos informáticos en la legislación guatemalteca, aportando criterios de importancia tanto para la práctica como la doctrina sobre esa rama del Derecho Penal muy relacionada con el Derecho Informático, puntualizando en cuanto a breves antecedentes, características, elementos principales y su clasificación, las explicaciones permiten dar razón al proyecto de tesis. Se realiza una propuesta de la tipificación del delito informático de robo de identidad, argumentando en el trabajo la necesidad que existe en nuestro ordenamiento jurídico para que se tipifique este delito, a raíz del crecimiento tecnológico y la globalización.

b) La estructura y contenidos del trabajo de tesis realizado por el sustentante en estrecha colaboración con el Asesor de Tesis, reúnen y satisfacen plenamente todos los requisitos reglamentarios y de aportación científica a las ciencias sociales, tratándose de un tema de importancia, actualidad y valor para la práctica jurídica, esgrimiendo justificaciones y argumentos válidos y arribando a conclusiones y recomendaciones concretas a que conviertan el trabajo de tesis en material dable a la discusión para reformas normativas específicas que puedan traducirse en

cambios notorios, específicamente lo relacionado a la tipificación del delito informático de robo de identidad, tema de suma importancia para el Derecho Penal y el Derecho Informático.

c) En el desarrollo y preparación del trabajo de tesis, el sustentante utilizo métodos de investigación diversos, como lo son el método científico y el método histórico, asimismo utilizó variedad de técnicas de investigación y se apoyo en extensa bibliografía como antecedente así como fuente de doctrina contemporánea, lo que hace de su trabajo una fuente de referencia en la materia, debido al esfuerzo recopilatorio realizado.

Como Revisor del trabajo de tesis del sustentante, Miguel Alexander Bermejo García, tuve el agrado de corroborar la utilización correcta y docta del lenguaje y el léxico técnico jurídico propios de un profesional de las ciencias jurídicas, cumpliendo los requisitos plasmados en el Artículo 32 del Normativo para la elaboración de Tesis de Licenciatura de Ciencias Jurídicas y Sociales y del Examen General Público de nuestra facultad; es un trabajo bien cimentado y correctamente dirigido tanto por el ahínco del estudiante, como por la experiencia del señor Asesor de Tesis, como guía y experimentado abogado. Se debe anotar que lo anterior hizo amena esta labor, contando siempre con la mayor disposición del sustentante para atender las observaciones y recomendaciones que como revisor le propuse y que, gracias al alto grado de conocimientos en la materia y jurídicos en general, pudo seguir de forma puntual. Todo ello, me permita extender **DICTAMEN FAVORABLE** al trabajo bajo análisis, a efectos de dar continuidad con el procedimiento de mérito y al final, la correspondiente evaluación por el Tribunal Examinador en el acto de Examen Público de Tesis, que le permita optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales, meritoriamente otorgado por la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala.

Deferentemente,

Lic. Guillermo Rolando Díaz Rivera

Revisor

Colegiado 3,738

Guillermo Rolando Díaz Rivera
ABOGADO Y NOTARIO

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, dieciocho de marzo del año dos mil once.

Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante MIGUEL ALEXANDER BERMEJO GARCÍA, Titulado TIPIFICACIÓN DEL DELITO INFORMÁTICO DE ROBO DE IDENTIDAD. Artículos 31, 33 y 34 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.-

CMCM/sllh.

DEDICATORIA

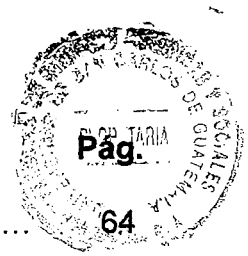
A Dios:	Por regalarme el don de la vida y acompañarme en todo momento sin dejarme desfallecer.
A la Virgen María y San Marcelino Champagnat:	Por interceder por mí y guiarme siempre por el buen camino para alcanzar mis metas.
A mis padres:	Miguel Ángel y Mildred Regina por darme su amor y apoyo siempre, en todos los aspectos de mi vida, ya que no sería nada sin ustedes. Gracias por ser dos de las personas más importantes de mi vida y aguantarme todo el tiempo.
A mis hermanas:	Andrea por estar conmigo siempre que te necesito, ya que sos una de las personas que más me comprende. Lourdes gracias por recordarme lo bello de la infancia.
A mis abuelitos:	Miguel Bermejo, Irma Betancourt y Dámaso García que en paz descansen, gracias por ser mis angelitos e intercesores desde el cielo y Nohemí Pineda, por brindarme su amor incondicional y regalarme una sonrisa. Los amo.
A mis tías, primas e hijos:	Especialmente Carolina y Miriam, por su apoyo y ser muy especiales en mi vida.

A mi familia en general:	En especial a mis tías abuelas y tío abuelo y demás familia con un cariño muy especial.
A Sherlyn Padilla:	Por brindarme su apoyo y comprensión en este tiempo.
A mis amigos y amigas especialmente del Liceo Guatemala y de la Universidad:	Por todo su aprecio y apoyo que me han mostrado, gracias por su amistad y los buenos momentos que hemos compartido. Sin ustedes no hubiera sido lo mismo esta experiencia, a todos los llevo en mi corazón.
A la Jornada Matutina de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala:	Por abrirme sus puertas y ser como mi segundo hogar, guiándome en la búsqueda de la excelencia académica. Les agradezco especialmente a todos mis catedráticos por sus sabias enseñanzas.
A la XII Promoción de la Jornada Matutina:	Por todas las experiencias buenas que vivimos y hacer que estos años fueran muy amenos.
Al Licenciado Rafael Godínez:	Por ser un excelente ser humano y catedrático ejemplar.
A la Licenciada Rosario Gil e Irma Oliva:	Por el apoyo y cariño que me han brindado.
A todos los que hicieron esto posible:	Mi eterna gratitud.

ÍNDICE

CAPÍTULO III

CAPÍTULO IV



Pág.

CAPÍTULO V

INTRODUCCIÓN

En la actualidad la informática tiene un crecimiento inmenso a nivel mundial, abarcando todos los ámbitos de las relaciones sociales, por lo que debemos enfrentarnos a grandes cambios en los aspectos comerciales, civiles, administrativos y jurídicos.

Con el desarrollo y masificación de las nuevas tecnologías de la información debemos realizar un verdadero análisis de la suficiencia del ordenamiento jurídico guatemalteco actual para regular las nuevas posiciones, los nuevos escenarios, en donde observamos los problemas del uso y abuso de la actividad informática y su repercusión en el territorio guatemalteco.

Por medio del Decreto 33-96 del Congreso de la República, se implementaron algunos delitos informáticos dentro de la legislación guatemalteca, siendo un verdadero avance en materia penal e informática. Por lo que es muy importante que se lleve a cabo la tipificación del delito informático de robo de identidad, debido a que este es uno de los ilícitos que ha tenido mayor crecimiento en la red alrededor del mundo. Este delito es una forma de engañar a los usuarios para que revelen información personal o financiera de carácter confidencial, mediante un mensaje de correo electrónico, algún sistema de mensajería instantánea o sitio web fraudulento, debido a que un delincuente realiza operaciones o acciones en nombre de la victima, para cometer fraudes, causando un daño patrimonial y en otras ocasiones también puede darse un daño de carácter moral. Con la implementación del delito informático de robo de identidad, el Estado va brindar más seguridad jurídica a los usuarios de Internet, ya que van a tener la garantía que sus datos privados se encuentran protegidos contra los fraudes.

La presente tesis se desarrolla en V Capítulos, partiendo del análisis de dos conceptos fundamentales como son el derecho informático e informática jurídica, incluyendo los antecedentes, concepto, clasificación, contenido y sus diferencias (Capítulo I), se establece lo relativo a la protección de los datos personales y el derecho a la intimidad (Capítulo II), otro tema relacionado con los anteriores de mucha importancia es el Habeas Data, desarrollando el concepto, características y sus aspectos más relevantes (Capítulo III). En el Capítulo IV se desarrolla el delito informático, iniciando con la teoría del delito, asimismo el concepto, características, clasificación y la regulación de los delitos informáticos en Guatemala. Los capítulos expuestos, permiten desarrollar el delito informático de robo de identidad, partiendo de sus generalidades, concepto, métodos de comisión, elementos, asimismo se realiza un análisis crítico de la importancia de la tipificación del delito de robo de identidad y una propuesta de la tipificación del delito de robo de identidad.

A lo largo de la presente investigación se utilizo el método científico, histórico, se buscó determinar la importancia de introducir un nuevo tipo penal que castigue expresamente el delito informático de robo de identidad, observado desde la perspectiva del derecho informático, ya que esta rama del derecho va ser la encargada de darnos los lineamientos que se necesitan para realizar la correcta tipificación de este delito. En ese sentido, la presente investigación pretende ahondar en la necesidad de llevar a cabo la implementación del delito informático de robo de identidad que debe realizar el legislador guatemalteco, del delito informático de robo de identidad, llevando a cabo una determinación correcta de todos los elementos que lo componen y los casos en que este tipo penal debe aplicarse dentro del territorio del Estado de Guatemala.

CAPÍTULO I

1. Derecho informático e informática jurídica

1.1. Antecedentes

El avance que ha tenido la tecnología es de notable importancia para el derecho, ya que con el surgimiento de la informática jurídica que se ha desarrollado intensamente en la cultura mundial, abarcando todos los ámbitos de las relaciones sociales y jurídicas, debiéndose enfrentar a grandes cambios en muchos aspectos que dependen cada día más de un adecuado desarrollo, entre los que podemos mencionar son el ámbito legal, las relaciones comerciales y la administración pública.

En la actualidad la extensión de la informática y de las redes, como Internet, ha alcanzado la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo del país, ha hecho que los peligros que sufre la información almacenada en los diversos sistemas informáticos, crezcan y se diversifiquen, debiéndose tomar medidas legales que se han adoptado, pero hasta el momento han resultado insuficientes.

La interdisciplina es un elemento importante en la aplicación de las ciencias y las técnicas, ya que para comprender mejor la totalidad de la existencia, se deben de organizar los elementos en forma concatenada, armónica y lógica de las ciencias y las

disciplinas. Dentro del campo del derecho, la interdisciplina se puede manifestar de forma intrínseca y extrínseca. [1]

En forma intrínseca se observan dos ramas, relativas a relaciones distintas con el derecho, verbigracia la relación que existe entre el derecho civil y el derecho penal; de forma extrínseca se observa la relación que concatena al derecho con otras ciencias y disciplinas, como la relación que surge entre la informática y el derecho.

Con el transcurso del tiempo, las necesidades sociales o como en el presente caso relativo a la tipificación de nuevos delitos informáticos, con base en los avances tecnológicos, se crean y modifican estructuras que reclaman su emancipación, cuya culminación es el nacimiento o no de esta estructura, tal es el caso del derecho informático.

La autonomía de una rama del derecho no implica que se separe o desentienda de la ciencia jurídica, sino que aborde los problemas con instituciones propias, para que ésta adquiera autonomía se debe fundar en cuatro principios que son: el campo normativo, el campo docente, el campo científico y en el campo institucional.

El derecho informático no siguió el proceso normal de nacimiento y emancipación de una rama del derecho, que conlleva una evolución que surge por un cambio social y por un periodo largo de tiempo, ya que se buscan soluciones normativas que se adapten a la realidad que esta viviendo la sociedad. Con el derecho informático, no se llevó a cabo la evolución en un periodo de tiempo, ya que los avances tecnológicos

[1] Riascos Gómez, Libardo Orlando, **El derecho a la intimidad, la visión lusinformatica y el delito de los datos personales.** Pág. 5.

modificaron el cuadro de relaciones, y creciendo a una velocidad vertiginosa ahora la tecnología cambia en cuestión de segundos y naturalmente esto lo debemos ver reflejado en el mundo jurídico, donde el derecho aún tiene algunas falencias que se deben superar.[2]

1.2. La informática jurídica

1.2.1. Antecedentes

A través de la historia humana se han dado algunos hechos que debemos conocer brevemente, ya que son antecedentes de la informática, como el del ábaco que fue tan importante para la milenaria cultura, instrumento que servía para contar grandes cantidades en una época muy antigua, de la que se desconoce el inicio de tales prácticas, pero que presuponen una antigüedad mayor a los cuatro mil años antes de nuestra era y evidencian una gran organización en todos los órdenes, de administración, de control de los impuestos, del control económico, del control político, entre otros. En el mismo sentido podemos hablar del sistema de numeración y del uso del cero por el gran imperio maya, cuya práctica de conteo en general, fue utilizada para los usos civiles y militares de la época; también se puede hablar acerca de los utensilios o similares de otras culturas, así como los instrumentos o máquinas para contar por ejemplo de Blaise Pascal, que realizan diversas operaciones matemáticas.

Entre otros antecedentes de los instrumentos usados en diferentes épocas para contar, por cuyas características fueron considerados elementos clave, para almacenar los

[2] **Ibíd.**

datos y en ese sentido sirvieron para que Charles Babbage instrumentara la primera máquina propiamente, como antecedente de la computadora moderna.[3]

Posteriormente diversos grupos iniciaron la fabricación de múltiples plataformas de computadoras, entre ellas la famosa Apple, que después de su gran éxito pareció no repetirlo, lugar que fue ocupado por la plataforma de IBM, que aprovechó mejor las posibilidades de desarrollo, irrumpiendo en los mercados mundiales con gran fuerza e impacto hasta el presente al estandarizar una plataforma tipo para las décadas de los años ochenta y noventa. Después se presentaron las plataformas populares conocidas como: 286, continuaba con la 386, después la sucedería la 486 y a partir de ésta, muchas otras; pero también es importante señalar que simultáneamente se iniciaron otras plataformas de servidores, así como de grandes computadoras y supercomputadoras, situación que continúa hasta el presente, destacando que se inició la producción concomitante de computadoras portátiles y de escritorio, desde el inicio de la estandarización hasta la consecuente aceptación de la plataforma de IBM, así como una serie de accesorios y muchos otros aparatos importantes para multiplicar la función de las computadoras.[4]

1.2.2. Concepto

La informática surge de la fusión de los términos información y automatización. Se reconoce a la informática como un proceso científico, de lo relacionado con el tratamiento automatizado de la información, en un plano operativo eminentemente

[3] Castellanos Hernández, Eduardo. **Temas de derecho informático.** Pág. 14.

[4] **Ibíd,** pág. 15.

interdisciplinario. Es un proceso dentro del cual el papel técnico de los mecanismos de automatización y el carácter científico del método y lógica del diseño del sistema debe realizarse desde la óptica del usuario final.

Por su parte Jordan identifica a la informática "como la ciencia que tiene como objeto propio de su conocimiento la información; como método, la teoría de sistemas; como instrumento operativo, la computación; como ámbito de desarrollo, la organización; como objetivo, la racionalización, la eficacia y la eficiencia de la acción, a partir del control del proceso de producción y circulación de información; como misión, la de contribuir a la libertad del ser humano y a la consolidación de la democracia; y como valor, el de un bien económico".[5]

El Licenciado Omar Barrios define a la informática: "como la ciencia que estudia los procedimientos de automatización de los datos y la información, para posteriormente procesarlos y acceder a ellos para la toma de decisiones".[6]

La informática es una interdisciplina que se relaciona con varias ciencias, siendo una de estas ciencias la jurídica. Por lo que con el concepto de informática debemos proporcionar un concepto de la informática jurídica, por lo que Jordan la define como "La utilización de los diferentes conceptos, categorías, métodos y técnicas propios de la informática en el ámbito jurídico. Se relaciona con la creación, flujo, clasificación, organización, sistematización y utilización de datos requeridos en la producción y en la

[5] Jordan Flórez, Fernando. **La informática jurídica.** Pág. 40.

[6] Barrios Osorio, Omar Ricardo. Derecho e Informática: Aspectos fundamentales. Pág. 3.

administración de lo jurídico, así como el estudio de las implicaciones o efectos que esta utilización produce en el seno mismo del derecho y por ende de la sociedad".

Una definición que engloba la esencia de la informática jurídica es la que nos proporciona Pérez Luño indicándonos que "La informática jurídica estudia el tratamiento automatizado de: las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal. (Informática jurídica documental); las fuentes de producción jurídica, a través de la elaboración informática tanto de los factores lógico-formales que concurren en el proceso legislativo y en la decisión judicial. (Informática jurídica decisional); y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el derecho. (Informática jurídica de gestión)."[8]

Con base a lo anteriormente expuesto podemos determinar que la informática jurídica, es una rama de la Informática, que tiene por objeto utilizar los procedimientos, técnicas, herramientas y recursos propios de ésta, en el campo del derecho.

1.2.3. Clasificación de la informática jurídica

Existe diversidad de clasificaciones acerca de la informática jurídica, por lo que vamos a presentar la que ha tenido más aceptación para su estudio en el derecho, clasificándose de la siguiente manera:

---

[7] Jordan Flórez, Ob. Cit; pág. 45.

[8] Pérez Luño, Antonio, **Ensayos de informática jurídica**, pág. 43.

a) Informática jurídica de gestión

b) Informática jurídica documental

c) Informática jurídica decisional

1.2.3.1. Informática jurídica de gestión

La informática jurídica de gestión trata de aplicar todos los principios informáticos a las actividades de las oficinas jurídicas. Con la automatización de las actividades y gestiones de carácter jurídico que se realizan en la oficina jurídica, tribunales de justicia, administración pública o en cualquier lugar donde el ordenador o computador realiza de manera mas eficiente y óptima, que se refiere a todas las operaciones estandarizadas y que obedecen a pautas regulares y constantes en la escritura, el registro, la transcripción, la contabilidad, la documentación, la comunicación y la certificación. La informática jurídica de gestión se subdivide en:

a) Informática jurídica de gestión registral

Se ocupa de los procesos de automatización de todos los tipos de registros, sean estos públicos o privados, así como el acceso a ellos vía electrónica. Son muy importantes debido a que en los registros se encuentran datos que son muy útiles para la toma de decisiones en cuanto al cumplimiento de requisitos legales, al realizar alguna gestión en un determinado registro.

Entre los entes de carácter público que prestan el acceso a registros, que anteriormente se llevaban por medio del formato de papel, actualmente debido a los

avances de la informática se han digitalizado, y son administrados por sistemas informáticos a los cuales se permite el ingreso a los funcionarios públicos y a las personas particulares, que deseen obtener información acerca de información que se encuentre dentro del registro. Dentro de la Administración Pública de Guatemala contamos con algunos registros que cuentan con acceso en línea, entre los que podemos mencionar: El Registro General de la Propiedad de la Zona Central, que cuenta con una consulta denominada "Consulta a distancia", dentro de la cual se pueden consultar propiedades, seguimiento a documentos presentados y validar razones de testimonio; El Registro Mercantil, que tiene por objeto el acceso en línea registral y poder realizarse procedimientos administrativos en línea; y las municipalidades, como lo observamos en la de la Municipalidad de Guatemala, departamento de Guatemala, la cual cuenta con una amplía base de datos de los registros y otras gestiones que se realizan dentro de la municipalidad.

b) Informática jurídica de gestión operacional

Esta es una rama de la Informática jurídica de gestión, que trata de facilitar la actuación de las oficinas relacionadas con el derecho, por medio de la cual se le delega a la computadora la ejecución de tareas repetitivas, seguimiento de casos, vencimientos de prorrogas, entre otras. En un inicio se utiliza en el campo jurídico procesal para controlar la actuación o etapas de un proceso específico, tanto en la vía administrativa como en la judicial.

Estos servicios son prestados por la administración pública, ya que varios órganos del Estado que utilizan los sistemas informáticos en el control de sus procesos o

expedientes administrativos entre los que podemos mencionar: La Superintendencia de Administración Tributaria, ya que ha implementado un procedimiento administrativo electrónico para el cumplimiento de determinadas obligaciones tributarias, el Sistema de Información de Contrataciones y Adquisiciones del Estado, éste se administra a través de Internet para que el Estado de Guatemala pueda cumplir con una de las etapas en el sistema de contrataciones, como lo es poner en conocimiento de los oferentes de las personas, la compra y contratación de bienes y servicios. Dentro los servidores de administración privada podemos mencionar a INFILE, que cuenta con un sistema para la actualización de los juicios que se presentan en la Torre de Tribunales en la ciudad de Guatemala.

1.2.3.2. Informática jurídica documental

Esta clase de informática jurídica consiste en el tratamiento automatizado de las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal. Esta información puede encontrarse de una forma simple o de una forma automatizada para su búsqueda. Las clases de documentación que procesa la informática documental se clasifican así:

a) La documentación legislativa

Surge a raíz del crecimiento del volumen de los ordenamientos legales, ya que al darse nuevos hechos o actos en la sociedad, el legislador debe crear, reformar o en algunos casos derogar o erogar normas. Anteriormente solo se tenía acceso a la documentación legislativa en el formato papel por medio del Diario de Centroamérica,

pero actualmente hay una serie de sitios web que proporcionan información legislativa, estos pueden ser de acceso público como la página web del Congreso de la República y de acceso privado como lo brinda Lexdelta o INFILE.

b) La documentación jurisprudencial

Se refiere al acceso a los fallos en materia de jurisprudencia y doctrina legal. Estas bases de datos jurídicos se han almacenado en dispositivos ópticos y electromagnéticos, al mismo tiempo puede consultarse vía Internet. Este servicio es proporcionado por la Corte de Constitucionalidad, la Corte Suprema de Justicia y el Centro Nacional de Análisis y Documentación Judicial.

c) La documentación doctrinal

En Internet se encuentra diversidad de doctrina, ya que existe una gran cantidad de sitios web nacionales e internacionales, que estudian temas jurídicos, realizan publicaciones de vital importancia para la práctica del Derecho. Podemos mencionar la página web DERECHOgt, el Centro de Estudios de Derecho, el Instituto Guatemalteco de Derecho Notarial y la página del Colegio de Abogados y Notarios de Guatemala.

1.2.3.3. Informática jurídica decisional

Es conocida también como metadocumental, consiste en el empleo de ordenadores como ayuda a la toma de decisiones de carácter jurídico, esta clase es muy cuestionada, pero hay que hacer énfasis en que no se busca que el ordenador resuelva la decisión que le corresponde al juez, ya que su objeto es ser un apoyo en la toma de decisiones.

1.3. Derecho informático

Los precursores informáticos nunca imaginaron los alcances que llegarían a tener las computadoras en general o aún en campos tan aparentemente fuera de la influencia como el jurídico, todavía más difícil hubiera sido el concebir que el derecho llegaría a regular a la informática. De esta forma a finales de los años sesenta y luego de cerca de diez años de aplicaciones comerciales de las computadoras empezaron a surgir las primeras inquietudes respecto a las eventuales repercusiones negativas motivadas por el fenómeno informático y requirentes de un tratamiento especial.

El derecho de las tecnologías de la información, es una materia típicamente jurídica conformada por un conjunto de disposiciones dirigidas a la regulación de las nuevas tecnologías de la información y las comunicaciones, es decir, la informática y la telemática.

Según Edgar Salazar Cano este nuevo derecho reuniría tres características esenciales: que no se encuentra sectorizado o ubicado en una sola actividad, sino que es amplio y general, debido a que la informática se aplica en numerosos sectores de la actividad socioeconómica; que su unidad viene dada por la originalidad técnica impuesta por el fenómeno informático; y que es un derecho complejo porque los aspectos técnicos de la informática en su interrelación con el derecho, recaen sobre diversas ramas o especialidades jurídicas. [9]

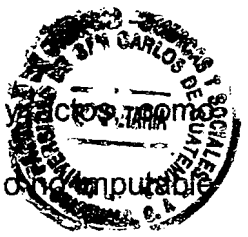
[9] Herrera Bravo, Rodolfo, **El derecho en la sociedad de la información: Nociones generales sobre el derecho de las tecnologías de la información y comunicaciones**. Pág. 3.

1.3.1. Concepto

El derecho de la informática como instrumento regulador del fenómeno informático en la sociedad no ha sido igualmente incursionado por la informática jurídica, probablemente porque se ha dado más importancia a los beneficios que a los eventuales perjuicios que puedan traer consigo los programas de las computadoras. Dentro del reducido grupo de tratadistas sobre el derecho de la informática tenemos a algunos que consideran al mismo como una categoría propia que obedece a sus reglas, que surge como una inevitable respuesta social al fenómeno informático y que, por lo mismo, es un derecho existencialista, en tanto su existencia precede a su esencia.

Si lo anterior implica dificultades, podemos observar que la conceptualización de este derecho a la informática contiene algunos inconvenientes. Esta área al igual que la informática jurídica, permite una creatividad muy amplia, sin que esto, necesariamente trascienda a niveles demasiado especulativos. Por lo que podemos definir el derecho informático como: "El conjunto de leyes normas y principios aplicables a los hechos y actos derivados de la informática".[10] Este concepto permite analizar y distinguir, en primer lugar, que se trata de un conjunto de leyes ya que existen algunos ordenamientos jurídicos nacionales e internacionales con alusión específica al fenómeno informático. Además, son normas en virtud de las cuales se forma la llamada política informática, institución diferente de la legislación informática. Por último, son principios en función de aquellos postulados emitidos por jueces, tratadistas y

[10] **Ibíd.**



estudiosos respecto del tema. Por otra parte, es aplicable a hechos y actos como resultados de un fenómeno vinculado directamente a la informática, sea o no imputable al hombre.

Podemos concluir que el derecho informático es el conjunto de principios, instituciones, doctrina y normas jurídicas, que regulan los bienes jurídicos creados por la informática, al mismo tiempo las acciones y responsabilidades que tienen las personas derivadas del uso de la tecnología.

1.3.2. Contenido

El contenido del derecho informático es muy amplio y tiene cambios constantes debido al desarrollo de la tecnología. El tratadista Rodolfo Bravo[11] nos brinda una recopilación del contenido del derecho informático, cuyos temas son los siguientes:

a) El valor probatorio de los soportes modernos de información, provocado por la dificultad en la aceptación y apreciación de elementos de prueba derivados de estos soportes entre los órganos jurisdiccionales.

b) La protección de datos personales, ante el manejo inapropiado de informaciones nominativas que atentan contra derechos fundamentales de las personas.

c) Los delitos informáticos, es decir, la comisión de verdaderos actos ilícitos en los que se tenga a los computadores como instrumentos o fines.

[11] **Ibíd**, pág. 4.

d) El flujo de datos transfronterizos, con el favorecimiento o restricción en la circulación de datos a través de las fronteras nacionales.

e) La protección de los programas computacionales, como respuesta a los problemas provocados por la piratería de software que atenta contra la propiedad intelectual.

f) Los contratos informáticos, en función de esta categoría contractual sui generis con evidentes repercusiones fundamentalmente económicas.

g) La regulación de los bienes informacionales, en función del innegable carácter económico de la información como producto informático.

h) La ergonomía informática, como aquellos problemas laborales suscitados por la informatización de actividades.

Los temas expuestos anteriormente, no excluyen a las ramas y fuentes tradicionales del derecho informático. Debido a que no es fácil atribuirle a una rama en particular tal o cual problemática de estudio del derecho de la informática. Por el contrario, cada vez se estrechan más estos temas afectando al derecho civil, penal, constitucional o procesal simultáneamente.

1.3.3. Diferencia entre el derecho informático e informática jurídica

Debemos delimitar la diferencia entre la informática jurídica y el derecho informático, para realizarlo de una manera sencilla debemos observar cual es el objeto básico de cada una. La informática jurídica, consiste en incorporar los avances tecnológicos de la

informática al derecho, se refiere a utilizar sus creaciones por medio del hardware, software, se refiere a la Informática, aplicada al estudio, desarrollo y ejercicio del derecho, la informática es un instrumento del derecho; y el derecho informático tiene como objetivo investigar y regular el fenómeno informático en cuanto a su incorporación en la sociedad, debido a los hechos relacionados con la informática, que surjan dentro de la sociedad que deban de ser regulados, para brindar seguridad jurídica a los derechos de las personas ante el inminente desarrollo de la tecnología.

1.4. Relación del derecho penal con el derecho informático

El derecho penal, a lo largo de la historia ha evolucionando con base al devenir que ha tenido la sociedad, ya que ha tenido que incrementar la aparición de delitos con base a los hechos que surgen en el seno de las relaciones sociales. Ha existido una adaptación al sistema social, ya que el legislador debe regular toda conducta que afecte a los miembros del conglomerado, por lo que deben agregarse nuevas formas de comportamiento delictual. Por medio de la informática las personas han encontrado nuevas formas para poder realizar ilícitos, ya que han utilizado los avances tecnológicos para lograr poner en peligro o dañar los derechos de las personas. El primer delito informático se produjo alrededor del año 1966 en los Estados Unidos de Norteamérica, ya que un programador de un banco manejaba un ordenador al que le agregó una especie de parche, para que cuando el realizara operaciones bancarias con su cuenta, el ordenador las ignorara, por lo que este trabajador obtenía un beneficio a costa del banco.

Existen una serie de posiciones doctrinarias acerca de las nuevas formas de cometer delitos informáticos, ya que estos delitos no se han estandarizado a nivel mundial, y algunos juristas creen que estos delitos deben de encuadrarse como convencionales. Se observa que la forma de cometer estos delitos, es utilizar la computadora como un medio y como fin, por lo que esta característica los individualiza como delitos informáticos.

Existen algunos vacios en el ordenamiento jurídico penal, sobre nuevas conductas delictivas relacionadas con la informática, que los legisladores deben de tomar en cuenta para realizar algunas reformas posteriores al Código Penal, agregando estos delitos que actualmente se están llevando a cabo sin que exista una regulación penal que los tipifique. El derecho informático debe servir de base y actuar conjuntamente con el derecho penal, para lograr una adecuada regulación de los delitos informáticos que aquejan a la sociedad.

CAPÍTULO II

2. Protección de datos personales y derecho a la intimidad

En la actualidad han aparecido nuevas técnicas que limitan nuestro derecho a la intimidad, relacionadas con el abuso de poder, así mismo como la necesidad de contar con información acerca de las personas y la libertad de acceso a la información, es necesario que se realicen algunas reformas en la legislación, para que se pueda proteger la vida privada e intimidad de las personas, teniendo como objeto que esta privacidad no sea transgredida, para lo que se necesita del apoyo de la ciencia informática, por medio de la cual se violan con frecuencia estos derechos, y para que surja esta protección se necesita que exista una sólida protección de datos que nos debe brindar el Estado, por medio de una regulación específica y que debe llevarse a cabo por sus órganos, actualmente se encuentra vigente la Ley de Acceso a la Información Pública, Decreto 57-2008 del Congreso de la República.

Es necesario que se tomen las medidas pertinentes que tengan como finalidad evitar que miembros del Estado, de cualquier empresa privada o una persona particular, pueda realizar acciones con total discrecionalidad y sin ningún tipo de control, ya que se deben de establecer una serie de mecanismos adecuados que permitan a la ciudadanía conocer los actos efectuados por cualquiera de estos funcionarios o empleados, ya sean públicos o privados. Uno de los mecanismos que se plantean es el reconocimiento del derecho de acceso a la información regulado en la Ley de Acceso a la Información, que tiene como fin, evitar que se caiga nuevamente en el

autoritarismo o en acciones violatorias de los derechos fundamentales de las personas o en acciones que afecten económica y socialmente a la mayoría de la población.

Existen numerosos motivos, por los cuales se ha generado la discusión de regular un conjunto de mecanismos con su respectivas garantías, que permitan generar la protección de los datos privados y el derecho a la intimidad, con el objetivo de evitar que se violen las garantías fundamentales de las personas, por lo que los miembros de la sociedad civil, van a poder controlar que datos van a ser públicos y cuales van a ser privados.

Es de vital importancia que exista una regulación y clasificación legal de los datos personales, ya que en el mundo virtual existe una infinidad de información, que puede contener datos que puede obtener cualquier persona, con los cuales puede realizar perfiles culturales, económicos y sociales. En este contexto podemos observar la importancia que tiene la información ya sea a nivel nacional, como en el ámbito internacional, por lo que se debe dar un tratamiento adecuado a esta información, conteniendo datos personales de las personas, que por medio de la tecnología, se escapa de nuestras manos y se convierte en una fuente de ingresos de empresas inescrupulosas, que comercian con nuestros datos privados, violentando nuestro derecho de intimidad.

Se debe establecer que por medio de la tecnología se pueden obtener una serie de datos personales que son de gran valor o que representan poder, entre los que podemos citar:

a) Datos biográficos: Nombre, lugar y fecha de nacimiento y raza.

b) Datos sobre el domicilio: Dirección exacta del domicilio y teléfono.

c) Datos civiles: Estado civil de la persona e información acerca de los parientes legales y civiles.

d) Datos laborales: Lugar y teléfono de trabajo, puesto de trabajo y salario.

e) Datos financieros: Información acerca de las cuentas bancarias y tarjetas de crédito.

f) Información policíaca: Antecedentes penales y policiacos.

2.1. Datos de carácter personal

Con base en la legislación comparada de España, según la Ley Orgánica de Protección de datos de carácter personal, se definen los datos de carácter personal "Como cualquier información concerniente a personas físicas identificada o identificables; y por tratamiento las operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, elaboración, conservación, modificación, bloqueo, y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones o transferencias". Estos datos personales son aquellos que tienen características identificadoras de las personas o que se les pueden imputar a ellas; adquiriendo una vital importancia temas como la regulación de su uso, su manipulación y su protección legal.

Se entiende por responsable del tratamiento la persona física o jurídica de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Por su parte se definen los ficheros como todo conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Los datos personales se encuentran clasificados como: Datos personales íntimos que se subdividen a su vez en datos personales sensibles y datos personales no sensibles; y los datos personales públicos que desarrollaremos a continuación:

- **Datos personales íntimos**

- **Datos personales sensibles**

Se definen como "aquéllos que por sí solos impulsan naturalmente a un individuo a la más íntima y absoluta reserva de dicha información. Por su carácter, requieren una regulación sumamente fina, detallada y muy especial que proteja correctamente la difusión de este tipo de datos y que su divulgación lo coloque en una situación de extremada incomodidad social"[12].

[12] Elías, Miguel S., **Situación legal de los datos de carácter personal frente a las nuevas tecnologías, Capítulo I**, 2001, http://vlex.com/vid/situacion-caracter-personal-frente-107859 (16 de junio de 2010)

- **Datos personales no sensibles**

Se definen como "Son aquéllos que se refieren a un sujeto individualizado y son relativos a su fuero interno o íntimo sin llegar a ser información puramente sensible. Identifican su personalidad, sus creencias e ideologías, sus pensamientos, sentimientos y salud, entre otras cosas".[13] Este tipo de datos son los relacionados al orden privado de los individuos, que los hacen merecedores de una protección más profundizada y específica que los demás tipos de datos generales, debido a que se revelan exclusivamente de forma particular e individual, y rara vez son objeto de tratamiento público.

- **Datos personales públicos**

Este tipo de datos se puede definir como: "Son aquellos datos que constan en numerosos registros de carácter público o privado."[14] Entre estos datos podemos citar el nombre y apellido, domicilio, estado civil, filiación, número de teléfono, la cédula de identidad y el pasaporte, título profesional, entre otros.

2.1.1. Los registros o bases de datos computarizados

A través del tiempo los seres humanos han basado su aprendizaje en experiencias que han tratado de preservar, ya que en los inicios de la sociedad, el aprendizaje era transmitido de forma oral, de generación en generación, como cuentos, leyendas o historias de las experiencias vividas por las personas de mayor edad en la comunidad.

---

[13] Ibíd.

[14] Ibíd.

Con la evolución de la sociedad y el surgimiento de la escritura, se crean formas más seguras para poder almacenar y conservar la información, ya que de los papiros se desarrolla la imprenta y así surgen los libros, que contienen una descripción de la historia al mismo tiempo que todo tipo de información y conocimiento útil para las personas.

Desde entonces se han creado numerosos instrumentos y sistemas de almacenamiento, en donde se archivan todo tipo de datos incluso los de carácter personal, sin que ésto afectara la intimidad y vida privada de los sujetos tal como señala el autor Santos Cifuentes "esa expansión de los archivos de toda índole, personales y de bienes, debido en general a la lentitud en la confección, falta de comunicación entre sí, tardanza en la búsqueda y encuentro de lo anotado, posibilidad de reaccionar a tiempo para evitar que se comuniquen los errores o que se publiquen las intimidades, facilidad en los pedidos de corrección antes de que se llegue al daño por causa de la entrada de asientos incompletos, inactuales o falsos, impidió que se levantara la inquietud ni se pensó en los peligros que para el ser humano tales registros podían representar". [15]

Actualmente la evolución de los sistemas computadoras, la proliferación de las computadoras utilizadas de forma masiva y la creación de las bases o bancos de datos computarizados, la protección de los datos personales ha cambiado, ya que se ha convertido en una preocupación para las personas que pueden verse afectados en sus derechos, debido a que no existe un control estatal que nos de la seguridad que toda

[15] Santos Cifuentes, **Derecho personalísimo a los datos personales en la Ley T.1997-E**, Pág. 35.

nuestra información, este protegida, por lo que se restringen nuestros derechos de privacidad y libertad de acción.

Con la informática surge una serie de posibilidades en beneficio de la sociedad como son la posibilidad de una mayor capacidad de almacenamiento, la rapidez de la visualización de los archivos y la posibilidad de transmitirlos de una forma rápida y eficaz de un lugar a otro. Al no ser utilizados estos beneficios de manera adecuada se pueden ocasionar daños a los derechos de las personas, pues dentro de las bases de datos, se encuentran diferentes tipos de características específicas de las personas como las sociales, psicológicas, somáticas, sanitarias, históricas, familiares, entre otras. Esta información puede ser utilizada por terceros, sin el consentimiento del titular, lo que acarrea una violación a sus derechos, al mismo tiempo, es un peligro para su privacidad, intimidad, su honor y su reputación.

Existe un temor en la proliferación de la violación de estos derechos fundamentales, que se lleven a cabo a través de los sistemas de archivos, ya que existen una serie de mecanismos tecnológicos que funcionan como medios de control o vigilancia de las actividades de las personas entre los que podemos mencionar: los teléfonos celulares, los software de red, el vídeo, medios para ver a través de la vestimenta o a través de edificios, software para reconocer el contenido de un mensaje electrónico y las cookies.

2.1.2. Conceptos fundamentales acerca de los registros y bases de datos

Dentro de este apartado se desarrollan una serie de conceptos que son importantes para comprender el presente capítulo, estos son los siguientes:

Existe una confusión entre el concepto de dato e información, no obstante estos conceptos son completamente diferentes. Por dato debemos entender "el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad y aceptamos que ese dato se encuentra en un documento o soporte con la calidad de testimonio. En cambio por la información entendemos "la acción de informar o dar noticia de alguna cosa"[16]. Con base a los anteriores conceptos, podemos determinar que al ser almacenados o sometidos los datos a diversos tipos de tratamiento, ya sea por medios informatizados o no, con la finalidad de obtener un resultado específico, entonces se convierten en información.

El almacenamiento de datos es la conservación o custodia de datos en un registro o banco de datos. Por el tratamiento de datos debemos entender, las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

[16] Davara Rodríguez, Miguel Ángel. **Manual de derecho informático**. Pág. 44.

La comunicación o transmisión de datos es el dar a conocer mediante cualquier mecanismo los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

Se entiende que registro es el: "lugar, archivo, oficina donde se asientan los datos. Estos datos se pueden incluir en patrones, protocolos, ficheros, y pueden ser manuales o informáticos. Los datos registrados pueden pertenecer a una persona o a una cosa, o a la relación de ambas"[17]

Finalizando otro concepto importante es el referente a las bases de datos que son el: "conjunto de archivos interrelacionados que son creados y manejados por un sistema de gestión o de administración de bases de datos, los cuáles controlan la organización, almacenamiento, recuperación, seguridad e integridad de los datos de dicha base"[18]

2.2. Libertad informática

Los derechos fundamentales han evolucionado debido a los cambios que ocurren en las diferentes sociedades, por lo que han surgido sucesivas generaciones de derechos fundamentales. Actualmente nos encontramos ante la tercera generación de derechos humanos, cuya característica específica es que se origina con base en las nuevas problemáticas surgidas a raíz de los grandes adelantos tecnológicos y científicos.

Debido a que existe la posibilidad de acumular grandes cantidades de datos que afectan a circunstancias personales, de almacenarlos ordenadamente, de recuperarlos

[17] Falcón, Enrique M, **Habeas Data. Concepto y procedimiento**. Pág. 52.

[18] Ibíd.

en forma inmediata, así mismo como transmitirlos sin problemas de distancias, se ha generado una nueva problemática y un nuevo reto para la defensa de los derechos fundamentales, incluso de un nuevo derecho denominado libertad informática que goza de una autonomía total.

Este nuevo reto surge a raíz del auge de los sistemas computarizados, el derecho informático, genera un poder informático de dimensiones insospechadas. El poder informático, se refiere a la capacidad de registro de las computadoras, la rapidez de consulta y de transparencia de datos y la cobertura de toda esa información genera para quién la posee o pude acceder a ella una fuerte dosis de poder, que puede ser económico y al mismo tiempo político.

La libertad informática es el derecho que tiene toda persona para hacer uso de las posibilidades que le brinda el sistema informático en su conjunto como son la de acceder rápidamente a la información, la posibilidad de crear o diseñar programas informáticos, así como el diseño de recolección, almacenamiento, procesamiento y difusión de la misma.

El derecho a la libertad informática garantiza el nuevo status del individuo de la sociedad digital, en tanto y en cuanto asegura que la información de carácter íntimo o privado del individuo no pueda ser manipulada o transmitida por terceros sin su consentimiento y que sea rectificada y/o actualizada en los casos necesarios. También le concede a una persona una especie de control frente al tratamiento automatizado que de sus datos realicen terceros, por tanto, estos derechos constituyen un cauce constitucional para el equilibrio de poderes, entre la libertad de información y

comunicación, y el respeto al derecho a la privacidad, entendido este último en su sentido positivo como facultad de disposición y control de la información individual como lo son los datos personales y no sólo en su acepción negativa como facultad para limitar las intromisiones o injerencias de terceros. Lo que se busca es mantener un equilibrio entre la libertad de expresión y de información en la sociedad cibernética y el derecho a la privacidad, vale decir, el derecho a que el Estado y los particulares no invadan las esferas privadas del individuo y que estos puedan ser protegidos a través de recursos eficaces, como lo es el Habeas Data.

El derecho a la libertad informática constituye un avance en la configuración de los derechos fundamentales, especialmente con las nuevas libertades en las sociedades tecnológicas.

La creación de nuevas tecnologías de la informática, de las telecomunicaciones y de la telemática crean nuevos espacios que requieren ser regulados por el derecho, pero sin duda irrumpen de manera agresiva en las dimensiones de la libertad humana, consecuentemente podemos sostener que el derecho a la libertad informática constituye una respuesta a la violación de las libertades es la sociedad informática.

2.3. El derecho a la intimidad y a la privacidad

Para iniciar, determinamos que la Intimidad es la parte de la vida de una persona que no ha de ser observada desde el exterior, y afecta sólo a la propia persona. Se incluye dentro del ámbito privado de un individuo cualquier información que se refiera a sus

datos personales, relaciones, salud, correo, comunicaciones electrónicas privadas, entre otros.

Es el derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida personal, es decir, de sus sentimientos y comportamientos. Una persona tiene el derecho a controlar cuándo y quién accede a diferentes aspectos de su vida personal.

La privacidad es la parte más profunda de la vida de una persona, que comprende sus sentimientos, vida familiar o relaciones de amistad. Según dicta el Artículo 12 de la Declaración Universal de los Derechos Humanos: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

El derecho a la intimidad y a la privacidad, se encuentran dentro de los derechos de ámbito personal o de personalidad, es decir comprenden el derecho de cada persona a tener una vida privada, sin que nadie pueda penetrar en ella a no ser con su autorización. Estos derechos garantizan que la persona pueda disponer libremente de una esfera propia, privada, sin interferencias del exterior, sea de la comunidad o de otras personas.

El derecho a la intimidad se configuró, tanto en el ámbito europeo como latinoamericano, sobre la base del derecho a la inviolabilidad de domicilio y a la

inviolabilidad de comunicaciones y papeles privados. Actualmente, este derecho incluye la protección del honor, la persona, la familia y la propia imagen.

El derecho a la privacidad tiene un tratamiento jurídico de origen angloamericano, debido a que la privacidad, fue transformándose a medida que los avances tecnológicos influían en cada uno de los aspectos de la vida social. De esta forma se propagaron varias teorías respecto al objeto de estudio: las que se referían únicamente a aspectos de la persona, a las que se referían a aspectos económicos y aquellás que daban cabida a las diferentes funciones de la protección legal del individuo en contextos diferentes de la sociedad automatizada: desde el procesamiento automático de información hasta la interceptación telefónica.

La privacidad en un primer momento fue percibida desde un punto pasivo: como protección de la vida privada relacionada con información de medios de prensa, posteriormente asume un papel más activo, ya que se concibe como el derecho de los individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y con qué extensión puede ser comunicada la información acerca de aquellós.

El juez Harlan estableció dos requisitos en relación a la privacidad que son citados en opiniones posteriores como determinantes: en primer lugar, que la persona exhiba una subjetiva pero cierta expectativa de privacidad, y segundo, que aquella expectativa sea reconocida por la sociedad como razonable.[19]

[19] Ramírez, William; Pons, Juan Pablo; y Vásquez Nadezhda. **Libre acceso a la información, protección de datos y habeas data.** Pág. 72.

En Inglaterra, si bien en un comienzo la discusión se centró en la de dar una definición de la privacidad y de cómo proteger este derecho de la persona, con posterioridad se consideró que este derecho no podía ser definido y por lo tanto la doctrina y legislación encaminaron sus esfuerzos a proteger sólo una parte especial de la intimidad de las personas, que es la que tiene que ver con sus datos personales.

En España, el derecho genérico a la privacidad encuentra su fundamento en el derecho a tener un ámbito personal y reservado de vida, sobre el cual sólo el propio individuo debe decidir. Estos derechos de intimidad implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, es necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana.

Estos hechos deben ser tratados como dos derechos distintos, siendo su ámbito el mismo, que se refiere a la protección de estos derechos frente al tratamiento de datos de carácter personal, por lo que no es necesario hacer distinción de los mismos.

2.4. Integridad y protección de los datos personales

Los países europeos y los Estados Unidos de Norteamérica han sido quiénes desde hace varias décadas han venido discutiendo e incorporando en su ordenamiento jurídico, leyes que protegen los derechos de intimidad y privacidad de las personas frente al tratamiento que se le puede dar a datos de carácter personal. Los legisladores de estos países no han creado una garantía procesal constitucional específica sino que, sobre la base de la interpretación de los derechos fundamentales

de las personas han aprobado leyes que regulan el tratamiento automatizado de datos de carácter personal.

En el plano latinoamericano, la protección del derecho a la intimidad y privacidad, específicamente de la protección de datos personales mediante el tratamiento de los mismos han merecido un tratamiento constitucional diferente. Estos derechos han motivado que se cree la garantía procesal constitucional del Habeas Data. No obstante ello, en la actualidad varios países de América han creado leyes específicas para la protección de datos personales.

2.4.1. Leyes de protección de datos personales

Entendemos como mecanismo de protección de datos personales "el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para que de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad"[20]

El jurista Hondius, citado por Ekmekdjian, la define como "aquella parte de la legislación que protege el derecho fundamental de libertad, en particular el derecho individual a la intimidad respecto del procesamiento manual o automático de datos". Pérez Luño, también es citado por Ekmekdjian, la define como "el conjunto de bienes o intereses que pueden ser afectado por la elaboración de informaciones referentes a personas identificadas o identificables". La protección de datos no ha sido imaginada

[20] Dávara, Miguel, Ob. Cit. Pág. 47.

para proteger a los datos per se, sino a su fundamento, que es la protección de una parte sustancial del derecho a la intimidad, que se refiere a la información individual, entendiendo ésta como la información que incluye el honor, la persona, la familia y la propia imagen.

Las leyes de protección de datos han ido evolucionando a través del tiempo, por lo que a nivel mundial se han emitido o han tenido vigencia, diferentes generaciones de leyes de protección de datos.

Las leyes de primera generación fueron emitidas como mecanismos de garantía con la finalidad de establecer los límites a la evolución y utilización de los sistemas informáticos. En este sentido se ubican la *Datenschuz* federal alemana de 1977 y la *Datalag* sueca de 1973.

Las leyes de la segunda generación fueron emitidas con la finalidad de garantizar la calidad de los datos introducidos en las bases o archivos. Estos mecanismos de garantía se plasmaron a través de cláusulas legales de protección para las informaciones consideradas sensibles por su incidencia sobre la vida privada. Se acogen a la *Privacy Act* norteamericana de 1974, la *Loi relative á L'informatique aux fichiers et aux libertés* francesa de 1978, y a las constituciones de Portugal de 1976 y de España de 1978.

Las leyes de la tercera generación se han emitido como respuesta a los nuevos problemas surgidos a raíz de los mayores adelantos tecnológicos y de política legislativa. Entre éstas tenemos el *Convenio para la protección de las personas con*

respecto al tratamiento automatizado de datos de carácter perso del Consejo Europeo de 1981 y la *Data Protection Act* inglesa de 1984.

Estas leyes se han emitido con la finalidad de armonizar los derechos y libertades informáticos con la gama de derechos que pueden verse afectados por el mismo como lo son la libertad política y religiosa, la intimidad, la privacidad, el honor, entre otros.

2.4.2. Principios que rigen las leyes de protección de datos

Dentro de las primeras normas europeas sobre datos personales se establecen diez principios comunes a las leyes de protección de datos que son los siguientes:

a) El de la justificación social: según el cual la recolección de datos debe tener un propósito general y usos específicos socialmente aceptados;

b) El de la limitación de la recolección: el cual estatuye que los datos deben ser obtenidos mediante medios lícitos, es decir, con el conocimiento y consentimiento del sujeto de los datos o con autorización legal, y limitarse al mínimo necesario para alcanzar el fin perseguido por la recolección;

c) El de calidad o fidelidad de la información: que implica la obligación de conservar los datos exactos, completos y actuales;

d) El de especificación del propósito o la finalidad: implica que los datos no sean usados con fines diferentes;

e) El de confidencialidad: conforme el cual el acceso de terceros a los datos debe tener lugar con el consentimiento del sujeto o con autorización legal;

f) El de salvaguarda de seguridad: por el cual el responsable del registro de datos personales debe adoptar medidas adecuadas para protegerlos contra posibles pérdidas, destrucciones o accesos no autorizados;

g) El de política de apertura: que implica asegurar el conocimiento, por parte del público, de la existencia, fines, usos y métodos de operación de los registros de datos personales;

h) El de limitación en el tiempo: que entraña su conservación hasta que sean alcanzados los fines perseguidos;

i) El de control público: que implica la necesaria existencia de un organismo responsable de la efectividad de los principios contenidos en la legislación; y

j) El de participación individual: que consagra el derecho de acceso a los datos y los derechos conexos.

Estos principios han sido reconocidos en las demás legislaciones a nivel mundial e incluso en los instrumentos de protección de datos de carácter mundial y regional.

CAPÍTULO III

3. Habeas Data

3.1. Concepto

El término Habeas Data, por analogía con el de Habeas Corpus, significa tráigase el dato o que vengan los datos, ya que Habeas, significa aquí tengas en posesión y Data es definido como representación convencional de hechos, conceptos o instrucciones de forma apropiada para la comunicación o procesamiento de los medios automáticos. El Habeas Data fue tomado parcialmente del antiguo instituto del Habeas Corpus, ya que su primer vocablo significa conserva o guarda tu, y del ingles data, sustantivo que significa datos, por lo que en síntesis puede traducirse como conserva tus datos.

Otra explicación que consideramos acertada es la que nos brinda Enrique Falcón, ya que establece que el Habeas Data es una extensión del Habeas Corpus y que viene a significar: traigan el dato y sométanlo al tribunal. Sin embargo el verdadero origen del término es desconocido, aunque reciente. La expresión, como en otros campos del derecho es una construcción nominal sustantiva en la cual el adjetivo habeas califica una cualidad permanente del sustantivo data.

El Doctor Samuel Abad Yupanqui, nos dice que el Habeas Data se define como el "derecho que tiene por objeto garantizar la facultad de las personas para conocer y acceder a las informaciones que les conciernen archivadas en bancos de datos;

controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados para disponer sobre su transmisión.

Una definición que consideramos adecuada para el término Habeas Data es la que nos expone Ekmekdjian, ya que nos señala que es "el derecho que asiste a toda persona –identificada o identificable- a solicitar judicialmente la exhibición de los registros –públicos o privados- en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación".[22]

Según el autor Pablo Andrés Palazzi el Habeas Data "puede ser concebido como una acción judicial para acceder a registros o bancos de datos, conocer los datos almacenados y en caso de existir falsedad o discriminación corregir dicha información o pedir su confidencialidad".[23]

El autor Juan Morales Godo destaca que el Habeas Data comprende: obtener información de la entidad responsable de los datos acerca de la existencia de datos que le conciernen; ser informado dentro de un plazo razonable y de manera comprensible; oponerse a cualquier dato que le concierna y a que esa oposición quede registrada; obtener que los datos relativos a su persona, en caso de prosperar su oposición, sean suprimidos, rectificados o completados; ser informado de las razones

---

[21] Abad Yupanqui, Samuel. **La Constitución de 1993. Análisis y comentarios.** Pág. 266.

[22] Ekmekdjian, Miguel Ángel y Caolgero Pizzolo. **Habeas Data. El derecho a la intimidad frente a la revolución informática.** Pág. 1.

[23] Palazzi, Pablo Andrés. **El Habeas Data en el derecho argentino.** Pág. 3.

por las cuales se deniega su derecho de acceso o éste no se le conceda en lugar, tiempo y forma razonable; y oponerse a toda negativa a darle las razones mencionadas precedentemente.

La formula utilizada por el Tribunal Constitucional alemán en 1983, establece que el Habeas Data es el derecho a la autodeterminación informativa, tuvo por objeto garantizar la facultad de las personas para conocer y tener acceso a las informaciones que les conciernen, las cuales son archivadas en bancos de datos para controlar su calidad, lo cual implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados y disponer sobre su transmisión.

Con base a las anteriores definiciones concluimos que el Habeas Data es la garantía procesal constitucional, diseñada para controlar la información personal contenida en bancos de datos, cuyo derecho implica la corrección, la cancelación, y la posibilidad de restringir y limitar la circulación de los mismos. Este concepto ha sido adoptado por diversos países latinoamericanos, simulando el recurso del Habeas Corpus que protege la libertad, mientras que el Habeas Data protege la información nominativa, es decir, aquélla que identifica el individuo.

Es elemental que desarrollemos esta garantía constitucional, ya que en la actualidad ha cobrado gran importancia en nuestra sociedad, con el auge de los bancos informáticos de datos, a los cuales se puede acceder de una manera relativamente fácil de muy diversos y sofisticados modos, por lo que se multiplica la posibilidad de propagar datos personales, cuya difusión puede perjudicar, de cualquier modo, a su titular, agraviando

su derecho a la intimidad y al mismo tiempo puede utilizarse esta información para la comisión de delitos.

3.2. Naturaleza jurídica.

El Habeas Data es una garantía procesal constitucional que protege el derecho a la intimidad, privacidad e identidad de las personas frente al mal tratamiento que se pueda realizar de los datos personales contenido en archivos, bases o bancos de datos en poder del Estado o de empresas particulares.

Es importante tomar en cuenta la reseña que realiza el Autor Pablo Palazzi respecto a lo que opinan diversos sobre el objeto de protección del Habeas Data, ya que establece que en nuestro derecho un sector de la doctrina lo ha asociado a la intimidad. Así Bidart Campos relacionó la indefensión de la persona frente al mal uso de sus datos y a la publicidad de los mismos con el derecho constitucional de la privacidad. Bergel lo ha caracterizado como un derecho humano de la tercera generación que surge frente a la necesidad de una protección adecuada de la privacidad en el desmedido avance de las tecnologías de la información. Ekmekdjian lo califica como una garantía al derecho a la intimidad.

Puede observarse que el Habeas Data tiene doble consideración, ya que es tratado como un derecho constitucional de las personas que se encuentra enraizado en el derecho a la intimidad; y en otras se atienda a su función como garantía o proceso constitucional, que se origina por su reconocimiento en la Constitución. La calidad del Habeas Data como proceso constitucional puede ser discutida cuando su origen no es

la Carta Magna. En Latinoamérica la mayoría de países establecen que el Habeas Data es una garantía procesal, diferenciándose de Europa, que la regula paralelamente con la protección sobre los datos personales, tomando como tutela fundamental el derecho de intimidad y Estados Unidos de América la regula como acciones individuales que deben encontrarse reguladas por una ley específica que defiende la privacidad e intimidad de los hogares y las personas. Por lo que se observa que el Habeas Data puede encontrarse regulada en la Constitución, en una ley procesal o reglamentada por una ley específica.

El autor Badeni sostiene que su propósito es evitar que mediante el uso de la informática se pueda lesionar el honor o la intimidad de las personas y particularmente el segundo. Sagues lo define como una subespecie de amparo destinada a preservar los valores constitucionales de verdad e igualdad.

Para Altmark y Molina Quiroga, el Habeas Data surge por la irrupción de la informática en la sociedad, como un replanteo del derecho a la intimidad, en atención al riesgo que para la persona implica la estructuración de grandes bancos de datos de carácter personal, y particularmente la potencialidad de entrecruzamiento de la información contenida en los mismo.

Existe otro sector de la doctrina que prefirió relacionarlo con el derecho a la identidad. Así, Julio Rivera señala que uno de los aspectos protegidos por el Habeas Data es el derecho a la identidad personal. El citado autor explica que este derecho procede de la doctrina italiana y tiende a amparar el patrimonio cultural, político, ideológico, religioso y social de la persona. Agrega que en la utilización de la informática, y en particular en

cuanto se trata de la recolección de información nominativa en bancos de datos, la cuestión puede exceder el derecho a la intimidad e ingresar en el ámbito de este derecho a la identidad personal.

Para Puccinelli se protegen en forma preferente la intimidad y el honor con especial amplitud, extendiéndose el primero a la intimidad familiar y el segundo a la reputación, que hace a la consideración que sobre la persona puedan tener los terceros. Para Gustavino se trata en última instancia de proteger el derecho a la identidad personal. Cifuentes establece "que en las intromisiones por medio de la informática se halla en juego el derecho fundamental a la identidad personal que es la personalidad cultural".[24]

Se observa que el Habeas Data no es un simple medio de acceso a la información sino que implica el derecho positivo de la persona de controlar los datos e informaciones que otros tienen sobre ella.

3.3. Características.

Como principales características de la garantía procesal constitucional del Habeas Data enumeramos las siguientes:

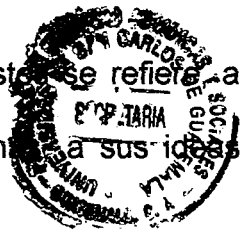
a) Protege la libertad de las personas cuando se ve amenazada o vulnerada como consecuencia de los datos recogidos y utilizados.

b) Protege el derecho al acceso a la información pública.

c) Es una respuesta que surge como consecuencia del exceso del poder informático.

[24] Ibíd.

d) El Habeas Data sólo puede alcanzar a la información sensible, esto se refiere a aquellos datos que hagan referencia a la vida intima de las personas, a sus ideas políticas, culturales, religiosas, gremiales, entre otras.



e) El Habeas Data prevé cinco metas fundamentales, siendo estas las siguientes: acceder a la información, rectificarla, actualizarla, suprimirla y asegurar su confidencialidad.

f) El sujeto afectado tiene el derecho a lograr la supresión del dato obrante en un registro informatizado, cuando el dato sea impertinente para la finalidad perseguida por la base de datos o en el supuesto que en función del transcurso del tiempo no resulte necesario mantener el dato en el registro.

3.4. Objetivos.

El objetivo fundamental del Habeas Data es brindar una protección especial al derecho a la intimidad, el cual debemos considerar como una derivación del derecho a la dignidad. Debemos evitar que se lleve a cabo el uso incorrecto de la información, ya que este puede lesionar el honor, el buen nombre y el ámbito privado de la persona, como consecuencia de la difusión de datos erróneos, incompletos o inexactos.

En la jurisprudencia argentina se han establecido cinco objetivos principales del Habeas Data:

a) Que una persona pueda acceder a la información que sobre ella conste en un registro o banco de datos;

b) Que se actualicen datos atrasados;

c) Que se rectifiquen los datos inexactos;

d) Que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros;

e) Supresión del registro de la llamada información sensible que se refiere a la vida íntima, ideas políticas, religiosas o gremiales.

Para lograr un cumplimiento a los objetivos planteados con anterioridad deben cumplirse los siguientes principios que son básicos para la protección de datos:

a) Principio de justificación social: Sólo permite la recolección de datos con propósitos generales y para usos específicos socialmente aceptables.

b) Principio de limitación de la recolección: Se establece expresamente la prohibición de recolectar información sensible como: raza, religión, salud, costumbres sexuales, opiniones políticas, uso de estupefacientes, entre otros.

c) Principio de calidad o fidelidad de la información: La información acumulada debe ser cierta a fin de que no produzca una imagen equivocada o falsa de la persona.

d) Principio de especificación del propósito o la finalidad: La finalidad con que se recolectan los datos debe ser previamente declarado, no pudiendo con posterioridad hacer uso de ellos para fines distintos a los que se señaló para su recolección.

e) Principio de confidencialidad: Sólo por mandato judicial o por consentimiento del propio sujeto de la información, los terceros pueden acceder a los datos almacenados.

f) Principio de salvaguarda de seguridad: El responsable de los archivos y registros tiene la obligación de adoptar todas las seguridades que sean necesarias para impedir que se pierda, se destruya o haya acceso a la información almacenada.

g) Principio de la política de apertura: La existencia, fines, usos y métodos de operación de los registros de datos personales deben ser de conocimiento público.

h) Principio de limitación en el tiempo: Los datos deben ser cancelados una vez alcanzada la finalidad por la cual fueron recolectados, salvo casos excepcionales.

i) Principio de control: La legislación debe prever un organismo de control responsable del cumplimiento de los principios enunciados.

j) Principio de participación individual: Toda persona tiene derecho a acceder a los registros de datos donde se halle almacenada información sobre su vida personal o familiar.

3.5. Objeto

El Habeas Data regula dos pretensiones sucesivas y secuenciales: El derecho de acceso a la información y el derecho de conocimiento y ejecución.

El derecho de acceso a la información está entendido como "aquél que permite a los afectados averiguar el contenido de la información que a ellos se refiere cuando ésta registrada en un registro o banco de datos, sea manual o automatizado".[25]

[25] Ekmekdjian, Miguel Ángel. **Ob. Cit.** Pág. 67.

Este derecho de acceso a la información requiere que se trate de diversas formas que son las siguientes:

a) datos personales de una persona;

b) que esos datos consten en registro público o privados;

c) que estos registros estén destinados a dar información de los datos del solicitante; y

d) en su caso se informe la finalidad de dichos registros.

Mediante la segunda pretensión del Habeas Data, que se refiere al derecho de conocimiento y ejecución se tiende a exigir la:

a) Actualización, mediante el cual se busca que los datos que hayan quedado desactualizados se actualicen.

b) Rectificación, con el cual se pretende que se corrija las informaciones falsas, erróneas, incompletas o inexactas que se tienen en los bancos de datos.

c) Confidencialidad, en este campo, el sujeto en cuestión exige que una información, por él proporcionada, habiendo sido legalmente requerida, se mantenga en reserva para terceras personas ajenas al asunto.

d) Exclusión, con la finalidad que se supriman los datos que no corresponden a la realidad o que afectan los derechos de intimidad o privacidad de las personas.

3.6. Tipos de Habeas Data

Siguiendo la clasificación realizada por el autor Nestor Pedro [illegible][26], que ha realizado un análisis de las diferentes constituciones americanas, por lo que clasificaremos al Habeas Data en los siguientes tipos:

a) Habeas Data informativo: Aquel que procura lograr el acceso al banco o base de datos a fin de indagar acerca de la información registrada, y que se puede agotar en tal operación. Este tipo de Habeas Data se subdivide en tres subtipos: el exhibitorio, el finalista y el autoral.

a.1) Exhibitorio: Se ejercita con la finalidad que el titular de los datos, pueda tener conocimiento integral acerca de los datos que se almacena en determinado registro , de manera que por este medio la persona tiene derecho a controlar que datos acerca de ella están contenidos o incorporados a un registro o base de datos. Su fin es conocer que se registró.

a.2) Finalista: Nos permite saber con que finalidad nuestro datos se encuentran archivados en determinada base y para que entidad o que persona o personas se registran nuestros datos, en tal supuesto la persona titular de los datos puede accionar contra el responsable de la base de datos a fin de exigirle una respuesta del motivo por el que en la base de datos de una entidad determinada se ha registrado información relativa a mi persona. Su fin es conocer el para qué y para quién se realizó el registro.

---

[26] Citado por Oscar Raúl Puccinelli en **El Habeas Data en el constitucionalismo indoiberoamericano finisecular en el Amparo Constitucional. Perspectivas y modalidades.** Pág. 210 y siguientes.

a.3) Autoral: Sirve para saber quien fue el agente que actuó como autor o la fuente de la que provino la captación de los datos insertados o contenidos en el registro, en tal sentido se persigue establecer la fuente u origen, es decir quien es la persona que recopiló, captó, o acopió la información que ingresó al registro. Su fin es conocer quién obtuvo los datos que obran en el registro.

b) Habeas Data aditivo: Mediante este tipo de Habeas Data el interesado reclama ante el responsable del fichero, por alguna omisión , de manera que su pretensión tiene por finalidad el que se agregue otros datos adicionales a los que ya figuran en el registro respectivo. Este tipo de Habeas Data se subdivide en dos subtipos que son: actualizador e inclusorio.

b.1) Actualizador: Se utiliza cuando se pretende actualizar datos vetustos.

b.2) Inclusorio: Se utiliza para incluir datos en el registro a quién fue omitido.

c) Habeas Data rectificador o correctivo: Su objetivo es corregir o sanear informaciones falsas, aunque también podría abarcar a las inexactas o imprecisas. Respecto a los cuales es factible solicitar determinadas precisiones terminológicas.

d) Habeas Data reservador o confidencial: Pretende asegurar que un dato legítimamente registrado, sea proporcionado sólo a quienes se hallen legalmente autorizados para ello y en las circunstancias que ello corresponde. Su función es mantener la privacidad, el secreto y la reserva de nuestros datos.

e) Habeas Data exclusorio o cancelatorio: Tiene por misión eliminar la información del registro en el cual se encuentre almacenada, cuando por algún motivo no se debe tener

registrada. Entonces podrá emplearse con la finalidad de erradicar del registro alguna información que se considere lesiva al derecho a la intimidad, por que probablemente se trate de un dato sensible, o secreto.

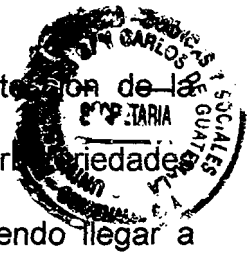
3.7. Relación con la Informática

Los avances tecnológicos han producido un verdadero cambio en la sociedad, ya que se establecen nuevas tecnologías en el campo de la comunicación, que permiten la transmisión de información de un país a otro inmediatamente, por lo que se observa que en este sentido las fronteras entre los países han desaparecido. Como es natural las personas ingresan sus datos a una diversidad de registros en el transcurso de su vida, como por ejemplo podemos encontrar que nuestros nombres, apellidos, estado civil, residencia o domicilio se encuentra inscrito en el Registro Nacional de las Personas, a raíz de la existencia de esta inscripción se emite el Documento Personal de Identificación, que viene a modificar la cédula de vecindad, se observa que este cambio surge a raíz de la automatización y digitalización de nuestros datos que hace muchos años eran impensables.

En el ciberespacio se transmite una serie de información que en estos momentos este proceso es incontrolable, ya que la producción, acceso, distribución y acumulación de datos ha dejado a las personas desprotegidas, por lo que el legislador se ha visto en la necesidad de regular estos hechos para brindar seguridad jurídica.

El poder informático viene a poner en peligro la finalidad del Habeas Data que es proteger la información de las personas y su derecho de intimidad, ya que no existen

los medios de control pertinentes, para que se lleve a cabo una protección de la información que se divulga. Esto puede conllevar abusos, excesos o arbitrariedades con el mal uso que se puede tener de la información obtenida, pudiendo llegar a lesionar los derechos de las personas.



La informática trae muchos beneficios como: la rapidez en el archivo en la formación de datos, la transmisión instantánea de datos, la simultanea comunicación de muchas personas en un acto, el almacenamiento completo abarcador en un espacio reducido, la posibilidad que tienen las personas de proyectarse en el mundo virtual y la rapidez en la búsqueda y el encuentro de los resultados en una forma muy rápida. Al mismo tiempo existen una serie de peligros que tiene la informática como: la recopilación de datos sensibles en instituciones no autorizadas para recabar estos datos, cesión a terceros de la información, vulnerando los fines para los cuales fue recogida, impedir que la persona interesada tome conocimiento de los datos que se manejan sobre ella y mantener eternamente la información. Por lo que el Estado debe proporcionar una adecuada protección a la privacidad de las personas y la protección de sus datos por medio del uso de sistemas automatizados.

La revolución informática, en el caso de recolección, tratamiento y transmisión de datos que se dirigen a la información de índole personal, puede ocasionar graves perjuicios a los registrados, ya que si no existe un control de la información que transita en la red, las consecuencias para las personas que se encuentran en las bases o bancos de datos pueden ser negativas, debido a que terceras personas malintencionadas pueden

tener acceso a sus datos y descubrir los aspectos más íntimos de las personas que se encuentran registradas.

Actualmente se vislumbran dos corrientes que relacionan el Habeas Data con la informática, la primera que trata de regular los avances informáticos que surgen en relación a los derechos personales, cuya meta es limitar la actividad de los operadores de las bases de datos en el tratamiento de datos personales; y la otra corriente, que busca la eliminación de los límites abusivos que se han impuesto, cuya finalidad es permitir el libre acceso y tratamiento a los datos vacantes.

CAPÍTULO IV

4. El delito informático

4.1. Antecedentes

El delito es una parte fundamental del derecho penal, por lo que para comprender sus alcances, debemos realizar un análisis de los aspectos más importantes de esta rama. El derecho penal es una rama del derecho que tiene su origen desde los inicios de la humanidad, debido a que surge con base a las relaciones sociales que existen entre las personas, por lo que estas ideas han tenido que evolucionar paralelamente con el devenir histórico que ha tenido la sociedad. Las relaciones entre las personas se manifiestan por medio de una acción u omisión, que pueden ser aceptadas socialmente y permitidas por el Estado o que al ser dañosas a los derechos e intereses de las personas, son reprimidas por el Estado por medio del derecho penal como *ultima ratio*.

La aplicación del derecho penal se ha visto influenciada por un conjunto de ideas de determinada época histórica, por lo que vamos presentar las diversas etapas que el Derecho penal ha tenido a lo largo de la historia.

a. Época de la venganza privada: En esta etapa surgen las guerras privadas entre los particulares, se practicaba el ejercicio de la justicia sin limites, utilizando como base la Ley del Talión por lo que se daba una venganza de igual magnitud la mal sufrido y surge la composición, que era una limitación para la aplicación de esta ley, remediando el mal causado por cierta cantidad económica que se le entregaba a la familia del ofendido, para que no se pudiera llevar a cabo la venganza.

b. Época de la venganza divina: Dentro de esta etapa se sustituye la voluntad del vengador por la voluntad divina, protegiéndose los intereses colectivos de las personas, por medio de la justicia penal que era ejercida en nombre de Dios. La iglesia tiene un papel preponderante dentro de está época, debido que los sacerdotes eran los encargados de administrar la justicia y las penas se imponían con la finalidad que el delincuente expiara su culpa y la divinidad deponga su cólera.

c. Época de la venganza pública: Esta época se ve caracterizada por la aplicación de la venganza por medio del poder público representado por el Estado, en nombre de la colectividad cuyos bienes jurídicos fueron dañados. Las penas dentro de esta etapa eran inhumanas y desproporcionadas, teniendo como finalidad ser un tormento para los delincuentes, pudiendo los jueces aplicar penas aunque no estuvieran previstas en la ley.

d. Periodo Humanitario: Inicia esta época con el Iluminismo, siendo su precursor Cesar Bonnesana "Marques de Becaria" con la publicación de su famoso libro "De los delitos y de las penas"[27]. Se buscaba impedir que el reo causare nuevos daños, pero se imponían penas más proporcionales que tenían una duración prolongada, pero eran menos dolorosas, por lo que la pena era más justa y útil. En esta etapa surgen los principios del derecho penal.

---

[27] De Mata Vela, José Francisco y De León Velasco Héctor Aníbal. **Curso de derecho penal guatemalteco.** Pág. 19

e. Etapa científica: En esta época el derecho se considera una ciencia y subsiste hasta la crisis del Derecho Penal Clásico dirigida por Francisco Carrara, que consideraba que el derecho penal es una disciplina única, general e independiente que estudiaba la pena y el delito desde el punto de vista jurídico, utilizando un método lógico y abstracto. Surge también la Escuela Positivista con Enrico Ferri, que consideraba al derecho penal como una rama de la sociología criminal, en esta escuela se estudiaban los factores individuales, antropológicos, físicos y sociales de la delincuencia. Un aspecto muy importante es que se deja de considerar el delito como un ente jurídico, ya que es una manifestación de la personalidad del delincuente, y la pena es un medio de corrección social.

f. Época moderna: Se da la codificación del derecho penal, estableciendo que es una disciplina que contiene doctrinas que son importantes para su estudio. Los temas fundamentales de estudia son el delito, el delincuente, la pena y las medidas de seguridad. En este periodo se origina la acción pública.

Con esta reseña de la evolución del derecho penal observamos que dependiendo de la época, surgieron diferentes ideas sobre el delito y la pena. Con el transcurso del tiempo y los cambios que se originan en el seno de la sociedad, es necesario que aumente la regulación del derecho penal, debido a que el devenir histórico de la sociedad hace necesario la tipificación de nuevos delitos.

Con el avance de la tecnología y la era de la información, los delincuentes han encontrado nuevas formas de delinquir, ante esta situación el Estado se ha quedado rezagado, originando lagunas legales, ya que dentro del derecho penal se prohíbe el uso de la analogía para crear figuras delictivas y aplicar sanciones. En la actualidad la utilización de la tecnología es indispensable para la vida diaria, ya que esta nos brinda muchos beneficios, pero al mismo tiempo existen personas inescrupulosas, que utilizan estos medios para realizar conductas delictivas con el fin perjudicar a los usuarios. Por lo que considero necesario que se plasmen dentro de la ley la comisión de los delitos que se originan del derecho informático.

4.2. El Delito

Desde el inicio de la civilización surge el delito, que es una figura del derecho penal, que tiene como finalidad la penalización de las infracciones que se establecen en las leyes penales, por lo que es muy importante que desarrollemos todos los aspectos relevantes del delito, para poder comprender los elementos que lo componen.

4.2.1. Concepto

En Roma se juzga por primera vez una conducta antijurídica, utilizando las acepciones terminológicas de *Noxa – Noxia* que significaba daño, también se conocía con los términos *flagitum, scelus, facinus, crimen o delictum.* La locución *crimen* se refería a las infracciones de mayor gravedad y pena y *delictum* para infracciones menores. Actualmente se utilizan los términos de delito, crimen, infracción penal, conducta delictiva, hecho antijurídico y contravención.

Durante el siglo XIX y a inicios del siglo XX, se recogió en los códigos la definición del delito de la siguiente manera: Delito es la infracción voluntaria de la ley penal.

Los romanos calificaban el delito como un hecho antijurídico y doloso, en cambio para el derecho común el delito es culpa, crimen o lesión a la legalidad y, por ello sancionable.

El Licenciado Wilfredo Valenzuela Oliva[28] desarrolla una serie de definiciones, destacándose las siguientes:

Maggiore acota que el delito se puede definir en sentido formal, jurídico-dogmático, o en sentido real.

- **Sentido formal:** el delito es toda acción legalmente punible.

- **Sentido Dogmático:** delito es toda acción o conducta típica, antijurídica, culpable y punible.

- **Sentido real:** delito es toda acción que ofende el orden ético-jurídico y por esto merece grave sanción que es la pena.

Civoli, expone que el delito es punible, debido a que es un hecho injusto; pero no es injusto por ser punible, opina que hay que atenerse a la historia y llegar a la abstracción de la razón, ya que para la historia, el delito ha sido la acción que la ética de un pueblo ha estimado punible.

[28] Valenzuela Oliva, Wilfredo. **Derecho penal, Parte General – Delito y Estado.** Pág. 34

La definición del delito se ha expuesto en proposiciones principales como: filosóficas, sociológicos, penalistas, procesales y jurídicas o técnicas.

• **Las posiciones filosóficas**: pretendieron universalizar lo que es el delito, consideraron que lo delictuoso en cualquier latitud es el delito natural. La consideraban una acción contraria a ala moral y a la justicia.

• **Las teorías sociológicas:** con base a lo expuesto por Ferri, quién configuró el delito como acto que de manera individual y antisocial hace cambiar las condiciones de existencia y vulnera la moralidad de una comunidad en un momento dado.

• **La posición de los penalistas puros:** expone Beling que el "delito es una acción típica, antijurídica, culpable, reprimida con sanción penal adecuada a la culpabilidad y que llena las condiciones de punibilidad." Para Carrara el "delito es una infracción a la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso." El jurista Von Liszt, dice que el delito es "un acto culpable, contrario al derecho y sancionado con una pena."[29]

• **Los procesalistas:** encabezados por Canelluti que define que un acto delictivo, es un hecho castigado con pena, mediante el proceso.

• **Posición Jurídica o Técnica:** Para el autor Franz Von Liszt el delito se define como "acción antijurídica y culpable castigada con una pena".[30]

---

[29] **Ibíd.** Pág. 35

[30] De Mata Vela, José Francisco. **Ob. Cit.** Pág. 133.

Jiménez de Asúa, expone: "el delito como acto típico, antijurídico, culpable, sancionado por una pena y conforme las condiciones objetivas de punibilidad."[31]

Los juristas alemanes del siglo XX, proclamaron la poca difundida concepción unitaria del delito, compuesta de una fuerza física, que es el elemento objetivo, y una fuerza moral, el elemento subjetivo.

Para concluir podemos definir al delito como toda acción u omisión típica, que es contraria al derecho lo que la hace antijurídica, que es culpable, sancionada con una pena adecuada y suficiente a las condiciones objetivas de la penalidad, que puede tener elementos que modifiquen o extingan la responsabilidad penal. La regulación del delito, se basa en el principio "*nullum crimen sine lege*", ya que los delitos deben encontrarse codificados en la ley penal.

4.2.2. Teoría del delito

La teoría del delito es una parte muy importante dentro del derecho penal, pues realiza un estudio de los elementos positivos y negativos de la estructura del delito, incluyendo determinar que conducta es constitutiva de un delito y la responsabilidad penal del delincuente. La teoría del delito puede definirse como: "la parte de la ciencia el derecho penal que se ocupa de explicar qué es el delito en general y cuáles son sus características"[32].

---

[31] Jiménez de Asuá, Luis. **Tratado de derecho penal.** Pág. 23

[32] González Cauhapé-Cazaux, Eduardo. **Apuntes de derecho penal guatemalteco.** Pág. 27.

La función primordial de la teoría del delito es generar un sistema de análisis, para poder tomar en consideración en forma lógica y ordenada todos los aspectos del delito. Para determinar si una conducta concreta es delictiva, se deben analizar todos los elementos, para lograr una interpretación de la norma, logrando así que incremente la seguridad jurídica.

Es necesario desintegrar el delito en sus elementos característicos por lo que se habla de una serie de elementos positivos como la acción, tipicidad, antijuridicidad, culpabilidad, imputabilidad, las condiciones objetivas de punibilidad y la punibilidad, que son esenciales para afirmar su existencia y determinar la responsabilidad del sujeto activo. Existen una serie de elementos negativos, que pueden llegar a eliminar la responsabilidad penal del delincuente. Vamos a desarrollar brevemente los elementos positivos de la teoría del delito.

- **La acción**

La acción es el primer elemento de la teoría del delito, debido que debe partirse de una conducta humana. El comportamiento humano es "prejurídico" por cuanto es previo a la norma. Solamente la conducta humana puede traducirse en actos externos y ser calificada como delito, al mismo tiempo que motivar una reacción penal. Debemos aclarar que los actos deben ser realizados por un ser humano, debiendo excluir los actos cometidos por animales y los fenómenos causales, que pueden ser fenómenos de la naturaleza.

La acción se define como "una manifestación de la conducta humana consciente (voluntaria) o inconsciente (involuntaria) algunas veces; positiva (activa) o negativa (pasiva) que causa una modificación en el mundo exterior (mediante un movimiento corporal o mediante una omisión y que está prevista en la ley".[33]

La acción es estudiada por dos teorías: la teoría causal que estudia las causas que originaron la acción; y la teoría finalista que tiene como objeto determinar la voluntad o finalidad del sujeto.

➢ **La tipicidad**

La tipicidad es el elemento positivo y conceptual del delito, este razonamiento se basa en el razonamiento del acto, no de la acción. La tipicidad se refiere a la adecuación de la conducta concreta a un tipo penal específico. El autor Jorge Alfonso Palacios la define como: "La abstracta descripción que el legislador hace de una conducta humana reprochable y punible"[34]

En la doctrina se le han asignado tres funciones a la tipicidad como lo establece De Mata Vela[35] siendo estas las siguientes:

a) Función fundamentadora: En virtud que constituye en sí un presupuesto de ilegalidad.

---

[33] De Mata Vela, Juan Francisco. **Ob. Cit.** Pág. 143.

[34] Palacios Motta, Jorge Alfonso. **Apuntes de derecho penal - Segunda parte**. Pág. 36.

[35] De Mata Vela, Juan Francisco. **Ob. Cit.** Pág. 159.

b) Función sistematizadora: Debido a que por su medio se tiene la relación formalmente la parte general con la parte especial del derecho penal.

c) Función garantizadora: La tipicidad resulta ser una consecuencia inevitable del principio de legalidad o de reserva, por medio del cual no puede haber crimen, ni pena, si no está previamente establecido en una ley penal que la regule.

Dentro de este elemento es importante que diferenciemos algunos conceptos que se encuentran muy relacionados a la tipicidad:

- **Tipificación:** Se refiere a encuadrar el hecho a la norma, ya que es la adecuación de un hecho a la descripción que del mismo se hace en la ley.

- **Tipo:** Es la descripción de una conducta prohibida en una norma penal, este debe ser claro y comprensible basándose en el principio de legalidad. El tipo básico nos da la conducta prohibida en general y el tipo derivado, nos da una variación del tipo básico.

» **Elementos del tipo**

- **Bien jurídico tutelado:** Es el interés jurídicamente protegido, siendo éste el fundamento de la norma.

- **Sujeto activo:** Es la persona que realiza la acción descrita en el tipo, a quien se sanciona.

- **Sujeto pasivo:** Es el titular del bien jurídico, objeto de la acción o el agraviado.

- **Elemento descriptivo:** Es la acción descrita en la norma.

➢ **La antijuridicidad**

La antijuridicidad surge por Beling, quien le dio vida como un elemento del delito. La antijuridicidad es una estimación sobre lo alcanzado por la actitud dañosa, vulnerando una garantía registrada en el orden jurídico, y en lo penal la conducta lesiva debe corresponder con la descripción o figura punible o inculpación. Según Muñoz Conde por antijuridicidad se entiende: "la contradicción entre la acción realizada y las exigencias del ordenamiento jurídico."[36]

La antijuridicidad es un juicio negativo de valor que recae sobre un comportamiento humano y que indica que ese comportamiento es contrario a las exigencias del ordenamiento jurídico, este concepto es unitario, debido a que es valido para todo el ordenamiento jurídico.

Se deben observar los comportamientos antijurídicos, que son seleccionados por la legislación penal vigente mediante la tipicidad, aquéllos que la misma considera como relevantes dentro de la sociedad. Cuando este supuesto se lleva a cabo, y se determina que esta conducta es penalmente antijurídica debe de determinarse si la misma se enmarca dentro de alguno de los tipos penales regulados dentro de la ley penal, así como también, no debe concurrir ninguna causa de justificación, que exima de responsabilidad penal sujeto activo.

La función de la antijuridicidad para Cuello Calón, presupone un juicio de oposición entre la conducta humana y la norma penal, juicio que solo recae sobre la acción

[36] González. **Ob. Cit.** Pág. 73

realizada, excluyendo toda valoración de índole subjetiva, por lo que podría decirse que su naturaleza funcional es de carácter objetiva; sin embargo penalistas alemanes han sostenido que hay hechos delictivos que presentan un marcado carácter subjetivo dirigida a un fin determinado.[37]

➢ **La culpabilidad**

Con el estudio de la antijuridicidad y la tipicidad determina si la conducta del imputado es contraria a la norma. La culpabilidad puede definirse como "el juicio de reproche de un hecho delictivo por haber realizado la conducta antijurídica."[38]

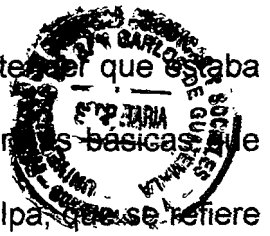
La culpabilidad tiene dos significados: la imputación de un delito y la responsabilidad penal que el agente tiene por su actitud. La culpabilidad se explica conforme la trayectoria que ha tenido de acuerdo a una serie de teorías, tomándose en cuenta que la culpabilidad debe ser inherente a la responsabilidad y a la imputabilidad, por consiguiente la responsabilidad y la imputabilidad son caracteres previos a la culpabilidad. La responsabilidad descansa en que el sujeto debe afrontar las consecuencias de haber lesionado mandatos jurídicos. La imputabilidad depende de la conducta asumida en términos de moral o de ética.

La culpabilidad debe tener como elementos: la imputabilidad o capacidad de la culpabilidad, el conocimiento de la antijuridicidad del hecho cometido y la exigibilidad de un comportamiento distinto, ya que la persona podía elegir entre varias conductas,

[37] De Mata Vela. **Ob. Cit.** Pág. 165

[38] González. **Ob. Cit.** Pág. 91

dependiendo de su grado de madurez psíquica y capacidad para entender que estaba cometiendo un ilícito. La culpabilidad puede manifestarse de dos formas básicas que son el dolo, que se refiere a la voluntad de cometer un delito y la culpa, que se refiere a obrar produciendo un resultado dañoso por impericia, negligencia o imprudencia.



➢ **La punibilidad**

La punibilidad es considerada como una categoría del delito que existe excepcionalmente, por razones de política criminal, para fundamentar o excluir la imposición de una sanción.[39] La doctrina latinoamericana no la considera un elemento del delito, ya que se entiende delito como la acción típica, antijurídica y culpable, no sin ser relevante que se imponga una sanción. De la Barreda Solórzano la define como "Es la conminación de privación o restricción de bienes al autor del delito formulada por el legislador para la prevención general, y determinada cualitativamente por la clase del bien tutelado y cuantitativamente por la magnitud del bien y del ataque a éste."[40]

Existen una serie de circunstancias que excluyen la punibilidad, siendo las condiciones objetivas de penalidad y las excusas absolutorias. Las condiciones objetivas de la penalidad son aquellas circunstancias que sin formar parte de la culpabilidad, son condicionantes en algún delito concreto para la imposición de una pena.

---

[39] **Ibíd.** Pág. 103

[40] De la Barreda Solórzano, Luis. **Justicia Penal y Derecho Humanos.** Pág. 79

4.3. Delito informático

Los delitos informáticos han surgido en los últimos años, debido a los avances tecnológicos, por lo que el Estado debe adaptarse a la realidad que se vive en la sociedad. En la actualidad existen muchas personas que los cometen debido a que la mayoría de estos delitos no se encuentran regulados dentro de nuestro ordenamiento jurídico, por lo que es de vital importancia ampliar la regulación de los delitos informáticos.

4.3.1. Concepto

Con el surgimiento de la era de la información se han dado una serie de cambios en todos los ámbitos de la sociedad, dentro del campo jurídico, los legisladores han tenido que tipificar nuevas conductas delictivas, que nacen a raíz del uso de las nuevas tecnologías, debiendo adaptar la legislación penal a las necesidades de la sociedad actual.

Se utilizan diversos términos en la doctrina para este concepto como ciberdelitos, delitos informáticos, delitos electrónicos, delitos cibernéticos, computer crime, aunque estos se consideran sinónimos, la acepción adecuada para estas acciones ilícitas cometidas dentro la informática, es la de delito informático.

Existe una diversidad de definiciones acerca del delito informático, ya que en este concepto convergen dos ramas del derecho, el derecho penal y el derecho informático. En la actualidad no existe una definición uniforme a nivel internacional

acerca de los delitos informáticos, por lo que vamos a presentar las definiciones que considero más relevantes.

El autor Davara Rodríguez define al delito informático como: "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software."[41]

Para Do. B. Parker los delitos informáticos son: "todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio".[42]

Parker además realiza una tabla por medio de la cual se definen los delitos informáticos de acuerdo a los propósitos que se persiguen:

1. Propósito de investigación de la seguridad: abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia.

2. Propósito de investigación y acusación: delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática.

---

[41] Davara Rodríguez, Miguel Ángel. **Ob. Cit.** Pág. 55

[42] Parker D.B. citado por Romeo Casabona, Carlos. **Poder informático y seguridad jurídica.** Pág. 10.

3. Propósito legal: delito informático es cualquier acto tal como está codificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica.

4. Otros propósitos: abuso informático (sea cual sea su objetivo), es cualquier delito que no puede ser cometido sin computador.

Julio Téllez Valdez establece dos conceptos acerca de los delitos informáticos; el concepto típico establece que son "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y el atípico que son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". [43]

Los autores Marcelo Huerta y Claudio Líbano definen los delitos informáticos como "todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro"[44]

Para finalizar exponemos la definición que realiza un grupo de expertos de la Organización para la Cooperación Económica (OCDE) en París en 1983, por lo que ésta, es la que han adoptado algunos países como Estados Unidos de Norteamérica,

---

[43] Téllez Valdez, Julio. **Derecho informático.** Pág. 81.

[44] Huerta Miranda, Marcelo y Líbano Manzur Claudio. **Los Delitos Informáticos**. Pág. 25

Europa occidental, Australia y Japón, estableciendo los delitos informáticos como "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la trasmisión de datos"[45]

4.3.2. Características

Con base al autor Julio Téllez Valdez[46], determinamos que los delitos informáticos presentan las siguientes características:

a) Son conductas criminales de cuello blanco (White collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.

b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras.

e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del derecho.

---

[45] Palazzi, Pablo Andrés. **Delitos informáticos.** Pág. 37.

[46] Téllez Valdez, Julio. **Ob. Cit.** Pág. 82.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i) En su mayoría son imprudencias y no necesariamente se cometen con intención.

j) Ofrecen facilidades para su comisión a los menores de edad.

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

4.3.3. Bien jurídico tutelado en los delitos informáticos

El Doctor Acuario del Pino[47] nos establece que el bien jurídico protegido en general es la información, pero esta considerada en diferentes formas, ya sea como un valor económico, como uno 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:

- **EL PATRIMONIO**, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a 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 Y PROBATORIO**, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.

[47] Acuario del Pino, Santiago. **Delitos Informáticos: Generalidades.** Pág. 21.

▪ **EL DERECHO DE PROPIEDAD**, en este caso sobre la información sobre los elementos físicos, materiales de un sistema informático, que es afectado por los daños y el llamado terrorismo informático.

Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

4.3.4. Clasificación de los delitos informáticos.

Se han elaborado un conjunto de clasificaciones de los delitos informáticos por parte de los doctrinarios, para tratar de establecer uniformemente como deben de clasificarse estos ilícitos. Es necesario que destaquemos dos de las más utilizadas y predominantes en la doctrina, que han adoptado algunos países, siendo estas la que establece el Doctor Téllez Valdez y la clasificación de la Organización de las Naciones Unidas.

El Doctor Téllez Valdez[48] la clasifica como instrumento o medio y como fin u objetivo.

- **Como instrumento o medio**

Dentro de esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

[48] Téllez Valdez, **Ob. Cit.** Pág. 83

Como método, se refiere a las conductas delictuales en donde los individuos utilizan técnicas informáticas para llegar a un resultado ilícito. Como medio son aquellas conductas en donde para realizar un delito se utiliza una computadora como medio o símbolo. Las siguientes conductas encuadran dentro de esta clasificación:

a) Falsificación de documentos vía computarizada.

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeamiento y simulación de delitos convencionales.

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) Uso no autorizado de programas de cómputo.

h) Introducción de Instrucciones que provocan "interrupciones" en la lógica interna de los programas.

i) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

j) Acceso a áreas informatizadas en forma no autorizada.

- **Como fin u objetivo**

Dentro de esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física. Las siguientes conductas encuadran dentro de esta clasificación:

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios.

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

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje.

El Doctor Acuario del Pino[49] desarrolla la clasificación que realiza la Organización de las Naciones Unidas, estableciendo los diferentes tipos de delitos informáticos que existen en la actualidad de la siguiente manera:

[49] Acuario del Pino. **Ob. Cit.** Págs. 22-28

- **Los fraudes**

a) Los datos falsos o engañosos

Conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

b) Manipulación de programas o los "caballos de troya"

Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado caballo de troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c) La técnica del salami

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

d) Falsificaciones informáticas

Las falsificaciones informáticas pueden tenerse como objeto, cuando se alteran datos de los documentos almacenados en forma computarizada; y como instrumento se utilizan las computadoras también para efectuar falsificaciones de documentos de uso comercial.

e) Manipulación de los datos de salida

Este delito se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

f) Pishing

Este delito se relaciona con la tipificación del delito de robo de identidad, pues este ilícito es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

En estos momentos también existe una nueva modalidad de Pishing que es el llamado Spear Pishing o Pishing segmentado, el cual ataca a grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior.

- **El sabotaje informático**

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

a) Bombas lógicas

Esta es una especie de bomba de tiempo que debe producir daños posteriormente. La comisión de este ilícito exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente.

b) Gusanos

Se fabrican de forma análoga al virus, con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus.

c) Virus informáticos

Son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a éstos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del caballo de troya.

d) Malware

El malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos, de los gusanos y las debilidades de los sistemas, desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos.

f) Ciberterrorismo

Conocido como terrorismo informático, este ilícito es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de sabotaje, sin que éste pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

g) Ataques de denegación de servicio

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios.

- **El espionaje informático y el robo o hurto de software:**

a) Fuga de datos

Conocida también como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Losa, "la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera."[50] La forma más sencilla de proteger la información confidencial es la criptografía

b) Reproducción no autorizada de programas informáticos de protección legal.

Este ilícito puede entrañar una pérdida económica sustancial para los propietarios legítimos. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, considero, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo

[50] Camacho Losa, Luis. **El Delito Informático.** Pág. 253

lugar que la protección al software es uno de los contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

- **El robo de servicios:**

a) Hurto del tiempo del computador

Este delito consiste en el hurto de el tiempo de uso de las computadoras, se da con el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso del Internet, pero sucede que el usuario de ese servicio da esa clave a otra persona que no esta autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

b) Apropiación de informaciones residuales

Este ilícito se refiere al aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

c) Parasitismo informático y suplantación de personalidad

Estas figuras se concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la suplantación

de personas para cometer otro delito informático. Para ello se prevalen de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización o empresa determinada.

- **El acceso no autorizado a servicios informáticos:**

a) Las puertas falsas

Consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

b) La llave maestra

Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador. Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación

c) Pinchado de líneas

Se origina este ilícito cuando se interfieren las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

4.3.5. Sujetos que participan en el delito informático

Deben establecerse de forma específica los sujetos que participan en la comisión de estos ilícitos, por lo que debe determinarse la responsabilidad penal de los autores y los cómplices. Vamos a establecer las características de los delincuentes informáticos (sujeto activo), como del sujeto sobre el que recae el ilícito penal (sujeto pasivo).

➢ **Sujeto activo**

El sujeto activo de un delito informático es la persona que realiza la prohibición establecida por la ley. Se debe tomar en cuenta como delincuentes informáticos no sólo a sujetos con conocimientos especiales, que laboren o no dentro de la empresa afectada, sino a personas normales, sin mayores conocimientos en informática que pueden cometer conductas nocivas a sistemas informáticos desde sus hogares. La red está siendo invadida por nuevos tipos de delincuentes, que valiéndose de las características de esta, como el anonimato por ejemplo, operan de un modo desfavorable de la persecución de los individuos que realizan estas conductas. Así, una persona puede actuar con características distintas a las que originalmente posee, pudiendo alterar desde sus nombres hasta rasgos de su personalidad.

Los sujetos que cometen este tipo de ilícitos, son aquellas que poseen ciertas características, pero al mismo tiempo no presentan el denominador común de los delincuentes, pues los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en

el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Por su grado de participación en el delito pueden ser autores o cómplices, como se encuentra regulado en el Código Penal.

Los autores Marcelo Huerta y Claudio Líbano dicen que "en lo relativo a tratarse de "Ocupacional Crimes", es cierto que muchos de los delitos se cometen desde dentro del sistema por personas que habitualmente lo operan y que tienen autorizado los accesos (Insiders). Sin embargo, las tendencias modernas apuntan hacia el campo de la teleinformática a través del mal uso del ciberespacio y las supercarreteras de la información o redes de telecomunicaciones. Es decir, cada día gana más terreno el delito informático a distancia. (Outsiders)."[51]

Las principales características que presentan los sujetos activos de esta conducta delictiva, son establecidas por De Sola Quintero[52], siendo estas las siguientes:

a) En general, son personas que no poseen antecedentes delictivos.

b) La mayoría de sexo masculino.

c) Actúan en forma individual.

d) Poseen una inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos; actitud casi deportiva en vulnerar la seguridad de los sistemas,

[51] Huerta Miranda. **Ob. Cit.** Pág. 31

[52] De Sola Quintero, René. "**Delitos informáticos".** Pág. 10.

características que suelen ser comunes en aquellas personas que generalmente se las difunde con la denominación "hackers".

e) Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en sí mismo.

f) También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.

g) En el caso de los "hackers", realizan sus actividades como una especie de deporte de aventura donde el desafío está allí y hay que vencerlo. Aprovechan la falta de rigor de las medidas de seguridad para obtener acceso o poder descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sitio. Eso suele suceder con frecuencia en los sistemas en que los usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sitio.

h) Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras y motivadas.

i) Con respecto a los que se dedican a estafar, nos encontramos ante especialistas. Algunos estudiosos de la materia lo han catalogado como "delitos de cuello blanco", debido a que el sujeto activo que los comete es poseedor de cierto status socio-económico.

Dentro de los diferentes tipos de sujetos activos de los delitos informáticos podemos citar los siguientes:

- **Hackers**

Es la persona que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras, utilizando sus conocimientos en materia informática para poder ingresar sin autorización a los sistemas informáticos.

- **Crackers**

Es aquella persona que haciendo gala de grandes conocimientos sobre la computación y con un propósito de luchar contra lo que está prohibido, empieza a investigar la forma de bloquear las protecciones hasta lograr su objetivo. Este sujeto ingresa a los sistemas informáticos con la finalidad de causar daño o apoderarse de los recursos del sistema o de la información contenida.

- **Phreacker**

Es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general con los celulares. Estos sujetos construyen equipos electrónicos que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

- **Pirata informático**

Es la persona que viola los derechos de autor de los programas de ordenador, en especial aquellos que reproducen sin la debida autorización sin la debida autorización las distintas clases de programas de computación, ya sea que tengan o no fines de lucro.

➢ **Sujeto pasivo**

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. Debemos distinguir que sujeto pasivo ó 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 las víctimas pueden ser individuos, instituciones privadas, los gobiernos y sus instituciones públicas autónomas y descentralizadas, que utilizan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, debido a que mediante él, podemos 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.

Es muy difícil llegar a 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, a esta situación debemos sumarle la falta de leyes o que

las leyes existentes no regulan todos los delitos informáticos, que protegían a las víctimas de estos ilícitos, al mismo tiempo existe una falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, por lo que la mayoría de victimas prefiere no denunciarlas, quedando estas conductas impunes.

4.3.6. Formas de control del delito informático

El Doctor Téllez Valdez[53] establece que este tipo de ilícitos requieren de un necesario control, y éste, al no encontrar en la actualidad un adecuado entorno jurídico que regule todos los delitos informáticos, ha tenido que manifestarse en su función preventiva, a través de diversas formas de carácter administrativo, normativo y técnico, dentro de las cuales destacamos las siguientes:

- Elaboración de un examen psicométrico previo al ingreso al área de sistemas de la empresa.
- Introducción de cláusulas especiales en los contratos de trabajo con el personal informático que por el tipo de labores a realizar así lo requiera.
- Establecimiento de un código ético de carácter interno en las empresas.
- Adoptar estrictas medidas en el acceso y control de las áreas informáticas de trabajo.
- Capacitación adecuada del personal informático, a efecto de evitar actitudes negligentes.
- Identificación y, en su caso, segregación del personal informático descontento.
- Rotación en el uso de claves de acceso al sistema.

[53] Téllez Valdez. **Ob. Cit.** Pág. 84.

Por otra parte, existe el control correctivo, éste podrá darse en la medida que se introduzcan la totalidad de los delitos informáticos en los códigos penales sustantivos, ya que debe de tipificarse claramente cada ilícito, para no violar el principio de legalidad que prohíbe la analogía. La existencia de una adecuada legislación al respecto trae consigo efectos no sólo correctivos sino eventualmente preventivos, para que se reduzcan en buen número este tipo de acciones que causan tanto daño a los intereses individuales y colectivos.

4.4. Regulación de los delitos informáticos en el derecho penal guatemalteco vigente

La Constitución Política de la República de Guatemala incorporó la protección de datos personales informatizados. Se reconoce el derecho de autor y el derecho de inventor; los titulares de los mismos gozarán de la propiedad exclusiva de su obra o invento, de conformidad con la ley y los tratados internacionales.

Asimismo recoge el derecho de acceso, unido a los de rectificación o cancelación en el Artículo 31. En el año 1954 el Congreso de Guatemala aprobó la Ley sobre el derecho de autor en obras literarias, científicas y artísticas por medio del Decreto 1037. Posteriormente, en el año 1995 y 1996 el Congreso de la República introdujo reformas al Código Penal destinadas a fortalecer la protección de los derechos de autor. El Decreto 33-96 del Congreso de la República incluye expresamente la protección al software y a los registros informáticos entre las obras protegidas y establece sanciones para los casos de violación de los derechos de autor correspondientes a los fabricantes del software.

El legislador en el Libro Segundo, Titulo VI de los Delitos contra el Patrimonio dentro del capítulo VII que regula los delitos contra el derecho de autor, la propiedad industrial y los delitos informáticos por medio del Decreto 33-96 del Congreso se adicionan específicamente algunos delitos informáticos que son de mucha importancia en la actualidad entre los que podemos mencionar los siguientes: La alteración de programas; Reproducción de instrucciones o programas de computación; Registros prohibidos; Manipulación de información; Uso de información; y los Programas destructivos.

Estos delitos incluyen solamente algunas de las conductas delictivas que pueden realizar por medios informáticos, por lo que creemos que es necesario que el legislador, tome en cuenta la existencia de nuevos delitos informáticos que aquejan a la sociedad.

CAPÍTULO V

5. El Delito Informático de Robo de Identidad

5.1. Generalidades

El delito de Robo de identidad se relaciona con la suplantación de identidad siendo una antigua práctica delictiva, que en la era de la globalización, de la nueva revolución tecnológica y del comercio electrónico ha adquirido nuevos contornos y dimensiones inimaginables desde hace pocas décadas.

La suplantación de identidad adopta muchas formas en Internet. En ocasiones, los infractores se apoyan en vulnerabilidades tecnológicas para poder hacerse con el control de cuentas de correo electrónico o perfiles de mensajería instantánea; otras veces hacen uso de técnicas de ingeniería social para engañar a los propios usuarios y convertirles en víctimas del Phising o estafas similares; y aumentan los casos en los que son los propios usuarios quienes crean cuentas ficticias o falsificadas con la intención de actuar bajo el anonimato de un nombre falso, dañar los intereses de terceros o cualquier otro motivo que se nos pueda ocurrir. En cualquier caso, la suplantación de identidad supone hacerse pasar por otra persona física o jurídica. La suplantación de identidad llegó hace ya tiempo al mundo de los blogs y las redes sociales arrasando con perfiles de empresas y particulares, y la realidad es que sigue presente, manteniéndose un cierto clima de inseguridad en la red. En el caso de muchos usuarios de Internet, la red es un espacio seguro de comunicación y negocio gracias a que han adoptado medidas tecnológicas y de sentido común para evitar ser objeto de ataques o relacionarse con perfiles falsos; sin embargo, el público en general

está aún muy lejos de haber sido concienciado sobre la naturaleza anónima de Internet y lo que ello supone, para bien y para mal.

Con el crecimiento del comercio electrónico y el uso de los servicios de banca por Internet han aumentado en forma alarmante los fraudes electrónicos, especialmente el robo de identidad. Esta nueva modalidad de fraude, comúnmente se refiere a toda aquella información de un individuo como el nombre, fecha de nacimiento, dirección, número de cédula de vecindad o documento personal de identificación, de tarjeta de crédito y de cuentas bancarias, nombre de usuario y contraseña de sitios web donde se encuentra inscrita la victima, que es obtenida y utilizada sin su consentimiento, y con el propósito de cometer actividades fraudulentas. El robo de identidad normalmente involucra la adopción de la identidad de una persona, mediante la información que el delincuente obtuvo de su víctima. Actualmente, el mayor número de casos de robo de identidad se dan a través del Phising, el cual consiste en el envío de correos spam que contienen links y direcciones web falsas, aparentemente provenientes de algún banco o empresa, donde se solicita el acceso por supuestas modificaciones o actualizaciones a sus bases de datos o sistemas; de esa forma, al darle clic el usuario a esos sitios falsos, los delincuentes obtienen sus datos y contraseñas y pueden rastrear fácilmente sus hábitos de navegación en la red.

El robo de identidad se torna cada día más común, ya que con un mínimo de recursos y conocimientos técnicos, los criminales pueden falsificar sitios web, marcas, logotipos e información de empresas y bancos para desviar fácilmente la atención de sus víctimas. Los delincuentes explotan principalmente tres recursos:

a. El uso y creación de plataformas técnicas basadas en la web;

b. Las técnicas de ingeniería social como vehículos alternativos para engañar y llevar a cabo fraudes;

c. La vulnerabilidad y falta de información de algunos usuarios, sobre todo aquellos que son nuevos o bien, tienen poco tiempo utilizando los sitios de subastas o de servicios financieros.

En la última década alrededor millones de personas, han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta.

Asimismo, los criminales se aprovechan de que la legislación aplicable es bastante escasa, imprecisa y enfocada al mundo analógico, por lo que encontramos casos en los que o bien no existe solución jurídica a un determinado supuesto o ésta es incapaz de atajar, reducir o impedir los hechos, siendo estos las consecuencias de los vacíos legales existentes y de la dificultad que representa a las autoridades ubicar exactamente el lugar físico donde se llevan a cabo las operaciones fraudulentas, así como la persecución hasta su lugar de origen..

No es extraño por ello que el robo de identidad haya entrado en la agenda de las organizaciones internacionales. La Organización para la Cooperación y el Desarrollo Económico, la Unión Europea y Naciones Unidas desde hace aproximadamente un lustro realizan estudios y proyectos tendentes a encontrar una respuesta global a un

tipo de criminalidad que ocasiona notables perjuicios económicos y lesiona intereses tan relevantes como la intimidad informática, siendo además un instrumento para cometer delitos tan graves como la financiación de organizaciones terroristas.

5.2. Concepto

Debido a que dentro de la doctrina el concepto de delito informático de Robo de identidad no ha sido estudiado con la profundidad que le merece, vamos a realizar un concepto tomando como base los conocimientos expuestos anteriormente y el Diccionario de la Real Academia Española, definiendo cada uno de sus componentes, para poder concretar una definición del delito informático de robo de identidad, que nos exponga la totalidad de elementos que lo conforman.

Para iniciar debemos definir al delito informático, considerando que la definición más exacta es la que nos brinda el autor Julio Téllez Valdez establece dos conceptos acerca de los delitos informáticos; el concepto típico establece que son "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y el atípico que son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".[54]

Definimos el concepto robar según el Diccionario de la Real Academia Española como "Tomar para sí lo ajeno, o hurtar de cualquier modo que sea"; y la identidad como el

[54] Téllez Valdez, **Ob. Cit.** pág. 81.

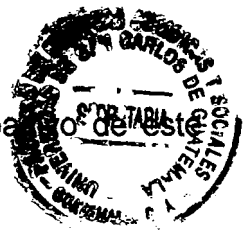
"Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás".[55]

Podemos definir al Robo de identidad como la conducta que se produce cuando alguien usa la información personal sin su permiso para cometer fraude u otros delitos.

El delito informático de Robo de identidad, que consiste en obtener datos personales privados del sujeto pasivo a través de la red, información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Los datos personales que los delincuentes obtienen, los utilizan para su beneficio propio, actuando con el nombre del sujeto pasivo, lo que conlleva un daño patrimonial y moral a la victima de este delito. Este tipo de ilícito se comete habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El Robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las victimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es peor.

Basándonos en los conceptos anteriores vamos a definir al delito informático de Robo de identidad como: La conducta típica, antijurídica, culpable y punible, que surge cuando una persona utiliza la información personal de otra sin su autorización, con el fin de cometer algún fraude u otros delitos, manipulando las computadoras como medio para obtener la información íntima de la persona a través de un engaño hacia la victima, y al mismo tiempo utiliza la computadora para realizar la conducta delictiva a

[55] Real Academia Española, **Diccionario de la Real Academia Española**. Edición Digital.



través de la red, que causa un daño patrimonial y/o moral al sujeto pasivo de este ilícito.

5.3. Métodos de comisión del delito informático de Robo de identidad

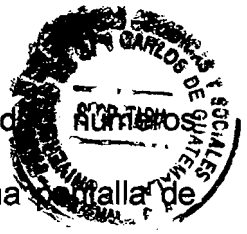
Establecemos que con la popularidad que han alcanzado el correo electrónico y la Web, además del aumento del uso de sistemas de pago electrónico, no es difícil entender porque los delincuentes se dedican a esta actividad. Los ladrones de identidad han adoptado nuevas técnicas, en el mundo virtual podemos ver varios tipos de ataques que se aplican al mundo real como métodos de comisión del delito de robo de identidad:

- **Pirateo informático, acceso no autorizado a sistemas y robo de bases de datos.**

Además de robar el hardware, con frecuencia los delincuentes ponen en peligro los sistemas, desviando la información directamente o con la ayuda de dispositivos de escucha, como rastreadores y escáneres en la red. Los piratas consiguen acceso a una gran cantidad de datos, los descifran (en caso necesario), y los utilizan para lanzar ataques en otro lugar.

- **Phishing**.

Los ciberdelincuentes utilizan sitios Web y de correo electrónico fraudulentos (conocidos como sitios de "réplica") que se asemejan a bancos en línea o a sitios de compras. Estos sitios están diseñados para engañar a los usuarios de forma que



revelen información personal, en especial sus números de tarjeta de crédito, números de cuenta y contraseñas. A continuación se muestra un ejemplo de una pantalla de eBay falsa.

- **Pharming**.

Se trata de una sofisticada forma de Phising que redirecciona la conexión entre la dirección IP y el servidor de destino. Esto puede llevarse a cabo en el servidor DNS (a través de envenenamiento de caché o ingeniería social) o en el equipo local con la ayuda de un troyano que modifica el archivo hosts. El vínculo se altera de manera que cada vez que los usuarios intentan conectarse al sitio real de una organización son redirigidos de forma secreta a un sitio de réplica, sin haber introducido en ningún momento la dirección incorrecta o fraudulenta. El uso de ingeniería social es especialmente retorcido, ya que las propias víctimas terminan realizando acciones que les perjudican movidas por su propia codicia o generosidad. En 2005, el Instituto SANS informó que 1.300 empresas, entre las que se incluyen grandes nombres, habían sufrido algún ataque de envenenamiento de caché.

- **Redireccionadores**.

Se trata de programas malignos que redirigen el tráfico de red de los usuarios a ubicaciones que no tenían intención visitar. El Anti-Phishing Working Group observa un fuerte aumento de los redireccionadores de tráfico, así como de los registradores de teclas pulsadas basados en phishing. Según este grupo, el mayor volumen de tráfico se produce con código maligno que sencillamente modifica la configuración del servidor

DNS o el archivo hosts con objeto de redirigir algunas o todas las búsquedas de DNS a un servidor DNS falso. El servidor fraudulento utiliza respuestas correctas para la mayoría de los dominios. Si embargo, cuando los agresores desean redirigir a la víctima a un sitio fraudulento, sencillamente modifican las respuestas nombre-servidor. Esto resulta especialmente eficaz porque los atacantes pueden redirigir cualquier solicitud del usuario en cualquier momento sin que éste sea consciente de lo que ocurre.

- **Fraude de pago anticipado**.

Un usuario desprevenido recibe un mensaje de correo electrónico que supuestamente procede de un miembro de la familia de un dignatario africano. El remitente explica que tras la muerte del dignatario, se bloqueará en algún lugar una gran cantidad de dinero. Con la ayuda del usuario, y gracias a su apoyo financiero para la transferencia de fondos, el contacto afirma que sería posible liberar el dinero. Supuestamente una sustanciosa recompensa espera a los que acepten el contrato.

- **Registradores de teclas y ladrones de contraseñas**.

Estos términos hacen referencia a programas malignos que consiguen introducirse en los sistemas de sus víctimas. Cada programa obtiene determinadas pulsaciones de teclas y puede captar el nombre del usuario, las contraseñas y otro tipo de información personal o confidencial. A continuación, el malware envía los datos a los agresores, que los utilizan de manera fraudulenta.

5.4. Derecho Comparado

Dentro de la legislación de Norteamérica la primera codificación de la definición de Robo de identidad se incluyó en la Identity Theft and Assumption Deterrence Act de 1998 o ID Theft Act (Ley contra el robo de identidad), que consideraba el Robo de identidad como un delito independiente. Concretamente, modificaba el Código Penal federal de forma que fuera un delito: "...transferir o utilizar con conocimiento de causa, y sin autoridad legal, un medio de identificación de otra persona con la intención de cometer, colaborar o inducir a una actividad ilegal que constituya una infracción de una ley federal o bien un delito grave según cualquier ley local o estatal en vigor".

En el año 2003, la Fair and Accurate Credit Transactions Act o FACTA (Ley de transacciones de crédito justas y precisas), modificó la Fair Credit Reporting Act (Ley de informes comerciales justos) para incluir una definición civil de Robo de identidad: " El término Robo de identidad identifica todo fraude cometido mediante el uso de información identificativa de otra persona, quedando sujeta esta definición a otra ulterior que pudiera establecer la Comisión Federal de Comercio (FTC) mediante normativa".

De conformidad con la Ley de transacciones de crédito justas y precisas, la Comisión Federal del Comercio ha propuesto recientemente una definición de Robo de identidad más específica que describe lo que se entiende por "información identificativa":

a) El término Robo de identidad: designa todo fraude consumado o no consumado mediante el uso de información identificativa de otra persona sin autoridad legal.

b) El término información identificativa: se refiere a cualquier nombre o número que pudieran servir, de manera individual o junto con otra información, para identificar a un individuo concreto, incluidos:

1) El nombre, número de la Seguridad Social, fecha de nacimiento, permiso de conducir o número carné de identidad, ya sea expedido por el Estado o por el Gobierno federal, número de pasaporte o número de identificación fiscal o de empleado.

2) Datos biométricos exclusivos, como la huella dactilar, un registro de la voz, una imagen de la retina o el iris, o cualquier otra representación de un rasgo físico intrínseco.

3) El número de identificación, dirección o código de enrutamiento electrónico exclusivos.

4) Información de identificación de telecomunicaciones o dispositivo de acceso.

La Oficina australiana de estadísticas, a través de la Unidad nacional de estadísticas sobre crímenes y el Centro australiano de crímenes relacionados con las altas tecnologías, completan la definición del término, con los siguientes conceptos relacionados con el robo de identidad.

• **Falsa identidad:**

Puede utilizarse para describir

° La creación de una identidad ficticia

° La alteración de la identidad propia (o manipulación de la identidad)

° El robo o asunción de una identidad existente (robo de identidad), que puede conllevar también la posterior manipulación.

• **Delito contra la identidad:**

Puede utilizarse como término genérico para incluir el fraude de identidad, el robo de identidad a través de la tarjeta de crédito o skimming y los delitos relacionados como la posesión, distribución y fabricación de material, dispositivos, entre otros.

• **Fraude de identidad:**

Se puede utilizar para describir el uso de una identidad falsa con fines lucrativos, para la adquisición ilegal de bienes, servicios u otros beneficios, o bien para eludir obligaciones, y debe incluir los casos de skimming.

• **Robo de identidad:**

Se puede utilizar para describir el robo o la asunción de una identidad existente o una parte significativa de la misma, con o sin el consentimiento de la persona, y con independencia de si ésta está viva o muerta.

En el Reino Unido, el término preferido es *identity fraud* (fraude de identidad). Los países de habla francesa también emplean sus propios términos específicos. Algunos optan por *vol d'identité* (robo de identidad), mientras que otros hablan de *usurpation d'identité* (usurpación de identidad).

5.5. Análisis crítico de importancia de la tipificación del delito informático de Robo de identidad

Con el desarrollo y masificación de las nuevas tecnologías de la información debemos realizar un verdadero análisis de la suficiencia del ordenamiento jurídico guatemalteco actual para regular las nuevas posiciones, los nuevos escenarios, en donde observamos los problemas del uso y abuso de la actividad informática y su repercusión en el territorio guatemalteco. Por esta razón han surgido una serie de acciones delictivas, que en algunos casos son de difícil tipificación en las normas penales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad, regulado en el Artículo número siete del Código Penal, Decreto 17-73 del Congreso de la República.

Por medio del Decreto 33-96 del Congreso de la República, se reformo el Código Penal vigente, modificando el Artículo número doscientos setenta y cuatro e implementando los delitos contra los derechos de autor, la propiedad industrial y algunos delitos informáticos, entre los que podemos citar: la destrucción de registros informáticos, la alteración de programas, la reproducción de instrucciones o programas de computación, los registros prohibidos, la manipulación de información, el uso de información y los programas destructivos. La implementación de estos delitos

informáticos fue un verdadero avance para la legislación guatemalteca en materia penal e informática, ya que establece un antecedente para la tipificación de otros delitos informáticos que surgen a raíz del progreso de la tecnología, como en el presente caso, que se pretende la implementación del delito informático de robo de identidad dentro del ordenamiento jurídico guatemalteco.

Es muy importante que se lleve a cabo la tipificación del delito informático de robo de identidad dentro del ordenamiento jurídico guatemalteco, debido a que este es uno de los ilícitos que ha tenido mayor crecimiento en la red alrededor del mundo. Este delito es una forma de engañar a los usuarios para que revelen información personal o financiera de carácter confidencial, mediante un mensaje de correo electrónico, algún sistema de mensajería instantánea o sitio web fraudulento. Los delincuentes informáticos conocidos como hackers, obtienen por medio de engaños dentro de la Internet los datos personales privados del sujeto pasivo, para que después este individuo pretenda ser o hacerse pasar por el sujeto pasivo y realizar operaciones o acciones en su nombre para cometer fraudes, causando un daño patrimonial y en otras ocasiones también puede darse un daño de carácter moral, ya que se pueden utilizar los datos del sujeto pasivo para cometer algún delito y causar sentimientos en las victimas como la humillación, la ira y la frustración, al no poder realizar ninguna acción contra el delincuente que ha utilizado su información. Cualquier persona que ingrese sus datos confidenciales a la red puede ser victima de este delito y sufrir sus consecuencias.

El delito informático de robo de identidad al no encontrarse regulado dentro del ordenamiento jurídico guatemalteco, basándonos en el principio de legalidad, no pudiéndose aplicar la analogía, es un instrumento para que los delincuentes que lo cometen dentro del territorio guatemalteco no puedan ser procesados penalmente.

Con la implementación del delito informático de robo de identidad, el Estado va brindar más seguridad jurídica a los usuarios de Internet, ya que van a tener la garantía que sus datos privados se encuentran protegidos contra los fraudes. Pretendo con esta exposición científica profundizar en la necesidad de la implementación que debe realizar el legislador guatemalteco del delito informático de robo de identidad, llevando a cabo una determinación correcta de todos los elementos que lo componen y los casos en que este tipo penal puede aplicarse dentro del territorio del Estado de Guatemala.

Con relación a los elementos anteriormente mencionados en la teoría del delito, podemos determinar que el delito informático de Robo de identidad deberá comprender los siguientes elementos:

- **Elemento objetivo:** consiste en la obtención, utilización o transferencia de datos de identificación personal de otra persona física o jurídica. Asimismo la adopción, creación, apropiación o utilización de la identidad de una persona física o jurídica que no le pertenezca.

- **Elemento subjetivo:** consiste en la voluntad de obtener, utilizar o transferir datos de identificación personal de otra persona; como la de adoptar, crear, apropiarse o utilizar

la identidad de otra persona a través de la internet o cualquier medio informático, con la finalidad de causar un daño patrimonial y/o moral a la victima.

- **Sujeto activo:** puede ser cualquier persona que realice esta conducta delictiva.

- **Sujeto pasivo:** es la persona perjudica directamente por la acción delictuosa, siendo la titular de los datos de identificación o de la identificación suplantada.

- **Acción:** consiste en obtener, utilizar o transferir de datos de identificación personal de otra persona física o jurídica. Asimismo adoptar, crear, apropiarse o utilizar de la identidad de una persona física o jurídica que no le pertenezca a través de internet o cualquier sistema informático.

- **Bien jurídico tutelado:** se protege la intimidad, integridad y patrimonio de la persona.

- **Imputabilidad:** se refiere a que esta conducta delictiva se realiza con dolo.

5.6. Tipificación del delito informático de Robo de identidad

Es menester que el legislador realice una reforma del Código Penal, Decreto 17-73 del Congreso de la República, incorporando el delito informático de robo de identidad, dentro del Titulo VI relativo a los delitos contra el patrimonio en el Capítulo VII referente a los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos.

El delito informático de robo de identidad debería adicionarse al Artículo 274 del Código Penal, por lo que propongo que esta conducta delictiva se tipifique de la siguiente manera:

ARTÍCULO 274 "H" – Delito de Robo de identidad. Será sancionado con prisión de uno a cinco años y multa de cinco mil a cincuenta mil quetzales, al que obtuviere, utilizare o transfiriere datos de identificación personal de otra persona física o jurídica por cualquier medio, sin su autorización, con la finalidad de causarle un daño patrimonial y/o moral.

Igual sanción se impondrá a quien adoptare, creare, apropiare o utilizare, a través de internet o cualquier sistema informático, la identidad de una persona física o jurídica que no le pertenezca.

CONCLUSIONES

1. En la actualidad existe una gran variedad de conductas delictivas que se realizan por medios informáticos, que en Guatemala no se encuentran tipificadas como delitos, esto acarrea la existencia de un vacio legal en nuestro ordenamiento jurídico.

2. Todas las personas tienen el derecho a la protección de sus datos personales, asimismo a la protección de sus derechos a la intimidad y a la privacidad, pero estos derechos se han puesto en peligro con el auge de los sistemas informáticos.

3. Por medio de la libertad informática las personas tienen el derecho de hacer uso de todas las posibilidades que nos brinda el sistema informático, pero esto no quiere decir que toda la información que sea de carácter íntimo o privado va estar segura, ya que puede ser manipulada por un tercero, pudiéndose convertir en la comisión de un delito.

4. Del análisis de la realidad guatemalteca e internacional, se concluye que el delito informático de robo de identidad, ha crecido con mucha rapidez en la sociedad, observándose que esta conducta se comete a diario, estableciendo como su forma más leve la que se da en las redes sociales y al ser está más grave puede causar un daño patrimonial y moral a la victima.

5. Al culminar el presente trabajo de investigación, se pudo comprobar la hipótesis planteada, ya que quedó evidenciada la necesidad de llevar a cabo la tipificación del delito de robo de identidad, estableciendo correctamente los elementos que lo

componen, el bien jurídico tutelado y la protección que brinda a la población que diariamente ingresa a la Red datos personales y privados, que deben ser resguardados por el Estado.

RECOMENDACIONES

1. El Congreso de la República debe adaptarse en la actualidad a los avances tecnológicos, con la implementación de nuevas conductas delictivas que se realizan por medios informáticos, siendo éstos los delitos informáticos que no se encuentran regulados dentro del Código Penal, para resguardar la seguridad de la población.

2. El Estado de Guatemala por medio de sus instituciones, debe crear mecanismos eficaces, eficientes y un órgano especializado en resguardar los datos personales y con ellos los derechos a la intimidad y a la privacidad, en todos los ámbitos de su vida incluyendo los datos que se encuentren en la red informática.

3. Debe de realizarse un verdadero control a la libertad informática por un órgano especializado, estableciéndose los límites que implica la existencia de este derecho, para que cuando una conducta sobrepase estos límites, pueda procesarse penalmente al sujeto activo que cometió un delito en detrimento físico y moral de la victima.

4. El Organismo Ejecutivo a través de de la Secretaria Nacional de Ciencia y Tecnología, debe realizar programas informativos a la población guatemalteca, de las formas en que puede llevarse a cabo el delito informático de robo de identidad, para que estas puedan denunciar la comisión de este delito, no importando la gravedad que esté implique.

5. El Congreso de la República de Guatemala debe tipificar el delito informático de robo de identidad, con base a la propuesta establecida en el presente trabajo de investigación, porque es muy importante que no exista un vacio legal en el tema de la protección de los datos personales y privados que la población ingresa a la Red.

BIBLIOGRAFÍA

ABAD YUPANQUI, Samuel. **La Constitución de 1993. Análisis y comentarios**. Lima, Perú: Ed. Comisión Andina de Juristas, 1994.

ACUARIO DEL PINO, Santiago. **Delitos Informáticos: Generalidades.** Ecuador: Ed. PUCE, 2007.

BARRIOS OSORIO, Omar Ricardo. **Derecho e Informática: Aspectos Fundamentales**. 4ª.; Ed. Guatemala: Ed. Ediciones Mayte, 2007.

CABANELLAS, Guillermo. **Diccionario Enciclopédico de Derecho Usual.** Buenos Aires, Argentina: Ed. Heliasta, 1979.

CAMACHO LOSA, **Luis, El Delito Informático**. Madrid, España: Ed. Gráficas Cóndor, 1987.

CASTELLANOS HERNÁNDEZ, Eduardo. **Temas de Derecho Informático.** México: Ed. Orden Jurídico Nacional, 2006.

DAVARA RODRÍGUEZ, Miguel Ángel. **Manual de Derecho Informático**. Madrid, España: Ed. Arrazandi, 1987.

DAVARA, Miguel, **La protección de datos en Europa. Principios, derechos y procedimiento**. Madrid, España: Ed. Grupo Asnef Equifax, 1998.

DE LA BARREDA SOLORZANO, Luis. **Justicia Penal y Derecho Humanos.** México: Ed. Porrúa, 1997.

DE MATA VELA, José Francisco y DE LEÓN VELASCO, Héctor Aníbal. **Curso de Derecho Penal Guatemalteco.** 2a. ed. Guatemala: Ed. Edi-Art, 1989.

DE SOLA QUINTERO, René. **"Delitos Informáticos",** 2002, http://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RdeSola.pdf (22 de agosto de 2010).

EKMEKDJIAN, Miguel Ángel y Caolgero Pizzolo. **Habeas Data. El derecho a la intimidad frente a la revolución informática.** Buenos Aires, Argentina: Ed. De Palma, 1996.

ELÍAS, Miguel S., **Situación legal de los datos de carácter personal frente a las nuevas tecnologías, Capítulo I,** 2001, http://vlex.com/vid/situacion-caracter-personal-frente-107859 (16 de junio de 2010).

FALCÓN, Enrique M, **Habeas Data. Concepto y procedimiento**. Buenos Aires, Argentina: Ed. Abeledo Perrot, 1996.

GONZÁLEZ CAUHAPÉ-CAZAUX, Eduardo. **Apuntes de derecho penal guatemalteco.** Guatemala: Ed. Fundación Myrna Mack, 2003.

HERRERA BRAVO, Rodolfo, **El Derecho en la Sociedad de la Información: Nociones Generales sobre el Derecho de las Tecnologías de la Información y Comunicaciones**, Santiago, Chile: Boletín Hispanoamericano de Informática y Derecho, 2000.

HUERTA MIRANDA, Marcelo y Líbano Manzur Claudio. **Los Delitos Informáticos**. Chile: Ed. Jurídica Cono Sur, 1999.

JIMENEZ DE ASUÁ. Luis. **Tratado de derecho penal**. Editorial Lozada. Buenos Aires, Argentina: Ed. Lozada, 1963.

JORDAN FLÓREZ, Fernando, **La informática jurídica.** Bogotá: Ed. Universidad Piloto de Colombia, 1983.

OSSORIO, Manuel. **Diccionario de Ciencias Jurídicas, Políticas y Sociales.** Buenos Aires, Argentina: Ed. Heliasta, 1984.

PALACIOS MOTTA, Jorge Alfonso. **Apuntes de Derecho Penal (Segunda Parte).** Guatemala: Ed. Serviprensa Centroamericana, 1980.

PALAZZI, Pablo Andrés. **Delitos Informáticos.** Buenos Aires, Argentina: Ed. AD-HOC, 2000.

PALAZZI, Pablo Andrés. **El Habeas Data en el derecho argentino.** En Revista Electrónica de Derecho Informático. Número 4. Argentina, 1998. http://publicaciones. Derecho.org/redi/No._4_-Noviembre_de_1998/palazzzi. (20 de junio de 2010).

PÉREZ LUÑO, Antonio, **Ensayos de Informática Jurídica.** Distrito Federal, México: Ed. Fontamara, 2001.

PUCCINELLI, Oscar Raúl en **El Habeas Data en el constitucionalismo indoiberoamericano finisecular en el Amparo Constitucional. Perspectivas y modalidades.** Buenos Aires, Argentina: Ed. Ediciones de Palma, 1999.

RAMIREZ, William; PONS, Juan Pablo; y VÁSQUEZ, Nadezhda. **Libre acceso a la información, protección de datos y habeas data.** Guatemala: Ed. Fundación Myrna Mack, 2003.

RIASCOS GÓMEZ, Libardo Orlando, **El derecho a la intimidad, la visión lusinformatica y el delito de los datos personales,** España: Ed. Lleida, 1999.

ROMEO CASABONA, Carlos María. **Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la información**, Madrid, España: FUNDESCO, Colección impactos, 1987.

SANTOS CIFUENTES, **Derecho personalísimo a los datos personales en la Ley T.1997-E**, Buenos Aires, Argentina: Sección Doctrina, 1997.

TÉLLEZ VALDEZ, Julio. **Derecho Informático.** México: Ed. Instituto de Investigaciones Jurídicas, 1991.

VALENZUELA OLIVA, Wilfredo. **Derecho penal: parte general, delito y estado.** Guatemala: Editorial Universitaria, 2004.

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.

Reformas al Código Penal. Congreso de la República de Guatemala, Decreto número 33-96, 1996.