UNIVERSIDAD DEL AZUAY

"LOS DELITOS INFORMATIACOS: CONFLICTO ENTRE EL DERECHO AL HONOR Y LA INTIMIDAD Y EL DERECHO A LA INFORMACIÓN"

Trabajo de Graduación previo a la obtención del título de Abogado de los Tribunales Justicia de la República

AUTOR:

MARÍA FERNANDA POLO CASTRO

DIRECTOR:

DR. JOSÉ CORDERO ACOSTA

CUENCA- ECUADOR

2009

“LOS DELITOS INFORMATIACOS: CONFLICTO ENTRE EL DERECHO AL HONOR Y LA INTIMIDAD Y EL DERECHO A LA INFORMACIÓN”

DEDICATORIA

Esta monografía la dedico a:

Patricia,

Diego,

Joaquina y,

Paúl.

AGRADECIMINETO

Dar las gracias es obligar al corazón a recordar y es que, sin duda, el agradecimiento es la memoria del corazón. Hoy quiero agradecer a mi madre que con la luz de su cariño me forjo sueños nuevos llenos de alegrías, melancolías y misterios; le agradezco por enseñarme la bondad, el respeto y la responsabilidad; pero, sobre todo por apoyarme y transitar junto a mí dentro de este camino relleno de leyes y letras.

Agradezco, además, a mi director de tesis el Dr. José Cordero Acosta quien con su comprensión y sus conocimientos supo guiarme, de la manera más acertada, en la elaboración de esta monografía.

Y por último, agradezco a la vida por la vida de cada uno de mis seres amados y amigos, los mismos que de una u otra manera han compartido con mi alma las múltiples emociones que encierra el vivir.

INDICE DE CONTENIDOS

CAPITULO II

2. EL DERECHO A LA INTIMIDAD, AL HONOR Y EL DERECHO A LA LIBERTAD DE INFORMACIÓN.

CAPITULO III

CAPITULO IV

CAPITULO V

RESUMEN

El creciente desarrollo y perfeccionamiento de los sistemas informáticos no solo ha provocado beneficio dentro de la sociedad. Hoy es común observar como a través de la computadora se puede ejecutar ilícitos que van en contra de derechos de gran jerarquía como son: la intimidad, el honor y la libertad de información y expresión; los cuales han sido catalogados por nuestra Constitución como fundamentales.

Cada persona tiene derecho a proteger su reputación y a reservar su vida y el uso de sus datos personales, solo la información obtenida de manera lícita puede llegar a ser publicada; pero, lamentablemente la internet ha perjudicado estos criterios ya que por la red se populariza toda información.

Al carecer, nuestro ordenamiento jurídico, de jurisprudencia con respecto a la materia, se ve en la necesidad de crear nuevos tipos penales para combatir con este tipo de delitos que atentan a los bienes jurídicos protegidos dentro de la sociedad.

ABSTRACT

The current development and perfecting of informatics systems has benefited society but it is also very common to see how, through the computer, it is possible to perform illegal activities against important rights such as: privacy, honor, and freedom of expression and information; which have been declared fundamental in our Constitution.

Every person has the right to protect his reputation and private life as well as his personal data. Only information obtained legally can be published; however, the Internet has damaged this criterion given that through the net all information is publicly available.

Due to the lack of jurisprudence related to this subject in our legal system, the need to create new penal codes has arisen to combat crimes which attack the juridical rights protected within the society.

INTRODUCCIÓN

El creciente desarrollo de la información, que se vislumbra, en el mundo entero y que a través de la globalización se ha impregnado en nuestro país; ha incorporado en nuestra vida cotidiana un avanzado número de medios electrónicos que facilitan la comunicación individual y social a nivel universal y sobre todo suponen una vía rápida y económica entre los diversos usuarios de los mismos; en consecuencia podría decirse que el desarrollo de la tecnología informática y su enorme influencia en la vida diaria de los habitantes ha generado lo que se conoce con el nombre de "Segunda Revolución Industrial".

Y es que con este desarrollo informático las ideas y pensamientos de los hombres se pueden difundir de manera inmediata y llegar al alcance de millones de personas de todo el mundo, además los beneficios de la tecnología informática se pueden percibir en las transacciones comerciales, la comunicación, el transporte, la medicina, la educación, la seguridad, las investigaciones, la sanidad, entre otras aéreas.

Pero, este revolucionario progreso de la comunicación conlleva la aparición de diferentes ilícitos denominados de manera general como: "Delitos Informáticos" los mismos que lesionan o ponen en peligro muchos bienes jurídicos que se encuentran tutelados en nuestro ordenamiento jurídico; como, también, a aquellos bienes jurídicos que van surgiendo de forma concomitante al desarrollo de las comunicaciones y de los sistemas informáticos.

Por lo que, abordar el estudio de los Delitos Informáticos es tratar de un tema de gran controversia en nuestros días; ya que, se ha generado un expansivo desarrollo tanto en las comunicaciones como en los sistemas informáticos y con éste desarrollo ha surgido, también, la necesidad de crear nuevos tipos penales, para evitar los atentados a través del

empleo de las computadoras o por medios de las mismas; así por ejemplo la violación del derecho a la inviolabilidad y al secreto de la correspondencia que se encuentra contemplado y garantizado por nuestra Constitución en su Art. 66 numeral 21; derecho que se puede ver menoscabado por la utilización de los diversos medios informáticos.

Es por tal motivo, que pretendo concretar el estudio de lo que constituye un delito informático, sus características, los sujetos que intervienen y los diversos atentados que se pueden realizar por los sistemas de cómputo, basando este análisis en la ley de Comercio Electrónico, Firmas y Mensajes que se encuentra vigente en nuestro país desde el año 2002.

Se pretende, además, investigar los Delito Informáticos dentro de nuestra legislación, dentro de las legislaciones internacionales y la doctrina, a fin de obtener una investigación de derecho comparado.

Dada la importancia del tema realizaré un estudio del derecho a la intimidad o privacidad y al honor en la doctrina; derecho éste que se encuentra constitucionalmente reconocido en el Art. 66, numeral 20 de nuestra Constitución; para con posterioridad realizar una investigación de los conflictos que se pueden engendrar entre el derecho a la intimidad, el honor y el derecho a la Información; así como los problemas que se generan entre el hábeas data y el derecho a la intimidad.

Por último, tratare de dar repuesta a la pregunta que me he plateado: ¿Se protege o no el derecho a la intimidad y al honor en nuestra legislación?; para posteriormente con las conclusiones dar por terminado este trabajo investigativo.

CAPITULO I

LOS DELITOS INFORMÁTICOS

"LOS DELITOS INFORMATIACOS: CONFLICTO ENTRE EL DERECHO AL HONOR Y LA INTIMIDAD Y EL DERECHO A LA INFORMACIÓN"

CAPITULO I

1. LOS DELITOS INFORMÁTICOS

1.1. CONCEPTO DE DELITO INFORMÁTICO

1.1.1. Generalidades

El avance positivo de la información ha permitido al hombre obtener ciertos elementos tecológicos necesarios para facilitar el desarrollo de su vida. Desde los inicios de la sociedad, el ser humano a través de su ingenio, ha creado varios códigos para comunicarse: las señales de humo, los destellos producidos por los espejos, el sistema Morse… hasta llegar a la comunicación por vía telefónica. Sin embargo, con la revolución de la 1información que se forja a finales del siglo XIX y mediados del siglo XX, las tecnologías de la información adquieren un papel protagónico en el desarrollo económico, cultural, jurídico y social. Esta eclosión de la información y el ritmo acelerado de la comunicación conllevan aspectos positivos y negativos entre estos últimos se debe precisar que se a abierto la *puerta "ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no eran posibles"*.[1] Además precisa que: *"Los sistemas informáticos han ofrecido nuevas y complicadas oportunidades de infringir la ley y, a su vez, han creado la posibilidad de cometer delitos de manera tradicional a través de modus operandi no tradicionales"*.[2]

[1] Helen Peña y otros. Delitos informáticos, División de Estudios de Posgrado, Facultad de Derecho, Universidad Autónoma de México, México, 1999, publicación de internet en: http://www.unam.edu.mx, p.1.
[2] Ibídem.

Las conductas ilícitas no solo se dan de forma tradicional, sino que se generan nuevas conductas antijurídicas, que se dan a través de modus operandi no tradicional. Ejemplo: la intromisión no autorizada de una persona a un sistema informático o la destrucción y manipuleo de datos de un Estado.

1.2. EL DELITO EN EL CÓDIGO PENAL ECUATORIANO

Nuestro Código Penal ecuatoriano, en el Art. 10, precisa el concepto de delito: "*Son infracciones los actos imputables sancionados por las leyes penales y se dividen en delitos y contravenciones, según la naturaleza de la pena peculiar*"[3].

Este concepto considera delito a todo acto, que debe ser castigado con una pena establecida por el mismo ordenamiento jurídico. Lo que supone una definición de carácter formal y no estructural del delito.

No obstante, nuestro Código Penal recoge, de manera implícita, el concepto estructural de delito y señala los elementos esenciales e indispensables para considerar a un acto como tal. Es por este motivo que se considera delito todos aquellos actos contrarios al derecho, sancionados con una pena y que son imputados a alguien, es decir para que exista delito, el acto debe ser: típico, antijurídico y culpable; todos estos elementos, en conjunto, operan como presupuestos de la pena.

Cuando la acción (comportamiento voluntario que va siempre dirigida hacia un fin) es ilícita y ataca a un bien jurídico protegido, se genera responsabilidad y, por consiguiente, se da la imposición de la pena. Se considera a una persona autora de un hecho (sujeto

[3] Corporación de Estudios y Publicaciones, Código Penal, Quito: Edit. Corporación de Estudios y Publicaciones, 2003, p. 5.

activo) cuando su acción es considerada delito por la Ley, es decir, cuando la conducta sea típica ya que *"el tipo es el momento conceptual desde el cual arranca el delito"*.[4]

El tipo es la descripción de una conducta a la que el derecho asigna una pena; lo que siempre entraña una valoración; solo lo penalmente relevante debe estar tipificado. Cabe señalar que a cada tipo le corresponde una pena, la misma que puede constituir la limitación del goce de ciertos bienes jurídicos propios para el agente de la acción.

En consecuencia, los elementos de tipo penal son: los sujetos, los objetos y la conducta. **Los Sujetos**: Pueden ser Activos (cuando ejecutan la acción típica) y Pasivos (cuando son perjudicados por la ejecución de un acto)

Los Objetos: Se considera tanto al Objeto Material (persona o cosa, sobre la que recae la vulneración del interés jurídico tutelado) como al Objeto Jurídico (razón de ser del derecho penal, la protección a los bienes jurídicos)

La Conducta: Describe el comportamiento criminal a través de los elementos subjetivos u objetivos.

Una vez que se ha explicado, a grandes rasgos, lo que es el delito, dentro de nuestro ordenamiento jurídico y cuáles son las características que debe tener para ser considerado como un ente jurídico, se analiza el concepto de Delito informático.

[4] Carlos Creus, Esquema de Derecho Penal (parte general) Buenos Aires: Edit. Astrea, 1998, p. 73.

1.3.DEFINICIÓN DE DELITO INFORMÁTICO

Existe una gran discusión sobre el concepto de delito informático, puesto que hay muchos autores que opinan que no existe un concepto de carácter universal, ya que solo hay definiciones de acuerdo con la realidad concreta de cada país. He aquí algunas definiciones

Para el profesor Italiano Carlos Sarzana, un delito por computadora es: "*Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena o como mero símbolo*".[5]

Este concepto no hace referencia a lo que es un delito informático, solo define a los delitos cometidos por medio de una computadora, lo que vendría a ser una categoría del delito informático.

Nidia Callegari, también, profesora italiana, define al delito informático como "*aquel delito que se da con la ayuda de la informática o de técnicas anexas*".[6] Esta definición como salta a relucir es demasiado amplia y no ayuda a la compresión de la materia.

María De La Luz Lima sostiene que: *"el delito electrónico en su sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".* [7]

Dentro de este concepto, se puede dilucidar que existen dos delitos: uno electrónico, que utiliza energía eléctrica para la comisión del delito, en consecuencia, lo que interesa en esta

[5] Carlos Sarzana, Criminalitá e tecnología, citado por Peña, Palazuelos y Alarcón, Op. Cit. p. 3.
[6] Ibídem.
[7] María de la Luz Lima, El delito electrónico. Mexico: Edit. Ariel, 1998, p. 56.

definición es la manera en que se comete el delito, es decir, el modus operandi, y el delito informático que atenta contra la información o contra los sistemas que la procesan. En esta definición, lo importante es el objeto material que puede ser perjudicado por la conducta que, en este caso, sería la información.

El alemán, Klaus Tidemann señala: "*la expresión 'criminalidad mediante computadoras' alude a todos los actos antijurídicos, según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro) realizados con el empleo de un equipo automático de procesamiento de datos.*"[8] Esta definición nos conduce a entender que, a través de las computadoras, se puede cometer nuevos ilícitos de manera no tradicional, que van en contra de los bienes jurídicos protegidos en el futuro; por lo que el concepto abarca nuevas formas de criminalidad cometidas por el uso indebido del computador.

"*La acción típica, antijurídica y dolosa cometida mediante el uso normal de la informática, contra el soporte lógico o software de un sistema de tratamiento automatizado de la información*"[9] es un delito informático según el profesor Herrera Bravo. El autor aclara: "*únicamente estaremos ante un delito informático cuando se atenta dolosamente contra los datos digitalizados y contra los programas computacionales contenidos en un sistema; otros casos parecidos serán solo delitos computacionales que no ameritan la creación de un ilícito penal*".[10]

[8] Klaus Tiedemann, Poder Económico y Delito, Barcelona: Edit. Ariel, 1985, p. 123.
[9] Rodolfo Herrera, Bravo, Ponencia: "Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la Ley Chilena", N.19.223, Ponencia presentada en el X Congreso Latinoamericano y II Congreso Iberoamericano de Derecho Penal y Criminología. Santiago de Chile: Universidad de Chile agosto-de 1998, en http.//publicaciones,derecho.org/redi/N.5.
[10] Ibídem.

Personalmente, considero como delito informático a todas aquellas acciones u omisiones típicas y antijurídicas que atentan contra la información[11] o contra los mecanismos que se encargan de su almacenamiento, con el fin de obtener un beneficio o causar un perjuicio a los datos que soportan información.

1.4.SUJETOS QUE INTERVIENEN EN LOS DELITOS INFORMÁTICOS

La criminalidad informática envuelve conductas que atentan contra los bienes jurídicos tanto individuales como colectivos; lo que se produce porque en la red informática no se reconozca limitaciones ni fronteras. A través del ciberespacio, se cometen un creciente número de crímenes informáticos perpetrados por cualquier persona ya sea natural o jurídica y desde cualquier lugar, afectan a todo usuario en el mundo. Los sujetos que interviene en la ejecución de los mencionados delitos son los siguientes:

1.4.1. SUJETO ACTIVO

Es el autor que realiza la acción prohibida y, en consecuencia, debe sufrir la pena correspondiente. Es el que conjuga el verbo rector y el que incurre en la acción u omisión.

El moderno Derecho Penal ha establecido que solo el ser humano, la persona natural, puede ser sujeto activo del delito, ya que este goza de conciencia y voluntad.

El sujeto activo, en este caso no es cualquier persona natural o jurídica que actúa u omite un comportamiento injusto, sino presenta ciertas particularidades, es decir, tiene una gran

[11] La información es un conjunto de datos envidos desde una fuente transmisora hasta una fuente receptora. Toda información está compuesta de datos y es el receptor consciente quien interpreta tales datos, para que se conviertan en elementos con significado.

destreza en el manejo de la informática;[12] habitualmente, por sus conocimientos en la materia, localizan información de carácter sensible y obtienen provecho de esta para sí o para un tercero.

Algunos doctrinarios propugnan que el nivel de capacidad del delincuente informático es muy elevado y es por tal motivo que se los conoce como "*delitos de cuello blanco*", término introducido por el norteamericano Edwin Sutherland. Este criminólogo estadounidense considera al sujeto activo como una persona de cierto status social y socio-económico; además, los injustos que realizan estos sujetos son motivados por el deseo de hacer conocer al resto de las personas sus capacidades intelectuales y cognoscitivas o, incluso, para demostrar qué tipo de delitos se pueden cometer mediante los ordenadores de información.

Los sujetos activos más conocidos son: los Hackers, los Crackers, los Phreakers y los delincuentes informáticos

1.4.1.1. Los Hackers

Son aquellas personas con vastos conocimientos en informática; son genios informáticos, que centran su vida en la investigación y en el desarrollo de sus capacidades cognoscitivas. Son apasionados e incluso, maniáticos de las computadoras por lo que buscan perpetrar en los sistemas informáticos y resolver todas las dificultades que se les presen te en su camino indagador; no poseen límites, su obsesión los lleva cumplir sus desafíos.

[12] Es la ciencia que estudia la información y los medios de transmisión de la información para el almacenamiento y procesamiento; la acumulación de varios datos se llama "datos agregados"; la unión de estos "registros" a la colección de varios de ellos se les conoce como "archivos" y a la unión de varios archivos se le denomina base de datos.

Este tipo de personas disfrutan aprendiendo los detalles que encierran los sistemas de programación y son navegadores muy hábiles. Su talento e inteligencia los sumerge en un mundo dificultoso de redes, sistemas de seguridad y programas de cómputo, que los cautiva. Habitualmente, no buscan estropear los sistemas, ni obtener rédito de sus conocimientos; son, simplemente, observadores y curiosos informáticos.

1.4.1.2. Los Crackers

Son grades técnicos de programación informática; por este motivo, encuentran las formas más sofisticadas para vulnerar las claves de los sistemas y alcanzar beneficio propio o para un tercero. Son más conocidos como ladrones de guante blanco; delinquen para sentirse superiores al resto e, incluso por no estar de acuerdo con el sistema político o social.

Estos bandidos penetran virus en los sistemas informáticos y los quebrantan por lo que dificultan el manejo de los sistemas de seguridad instalados en los sistemas informáticos; este tipo de conducta afecta, especialmente, las empresas privadas y a las agencias gubernamentales; por lo tanto, es aplicable como a los demás sujetos activos, las acciones por falsedad, daño, espionaje o estafa informática.

1.4.1.3. Los Phreakers

Son aquellas personas que durante su vida han adquirido extensos conocimientos sobre redes telefónicas; pero, ordinariamente, con su experiencia en telefonía realizan actividades indebidas con los teléfonos, en especial, con los celulares. Son diestros en intervenir centrales telefónicas de países extranjeros y, por estas acciones, logran incrementar su economía de forma ilícita y vertiginosa**.**

Son capaces de elaborar equipos electrónicos para interceptar llamadas, de una forma tan astuta, que sus titulares no logran captar la intromisión; incluso este tipo de especialistas en redes telefónicas, logran implantar ciertos dispositivos en los sistemas de cómputo y, por medio de la internet, roban la señal y consiguen comunicarse de manera inmediata con cualquier parte del mundo; obviamente, la comunicación obtenida no tiene costo alguno. En definitiva, los Phreakers obtienen el control sobre la orientación de las llamadas telefónicas, basándose en la individualización y uso de los distintos tonos originados en los aparatos de comunicación.

1.4.1.4. Los Delincuentes Informáticos

Son personas que utilizan las computadoras de forma indebida consiguiendo perjudicar a terceras personas, ya sea de forma local o a través del internet. Uno de los métodos más conocidos de este tipo de injustos constituye el interceptar las compras por medio de la internet, para lo que el delincuente informático duplica las tarjetas magnéticas y manipula la información original, consiguiendo comprar bienes costosos que son enviados a direcciones distintas a la del titular del número de la tarjeta duplicada.

Julio Villanueva Lara nos explica en su obra *Introducción a la Computación* que el delincuente informático "*es aquel pirata que distribuye software sin contar con las licencias de uso proporcionadas por su autor, atentando de esta forma contra la propiedad intelectual.*"[13]

[13] Julio Villanueva Lara, Introducción a la Computación, Washington: Edit. O.E.A., 1981, p. 73.

Es así como se evidencia que el sujeto activo es el agente que ejecuta el acto delictivo, quien, en muchos de los casos, puede ser un solo individuo; pero, en otros, son varios los bandidos que ejecutan las acciones inicuas.

1.4.2. SUJETO PASIVO

Este es el titular del bien jurídico protegido, en definitiva, es el que sufre la acción delictiva realizada por el sujeto activo estos puede ser: las instituciones crediticias, los órganos estatales, los individuos, etc. que utilizan sistemas informáticos. Es a través de los perjuicios ocasionados al sujeto pasivo que se puede conocer las nuevas formas de criminalidad informática y su modus operandi.

Cabe recalcar que, en los injustos de carácter comunitario, sujetos pasivos podemos ser todos, en consecuencia, se debe tener presente, también, los delitos difusos.

1.5. CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

Estos delitos presentan algunas particularidades, entre ellas tenemos las siguientes:

- Son delitos cuyo sujeto activo, la mayoría de las veces, es experto en lo referente a sistemas informáticos; se los conoce como delincuentes de "*cuello blanco"* (*white collar crimes*) además, gozan de cierto status social, puesto que están rodeados de ordenadores de información y materiales técnicos que facilitan la comisión del delito.
- Este ilícito informático se caracteriza por ser eminentemente doloso, es decir, su autor lo realiza con intención y voluntad de causar daño a los sistemas de cómputo o se ingenian para utilizar como medio a la computadora y ejecutar otros ilícitos. Es

por este motivo, que las conductas culposas como aquellas que por juego o error se entrometen en los sistemas de computo, en los archivo ajenos o dañan las computadoras, no comenten ilícito alguno.

- Se caracterizan por el empleo abusivo de ordenadores y por el ingreso el ingreso a una base de datos de forma ilegítima e, incluso, por la introducción de virus en el sistema telemático.
- La mayoría de estos injustos son de resultado, porque se logra detectar, dentro de los sistemas, las conductas delictivas que tienen como fin o como medio, a las computadoras.
- Habitualmente los agentes de este tipo de delitos son personas que delinquen cuando se encuentran en su trabajo y es en base a los datos que obtienen de su empleo que generan perjuicios en contra de empresas de la competencia o en contra de la empresa para la que trabajan.
- Este tipo de injustos, generalmente producen pérdidas económicas de gran magnitud porque se acometen contra procesadores de empresas millonarias.
- Son ilícitos que, muchas veces, permanecen en la impunidad; no se los denuncia por falta de regulación y porque en el caso de las empresas tienen temor de mostrarse débiles frente a su mercado, lo cual implicaría quebrantos en su economía.
- Estas acciones se consumen en milésimas de segundos, debido a que la tecnología ofrece la difusión de la información de manera inmediata desde y hacia cualquier parte del mundo.

- Producen un riesgo masivo en la sociedad porque la información quebrantada puede estar constituida de datos sensibles de una persona o grupo de personas (sus cuentas bancarias, sus favoritismos o tendencias y, en un futuro, gracias al descubrimiento del genotipo humano se podría averiguar, inclusive, sus enfermedades y molestias) lo que afecta al desarrollo de una vida normal. En definitiva, los delitos informáticos atentan contra la intimidad y la propiedad de las personas.
- No hay una regulación por lo que tienden a difundirse con mayor rapidez.

Al conocer las características de los delitos informáticos, se puede señalar que es necesaria una regulación de la materia para frenar el ingreso, la destrucción, la alteración o la modificación de datos a través de programas informáticos destructivos. Con una adecuada legislación, la proliferación de las conductas delictivas que se llevan a cabo por medio de sistemas informáticos no estarían inmersos en la impunidad.

Es conveniente manifestar, también, que al ser la infracción informática de carácter doloso y no de mera contravención, debe ser investigado por el Ministerio Público, ya sea de oficio o a través de las denuncias de los particulares afectados.

1.6. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

La clasificación que plantea la doctrina es:

- Delito Informático como Medio y como Fin.
- Delito Informático como Método, Medio o Fin.
- Delito Informático, según el Objeto, el Sujeto o la Función.

1.6.1. Delito Informático Como Medio y Como Fin

Tellez Valdés[14] clasifica a los delitos informáticos siguiendo dos patrones: *"el uso de la computadora como instrumento o medio o el computador como fin u objetivo"*.

1.6.2. Como Instrumento o Medio: Los delitos informáticos son aquellos que contienen conductas criminógenas que se valen de la computadora como "*método, medio o símbolo en la comisión del ilícito*".[15] Se puede efectuar varios ilícitos en contra de bienes jurídicos tutelados aprovechándose de los sistemas de cómputo.

1.6.3. Como Fin u Objetivo: Son las conductas que se realizan y "*van dirigidas en contra de la computadora, accesorios o programas como entidad física"*.[16] El objeto material de la infracción es la computadora ya que va en contra de su integridad o funcionamiento y este detrimento es cometido a través de medios electrónicos.

1.6.4. Delito Informático Como Método, Medio o Fin

En la construcción de esta clasificación hay autores que consideran que se utiliza la tecnología electrónica como medio, método o fin. La conducta criminal es cometida como método cuando: "*los sujetos utilizan métodos electrónicos para cometer el ilícito. Como medio son consideradas aquellas conductas criminales en donde, para realizar un delito, se usa una computadora como medio o símbolo. Como fin son las conductas criminales dirigidas en contra de la entidad física del objeto o máquina electrónica o su material con el objeto de dañarla*".[17]

[14] Téllez Valdés, Derecho Informático, México: Edit. McGraw, 1997, p. 105 y ss.
[15] Ibídem.
[16] División de Estudios de Postgrado, Op. Cit., p. 6.
[17] El delito electrónico, Op. Cit., p. 48.

1.6.5. El Delito Informático Según el Objeto, el Sujeto o la Función

Esta clasificación, según su autor Pérez Luño *"es a partir del criterio objetivo, subjetivo y funcional"* [18].

1.6.5.1. Desde Lo Subjetivo: Se centra en las características que poseen los delincuentes informáticos, por lo que investiga si se trata de sujetos que tienen una posición favorable, es decir, una relación con el sistema o si son sujetos comunes que no tienen poder frente al sistema.

1.6.5.2. Desde Lo Objetivo: Considera los perjuicios que las conductas han originado; define el delito y su modus operandi, según el tipo de delito de la siguiente manera:

1. Los fraudes.
2. Manipulaciones contra los sistemas de procesamiento de datos.
3. El sabotaje informático.
4. El espionaje informático y el robo o hurto de software.
5. El robo de servicios.
6. El acceso no autorizado a servicios informáticos.

1.6.5.3. Desde Lo Funcional: Abarca el proceso informático o el procesamiento de datos y presenta una nueva clasificación de los delitos:

1. Atentado contra la fase de entrada del sistema.
2. Atentado contra la fase de salida del sistema.
3. Atentado contra los programas del sistema, y

[18] Citado por Carlos Escobar Márquez, El Delito Informático, Bogotá Colombia: Edit. LEYER, 1999, p.123.

4. Atentado contra la elaboración, procesamiento de datos y comunicación telemática.

Se puede observar en la clasificación de los delitos informáticos varios puntos de vista, pero es necesario concretar esta clasificación, según los elementos del tipo penal que son tres:

a. **Los Sujetos:** Son personas tanto naturales como jurídicas que realizan el injusto o que sufren perjuicios por el delito
b. **El Objeto:** Son los bienes jurídicos menoscabados por este tipo de conductas; y
c. **La Conducta:** Es el proceder de tal manera que, el actuar, se acople a lo descrito en el tipo penal

Es necesario, además, ubicar un nuevo elemento para la clasificación de los delitos informáticos y este es el **Medio**, que se enfoca en el modus operandi o en el papel del sistema de procesamiento informático, dentro de la comisión la conducta.

1.7. TIPOS DE DELITOS INFORMÁTICOS

En la actualidad, desde la fase interna hasta la fase externa o de ejecución, es decir, en cualquier etapa del iter-criminis, los delitos informáticos se pueden llevar a cabo por medio de las computadoras, convirtiéndose estas en instrumentos idóneos para la comisión de delitos por lo que se ha llegado a catalogar el modo de cometer estos delitos.

1.7.1. Delitos Cometidos Mediante Manipulación De Computadoras

Este tipo de ilícitos se puede realizar de forma simple, ya que no se necesita adquirir extensos conocimientos en la materia para manipular los datos de entrada, de salida o los programas que constan en el procesador.

1.7.1.1. Manipulación de Datos de Entrada

Este tipo de injustos consiste en la sustracción de datos que puede efectuarse por cualquier persona; este injusto no necesita de conocimientos técnicos específicos. Además, esta conducta consiste en "*tomar alguno de los datos procesados por la computadora sustrayéndolos a través del medio magnético, óptico o magnético óptico, para luego ser leídos, manipulados o, simplemente, mantenidos en otra computadora*".[19]

Aparte de las particularidades ya manifestadas, se puede señalar que los agentes de este tipo de ilícitos no son detectados con facilidad, debido al frágil control que se da a los datos de salida.

1.7.1.2. Manipulación de Programas

Al contrario de lo ya se ha explicado sobre la manipulación de datos de entrada para ejecutar este delito, se necesita poseer vastos conocimientos técnicos en programación informática.

Los causantes de este tipo de infracciones a través de su conducta consiguen insertar nuevos programas informáticos o modificar los programas ya existentes en el sistema de la computadora, con el fin de obtener beneficio propio.

[19] Ibídem, p.274.

El método más conocido para cometer este tipo de manipulaciones es el llamado *Trojan Horse*, (caballo de Troya) método con el cual se consigue manipular un programa que al momento de iniciarlo, no cumple con las funciones previstas. Además, este subprograma puede causar daños severos en los programas del ordenador e, incluso, insertar otro programa llamado virus activo.

Los programas deberían estar provistos de controles específicos para evitar este tipo de manipuleo; en consecuencia, las empresas se ven forzadas a contratar personal especializado para contrarréstalo.

1.7.1.3. Manipulación de Datos de Salida

La perpetración de este delito se obtiene al fijar un objetivo al sistema y su funcionamiento; se instaura instrucciones falsas que la computadora las asimila y las ejecuta como si fueran auténticas. Ejemplo: la manipulación de cajeros automáticos a través de una línea telefónica, la misma que se conecta a la línea del banco y del cajero. Entre este tipo de manipulaciones se puede encontrar las siguientes:

1.7.1.3.1. Fraude Efectuado por Manipulación Informática

Se consigue al manipular los datos que se repiten en los sistemas de cómputo. La conocida *salami technics* o redondeo de cuentas es la técnica más destacada para realizar estos delitos; consiste en reducir saldos de cuentas bancarias a través de la alteración de las instrucciones de un programa.

1.7.1.3.2. Falsificación por Vía Informática

Existen dos maneras de falsificación mediante computadora, ya sea el computador, el objeto de la falsificación o sea el computador, el instrumento de la falsificación. Para estas falsificaciones, con frecuencia, las computadoras necesitan de un hardware específico para perfeccionar el resultado.

1. Como Objeto: Cuando el computador sirve de objeto para la falsificación, puesto que modifica los datos almacenados de manera computarizada.

2. Como Instrumento: Se utiliza el computador como instrumento para plasmar la imitación engañosa. Ejemplo: la imitación de un cheque o de un billete.

1.7.1.4. Modificaciones de Programas o Datos Computarizados

Sin lugar a duda, es en este tipo de ilícitos donde los genios en computación derrochan sus conocimientos, puesto que buscan destruir barreras de seguridad, con el fin de apoderarse o dañar los datos que están inmersos en otra computadora.

El llamado Sabotaje Informático "*Computersabotage*" consiste en la actividad criminal de borrar, suprimir y alterar los datos de una computadora para deteriorar el normal funcionamiento del sistema. Para ello, acude a ciertos recursos.

1.7.1.4.1. Virus

Fue en los años 60, con el desarrollo de la informática y la computadora, que se insertan estos virus que afectan al funcionamiento del sistema, ya que ejecuta órdenes que se propagan de computador a computador por medio de un código.

La perdida de información que alberga la computadora o las modificaciones de datos constituyen la enfermedad sin remedio de nuestra sociedad, que depende de la comunidad informática.

1.7.1.4.2. Gusanos

A diferencia de los virus, los gusanos no se propagan, pero consiguen infiltrarse en el sistema de la computadora y, al momento de la emisión de órdenes, se destruyen.

1.7.1.4.3. E-mails "bombs"

Con el correo electrónico, creado para que un individuo se comunique con otro u otros individuos por medio de mensajes a través de la red, se ha generado un tipo de injusto que causa detrimento a los sistemas de cómputo. Consiste en la incorporación de virus a los mensajes para que, al momento, de abrirlos destruyan los datos del ordenador.

Este tipo de bombas poseen diferentes características, algunas causan daños irremediables, en cambio, otras solo paralizan el sistema al intentar ver el mensaje. Carlos Márquez, en su libro El Delito Informático, manifiesta que usualmente quienes hacen este tipo de bombas suelen engañar al destinatario haciéndole creer que quien envía el mensaje es alguien con el que se comunica vía correo electrónico a menudo.

1.7.1.5. Acceso no Autorizado a Servicios y Sistemas Informáticos

Los delitos de esta clase tienen un trasfondo más complejo que los delitos anteriores, ya que se busca información secreta de un sistema para beneficio de terceros: el espionaje, por ejemplo.

1.7.1.6. Reproducción no autorizada de Programas Informáticos de Protección Legal

Lesiona la propiedad intelectual y estimula la piratería del software; la mayoría de los países condenan estas actuaciones, puesto que generan grandes pérdidas económicas a los creadores y comercializadores de software.

1.7.1.7.Sabotaje Informático

Primordialmente, produce daño y se apodera de los centros neurálgicos computarizados, logra, de esta manera, que el sistema solo le obedezca al intruso o se caiga cuando éste lo desee.

Rogelio Baón, en la elaboración de la clasificación de los delitos informáticos, señala que el sabotaje informático se puede presentar "*sobre datos y programas, bienes intangibles, como sería el caso de prácticas como la 'bomba de tiempo', que destruye el programa o 'una rutina de cáncer', que distorsiona el funcionamiento de aquél mediante instrucciones que se auto-reproduzcan, o bien, el equipamiento en sí.*"[20] La práctica llamada *logic bombing* constituye una serie de programas secretos que vienen activados con el fin de alterar los datos u otros programas del sistema.

1.7.2. Delitos Que Tienen Como Instrumento Las Computadoras

Son aquellos delitos en los que las computadoras ayudan para la comisión de los ilícitos. Entre los más conocidos, están:

[20] Rogelio Baón Ramírez, Visión General de la Informática en el Nuevo Código Penal, en Ámbito Jurídico de las Tecnologías de la Información, Madrid: Edit. Cuadernos de Derecho Judicial, 1996, p. 79 a 112.

1.7.2.1. Falsedad Informática

Consiste en una falsedad por vía computarizada, mediante la cual se puede modificar tarjetas de crédito, cheques, letras de cambio, títulos, valores, es decir, se puede alterar todo tipo de instrumentos de carácter público como privados, incluso, todo el sistema contable de una empresa y facilita llevar una doble contabilidad con la finalidad de evitar impuestos.

Dentro del título IV, de los delitos contra la Fe Pública del Código Penal ecuatoriano, se encuentra los tipos de falsedad documentaria y en el artículo 353.1, ya citado anteriormente, se habla sobre la falsificación electrónica y, manifiesta que:

> *Son reos de falsificación electrónica la persona o personas que con el ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático ya sea*:
>
> ***1.*** *Alterando un mensaje de datos en alguno de su elementos o requisitos de carácter formal o esencial;*
> ***2.*** *Simulando un mensaje de datos en todo o en parte de manera que induzca a error sobre su autenticidad;*
> **3.** *Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.*
>
> *El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.*[21]

De esta manera, se puede afirmar que nuestro Código Penal resguarda los datos almacenados en los diferentes sistemas informáticos al mismo nivel que los documentos públicos y privados, es decir, que gozan de idéntico efecto jurídico. El hecho de introducir datos a un elemento o requisito de carácter formal crea una situación que se asemeja a la

[21] Código Penal. Op. Cit., p. 136.

creación de un documento falso, mientras que las operaciones de alteración o supresión de información que induzcan a error, se las considera como falsificación de un documento auténtico.

En definitiva, lo que se busca es desarraigar las alteraciones de información, la introducción de datos falsos y que se borre información de manera intencional, con el fin causar perjuicio a un tercero o buscando beneficio propio.

El bien jurídico protegido es la fe pública que debe recaer en la confianza, la misma que se encuentra expresada en ciertos signos y que es indispensable para el desenvolvimiento social.

Con respecto a la definición de Fe David Baigún y Carlos Tozzini sostienen que: *"La Fe Pública debe ceñirse al amparo o tutela, en su primera función, de los signos e instrumentos convencionales que el estado impone con carácter de obligatoriedad y, en su segunda función, a los actos jurídicos que representan ciertas formas materiales y que son destinados a los objetivos legalmente previstos"*.[22]

Se puede apreciar que los delitos contra la fe pública están encaminados a proteger la confianza social, en base de la veracidad y autenticidad de ciertos documentos legales.

Advierte Muñoz Conde con respecto a los delitos de falsedad que:

> *Todos o casi todos los objetos penales sobre los que recae la acción en los delitos de falsedades: sellos o efectos timbrados, monedas, documentos públicos, documentos mercantiles, títulos profesionales, etc. son signos que engendran esa apariencia de realidad. La creación o manipulación ilegítima de esos objetos son ataques al tráfico fiduciario, a la fe pública en medida en que*

[22]David Baigún y Carlos Tozzini, La Falsedad Documental en la Jurisprudencia, Buenos Aires: Edit. Depalma, 1992, p. 13.

> *dichos objetos gozan de crédito en las relaciones sociales y su uso es indispensable para el normal desarrollo de la convivencia con un mínimo de organización.* [23]

Se asevera, con este concepto, que la fe pública constituye el bien jurídico tutelado penalmente, siendo este capaz de ser perjudicado por sistemas informáticos, mediante la manipulación de datos almacenados.

Los falsificadores tienen la ventaja de reproducir fácilmente distintos estilos y tamaños de letras, por medio de las computadoras, las mismas que pueden ser utilizadas en su beneficio con cualquier tipo de documento; incluso, por medio del scanner, se rastrea un documento se trasmite la imagen a una computadora para maniobrarla y cambiarla.

Es importante señalar que la falsedad del documento tiene que ser probada y poseer los tres requisitos señalados por la doctrina: *"a) la alteración de la verdad; b) que la alteración de la verdad afecte los datos o elementos esenciales del documento; c) y un elemento subjetivo, es decir, la conciencia y voluntad del agente de trasformar la realidad"*. [24]

Luego de todo lo expuesto, se puede concluir que este tipo de injustos se consuman desde que se produce la alteración, la ocultación o mutación de la verdad, llegando a producir los resultados esperados por su autor, es decir, cuando el tipo se ha realizado plenamente desde el punto de vista de la acción del autor como desde el punto de vista del resultado.

[23] Francisco Muñoz Conde, Derecho Penal Parte Especial, Valencia: Edit. Tirant lo Blanch, 1996, p. 606.

[24] Enrique Bacigalupo Zapater, Documentos Electrónicos y Delitos de Falsedad Documental, Buenos Aires: Edit. Depalma, RECPC04-12,2002.

1.7.2.2. El Hurto Informático

Consiste en el apoderamiento de bienes ajenos a través de las computadoras, generalmente, estos injustos se generan en el sistema financiero ya que se busca la sustracción de dinero de información o de bienes mercantiles.

Un ejemplo de este delito son las trasferencias que realizan los empleados de entidades bancarias a cuentas ficticias o de terceros, para luego asignárselos a sus cuentas. Sin lugar a duda, este tipo de hurto es más difícil de detectar y necesariamente es ejecutado por personas que poseen vastos conocimientos en materia bancaria.

1.7.2.3. La Estafa Informática

El delito de estafa se encuentra tipificado en nuestro Código Penal, en el Art. 563.

> *En el que, con propósito de apropiarse de una cosa perteneciente a otro, se hubiere hecho entregar fondos, muebles, obligaciones, finiquitos, recibos, ya haciendo uso de nombres falsos, o de falsas calidades, ya empleando manejos fraudulentos para hacer creer en la existencia de falsas empresas, de un poder o de un crédito imaginario, para infundir la esperanza o el temor de suceso, accidente o cualquier otro tipo de acontecimiento quimérico, o para abusar de otro modo de la confianza o de la credulidad, será reprimido con prisión de seis meses a cinco años y multa de ocho a cinto cincuenta y seis dólares de los Estados Unidos de Norteamérica.*
>
> *Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.*
>
> *La pena será de reclusión menor ordinaria de tres a seis años, si la defraudación se cometiera en casos de migraciones ilegales.* [25]

[25] Código Penal Ecuatoriano, Op. Cit., p.223.

Por consiguiente, la estafa sería aquel provecho ilícito que se obtiene generando un daño patrimonial a través de engaños o enredos con el propósito de inducir a un tercero en error.

Para que la estafa se consuma, el sujeto activo debe engañar a su víctima (sujeto pasivo) con ánimo de lucro, de manera que se desencadene un error esencial, ya que el ardid constituye el verbo rector de este tipo de ilícitos; además, este engaño debe ser suficiente o ajustado al objetivo para lo que es indispensable visualizar el contexto personal del sujeto pasivo y todos aquellos sucesos importantes que asistan en el caso. Inclusive, el error esencial, al que me he referido, debe facilitar la pérdida del patrimonio del sujeto pasivo; por lo que se exige una relación de causalidad entre el engaño provocado y el perjuicio conseguido. Siendo esta la manera de proceder en este tipo de delitos, la estafa informática se puede definir como aquella que se realiza sirviéndose de una computadora, ya sea para vulnerar su seguridad o para manipular su sistema informático; por ejemplo: el empleado que maniobra el sistema contable de la empresa en la que labora, con el objetivo de distorsionar la cantidad de pedidos de mercadería enunciados por esta, con la intención de que el excedente de mercadería sea trasladada a una tercera persona, en complicidad con el autor de la estafa.

Por lo tanto, existirá estafa informática en todos aquellos acaecimientos en los cuales el agente astutamente obtiene provecho, mediante el uso de mecanismos que permitan, de forma eficiente, la conexión autorizada por la computadora.

Es necesario recalcar que, dentro de la delincuencia informática, se acepta, como delito de estafa, el uso no autorizado de datos informáticos, debido que el almacenamiento, la

trasmisión o la utilización de ciertos datos, a cargo de personas autorizadas o no, permiten conocer circunstancias delicadas del cliente, lo que provoca perjuicios en su patrimonio.

Gustavo Eduardo Aboso y María Florencia Zapata con respecto a la estafa informática sostienen que: "*Los tipos penales especiales de estafa informática (Computerbetrug) regulan este tipo de comportamientos donde no media engaño o error alguno, sino un uso no autorizado por parte del interesado por lo que se ha generado la necesidad de regular, a la par de la previsión de la estafa genérica, otra que atienda de manera exclusiva a la mediación de un aparato mecanizado*". [26] Por este motivo, los ordenamientos jurídicos de España, Alemania, Francia, Suiza y Norteamérica han regulado a la estafa informática, mediante el uso abusivo de datos o mediante la alteración o introducción de programas informáticos, que generan un perjuicio económico; todo esto con orientación a solucionar los nuevos injustos originados por el desarrollo informático.

[26] Gustavo Aboso y María Florencia Zapata, Cibercriminalidad y Derecho Penal, Buenos Aires: Edit. BdeF, 2006, p. 89.

CAPÍTULO II

EL DERECHO A LA INTIMIDAD, AL HONOR Y EL DERECHO A LA LIBERTAD DE INFORMACIÓN

CAPITULO II

2. EL DERECHO A LA INTIMIDAD, AL HONOR Y EL DERECHO A LA LIBERTAD DE INFORMACIÓN.

Nuestra actual Constitución ha señalado ciertos derechos fundamentales entre los cuales se destacan tres: el derecho al honor, a la intimidad y a la propia imagen. Descubrir lo que cada uno de estos derechos representa, sus características y sus diferencias es lo que se pretende estudiar dentro de este capítulo para, posteriormente, revelar, también, el contenido del derecho a la libertad de información y los límites que existen entre este derecho y los derechos antes puntualizados.

Es necesario, en principio, diferenciar los tres derechos en cuestión, que se encuentran recogidos dentro de nuestra Carta Magna, en el Capítulo Sexto: De los Derechos de Libertad, en el artículo 66, numerales 18 y 20 que expresan lo siguiente: "*Se reconoce y garantizará a las personas:*

18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona.

20. El derecho a la intimidad personal y familiar."[27]

Partiendo de lo que expresa nuestra Constitución sobre los derechos que reconoce y garantiza, es necesario manifestar que estos son los llamados derechos de la personalidad que son de carácter extra-patrimonial y que se dividen en: derechos de la personalidad física y derechos de la personalidad espiritual o integridad moral de las personas, dentro de los cuales se consideran: el derecho al honor y buena reputación, el derecho a la dignidad y la intimidad personal, el derecho al respeto y consideración del Estado y el derecho a

[27] Asamblea Constituyente, Constitución de la República del Ecuador, Capítulo Sexto "Derechos de Libertad" Quito, Edit. Grafikos, s/f, p. 41.

desarrollarse plenamente dentro de una sociedad, sin que nadie humille o deshonre a una persona.

Vale recordar que estos derechos son inherentes al ser humano ya que nacen y mueren con él y, al ser fundamentales, están garantizados y protegidos constitucional, civil y penalmente y se los reconoce a todos los sujetos por igual.

Además, estos derechos, dentro de sus principios generales, tienen la consideración de ser llamados de primera generación ya que son innatos en las personas y el objetivo del Estado es reconocerlos, respetarlos y protegerlos e impedir cualquier discriminación por raza, riqueza, religión, condición social, nivel cultural u opinión pública.

Por lo tanto, nuestro ordenamiento jurídico reconoce estos derechos personales y garantiza no solo los derechos enumerados dentro de nuestros cuerpos legales, sino todos aquellos derechos que se originen de los diferentes instrumentos internacionales vigentes.

2.1. EL DERECHO AL HONOR

"*Al rey la hacienda y la vida se han de dar; pero el honor es patrimonio del alma y el alma solo es de Dios*".[28]

El derecho al honor es uno de los bienes jurídicos más preciados de la persona; es por esto que nuestro ordenamiento jurídico lo consagra como derecho fundamental y lo reconoce como parte de todo ser humano; sin embargo, el concepto de esta expresión "honor" ha sido un tanto difícil de establecerlo. Esto dice Beccaria: *"la palabra honor es una de las que ha servido de base para largos y brillantes razonamientos, sin que jamás se haya aplicado a una idea estable y bien determinada"*.[29]

[28] Calderón de la Barca; El Alcalde de Zalamea, Madrid, Edit. AICE, 1990, p. 56.
[29] C. Beccaria, De los Delitos y de las Penas; Madrid: Edit. Imprenta Nacional, 1986, p. 48.

Por lo tanto, la doctrina, a pesar de las múltiples controversias, ha logrado distinguir tres concepciones:

A) **Concepción Fáctica**: Considera el honor como la estima que la sociedad tiene de una persona o la estima que la propia persona tiene de sí misma.

B) **Concepción Normativa**: Según la cual el honor sería equivalente a la dignidad de la persona y, en consecuencia, se define como el derecho a ser respetado por los demás.

C) **Concepción Mixta o Fáctico-Normativa**: Define al honor *"teniendo en cuenta tanto la dignidad humana como el contexto social en el que está inmerso el individuo".*[30]

Desde esta perspectiva, el honor podría ser un derecho que se deriva de la dignidad de las personas, el cual debe ser respetado por los demás dentro del marco social.

Por su parte, Berdugo Gómez de la Torre manifiesta:

> *Toda definición del bien jurídico honor ha de ser conforme los principios de la Constitución debido al carácter normativo de la misma* –reconociendo, además – *que el honor es una realidad empírica, ya que la sociedad valora las cualidades y comportamientos de los ciudadanos".* [31] Con igual puntualidad señala: *"que de la determinación del contenido del honor requiere la puesta en relación de la realidad con el sistema social constitucionalmente consagrado; sistema social de evidente carácter personalista al consagrar la dignidad de la persona y el libre desarrollo de la personalidad como fundamento del mismo.* [32]

El honor, por lo tanto, es un derecho que debería estar instruido a todos los hombres por igual, sin discriminación alguna por sus condiciones personales o comportamiento social.

[30] Tomas Vidal Marín; El Derecho al Honor y su Protección desde la Constitución Española, Madrid: Edit. Centro de Estudios Políticos, 2001, p. 45.
[31] Berdugo Gómez de la Torre; Honor y Libertad de Expresión, Madrid: Edit. ONI, 1987, p. 57 y siguientes.
[32] Ibídem.

2.1.1. Concepto Subjetivo, Objetivo y Social de Honor

Al considerar los valores como parte del individuo, el derecho tiene la obligación de protegerlos de cualquier intromisión. En lo que respecta al honor, este se ve impregnado de valores íntimamente personales e individuales, producto de la autodeterminación de cada uno dentro de un grupo por lo que evita el descenso inmerecido en la consideración ajena.

Se habla del honor desde un plano **Subjetivo**, valoración que una persona tiene de sus actitudes dentro de una sociedad; lo que depende de la estima y consideración que cada persona tiene de sí misma. Sin embargo, el concepto subjetivo de honor no es apto, puesto que cada individuo puede tener un alto aprecio de sí o, al contrario, una escasa autoestima, que no se ajusta a la realidad. La doctrina señala que: *"la protección jurídica no pude hacerse depender de los cambiantes sentimientos del sujeto y de su mayor o menor sensibilidad, pues, además, de la enorme inseguridad jurídica que comportaría dejar en manos del ofendido la estimación de si se ha producido o no ataques a su honor"*[33]De esta manera el derecho al honor desde el punto de lo subjetivo es inapropiado.

Desde lo **Objetivo**, el derecho al honor es la valoración que los demás hacen de nuestras acciones; la reputación y el aprecio que tienen los demás de una persona. Es importante considerar que, en la actualidad, el honor es un derecho que se relaciona con la vida en sociedad por lo que la reputación de las personas dependerá del entorno social y la cultura en la que estas se desenvuelvan. Pero, optar por un concepto objetivo de honor nos encaminaría a ciertos conflictos en cuanto podrían existir personas *"que careciesen de*

[33] Cardenal Murillo A., y Serrano Gonzales de Murillo J.L., Protección Penal del Honor; p. 30 y 31; citado por Tomas Vidal Marín; El Derecho al Honor y su Protección desde la Constitución Española; Madrid: Edit. Centro de Estudios Políticos, 2001, p. 51.

reputación social por no haber estimación pública de sus cualidades" o *"la reputación social puede ser inmerecidamente buena o mala"*.[34]

Así, ciertos comportamientos deshonrosos para una sociedad no lo serán para otra porque dependerá de los valores, de las normas y de la cultura que posea, los cuales cambiarán de acuerdo con el tiempo y el desarrollo. Aquí se habla de un **Concepto Social** de honor que, según Joaquín Urías, *"es variable según el entorno cultural y social de la persona"*.[35]

Lo social coexiste en cada individuo y *"no solo es algo que nos oprime, es algo también que nos constituye; está en nuestras creencias, en nuestros sentimientos, gustos y actitudes, ésta amalgamado en aquel principio de individualización que late en cada uno pero que no puede manifestarse en su misma singularidad sin apoyarse y nutrirse de aquellos elementos de orden social"*.[36] Es por esto que el ser humano, al compenetrarse dentro de una comunidad, se desarrolla de manera libre, siempre que respete las reglas éticas y sociales establecidas dentro de ella por lo que, al incumplir las reglas, estaría irrespetando a los demás miembros de su comunidad y, como consecuencia, generaría descensos en la consideración ajena, es decir, la pérdida de su buena reputación, de su honor.

2.2. EL DERECHO A LA INTIMIDAD

La intimidad es otro derecho fundamental y personal que se encuentra reconocido constitucionalmente, el cual debe ser respetado por el Estado y sus respectivos órganos.

[34] Berdugo Gómez de la Torre, Revisión del Contenido del Bien Jurídico Honor, Madrid: Anuario de Derecho Penal, p. 306.
[35] Joaquín Urías; Lecciones de Derecho de la Información, Madrid: Edit. TECNOS, 2003, p. 138.
[36] López Jacoiste; Intimidad, Honor e Imagen ante la Responsabilidad Civil Pág. 579; citado por Vidal Marín Tomás en El Derecho al Honor y su Protección desde la Constitución Española; Madrid, Edit. Centro de Estudios Políticos, 2001, p. 61.

Es a finales del siglo XIX, en Estados Unidos, donde germina la idea de privacidad (*privacy*) concepto que fue introducido inicialmente en la constitución estadounidense con el artículo publicado en el año 1890, en el *"Havard Law Review"* por Brandies y Warren, llamado "El derecho a ser dejado solo" *–The Rigth to be let alone–* que se convirtió en los primeros pasos para llegar a entender lo que ahora es privacidad. Tiene la finalidad de impedir la intromisión desmedida en la vida privada de los individuos, en sus pensamientos, sentimientos y emociones por parte de terceras personas.

El derecho a la intimidad busca siempre mantener al margen la vida privada de las personas, sin que medie ningún tipo de interferencias.

Incluso, el concepto de intimidad se ha visto relacionado, muchas de las veces, con el concepto de libertad ya que se ha llegado a definir a la libertad como *"el apacible disfrute de la independencia privada"*.[37]

Dar una adecuada definición a este derecho ha sido uno de los inconvenientes de la doctrina; en este sentido Romero Coloma plantea la intimidad es *"todo aquello que es propio y exclusivo de una persona, en cuyo uso y ejercicio se afirma en su propiedad y exclusividad, al mismo tiempo que se manifiesta como persona y como tal, sujeto de derechos. En definitiva, la intimidad es el derecho que concierne a la persona de ser ella que determine cuándo y hasta dónde quiere entrar en contacto con la sociedad"*.[38]

Para Fariñas Mantoni, la intimidad *"es aquella parte de la vida del hombre que se pretende vivir en soledad o compartida con unos pocos escogidos, frente a todos los demás,*

[37] Joaquín Urías, Op. Cit. Pág. 140.
[38] Romero Coloma; De los Bienes y Derechos de la Personalidad, Madrid: Edit. Lavel, 1985, p. 37.

consistente en hacer algo privado, hacer algo en privado o controlar el uso o difusión de los datos personales". [39]

Es por esto que el derecho a la intimidad, a más de proteger las injerencias exteriores por parte de terceros, también, busca que los individuos controlen los datos e informaciones privadas que afecten a su persona.

Para profundizar el estudio, se considera favorable realizar una descripción de lo que ha de entenderse por intimidad; así, el domicilio, la correspondencia, las conversaciones telefónicas o en privado, los papeles, los archivos, relaciones sexuales, informaciones bancarias, anomalías físicas y psíquicas, los secretos sobre el estado civil y filiación, las situaciones de angustia y dolor y las relaciones afectivas o sentimentales son considerados como espacios privados e íntimos de la persona. Es por tal motivo que, ciertos sujetos a pesar de estar enterados de la vida privada de una persona, no pueden por ética divulgar la información que manejan. Tal es el caso de los médicos, los abogados, los psicólogos, etc., igual caso es el de los sacerdotes, por el sigilo sacramental del cual están investidos.

2.2.1. Esfera Protegida por la Intimidad

Conociendo que el ser humano es un ser social por naturaleza, su vida intima se ve sujeta a la vida en sociedad; por lo tanto, el derecho a la intimidad busca que los individuos de una sociedad puedan desenvolverse de forma libre, sin que el resto de personas conozca los detalles de su vida privada. Lo que implica establecer la distinción entre la vida privada y la vida pública. En esta última, las personas aceptan que los demás conozcan su información, sus datos y ciertos detalles personales, mientras que, en la vida privada, las personas

[39] Fariñas Mantoni, El derecho a la Intimidad; citado por Vidal Marín Tomás; El Derecho al Honor y su Protección desde la Constitución Española, Op. Cit. p. 73.

guardan para sí la información y los detalles, manteniendo el control de lo que se puede saber. Lo complicado es determinar qué es privado y qué es público porque lo que para una persona debe permanecer dentro de lo íntimo, para la otra puede ser revelado con normalidad.

Es así como surge la teoría ***subjetiva*** y ***objetiva***; la primera trata de la libertad que posee cada individuo para determinar qué considera íntimo, es decir, lo que no quiere que conozcan los demás, frente a los datos que no le importan que sean divulgados; mientras que la segunda, se basa en la existencia de ciertos datos sociales que se consideran públicos y en otros, que son privados, lo que dependerá de cada persona, si quiere convertirlos en públicos

En definitiva, ambas teorías se basan en una concepción liberal y personalista, lo cual no resuelve el problema entre lo íntimo y lo público.

Por lo tanto, el derecho a la intimidad traza una línea entre lo que se considera público y lo que se considera privado; toma como punto de partida lo sociológico, lo moral, lo cultural y el conjunto de valores pertenecientes a los individuos que conforman una comunidad. Existe datos íntimos como la salud de una persona, pero no menos íntimos que su vida sexual y otros de carácter públicos como es el caso del maquillaje que usa una mujer u otros datos menos publicables como el gusto por cierta ropa íntima.

Es importante puntualizar, dentro del tema que existen personas que renuncian de forma específica a su intimidad; por ejemplo: una mujer que decide exhibir su cuerpo en revistas. Esta potestad solo la tiene el titular del derecho, el cual interviene para exponer parte de su vida íntima a la vida pública; pero, es necesario especificar que solo lo que el individuo desea divulgar debe ser popularizado, el resto no.

Sin embargo, muchas de las veces, la renuncia a este derecho no es puntual sino implícita en los propios actos; por ejemplo: una persona que comente de su vida extramatrimonial a su mejor amiga. Es, sin duda, un riesgo que corre el titular de que su dato íntimo sea conocido por el resto de personas que rodean la vida de su amiga; de esta manera, puede perder el control del número de personas que han sido parte de su secreto. Frete a este tipo de renuncia, existe otra, que es más amplia, que afecta a una gama de datos íntimos de la persona y se produce cuando esta decide llevar su vida a un campo público, tal es el caso de los artistas, cantantes y los famosos, en general. Por este motivo, se concibe un alto nivel de intromisión en su vida, pero no se puede suponer que se dé una renuncia total o absoluta de su derecho a la intimidad.

En definitiva, el derecho a la intimidad puede ser modificado por las decisiones de su titular, ya sea, por medio de una renuncia tácita o por aceptar nivel público dentro de su vida, o puede ser modificado por decisiones de la sociedad a través de la importancia pública de ciertos hechos de carácter privados, en los que no cabe renuncia absoluta a toda la intimidad.

2.3. DISTINCIÓN ENTRE EL DERECHO AL HONOR Y EL DERECHO A LA INTIMIDAD

Tanto el derecho a la intimidad y el derecho al honor, a pesar de ser reconocidos por nuestra Carta Magna como derechos fundamentales, presentan ciertas características propias, las mismas que son de valioso interés para lograr un mayor entendimiento entre uno y otro, es decir, resulta muy adecuada la distinción para verificar cómo funcionan.

- En principio el derecho al honor se ejerce en las relaciones sociales, mientras que el derecho a la intimidad es un derecho personalísimo, que se ejerce dentro de lo

privado, por lo que el concepto de intimidad y de honor no se sobreponen ni coinciden.

- El derecho al honor tiene por objeto resguardar a una persona de otras que procuren humillarla o repulsarla, mientras que el derecho a la intimidad se centra en proteger a las personas de las injerencias de terceros dentro de su vida familiar o íntima.
- El derecho al honor puede ser invocado por las personas jurídicas, quienes, también, gozan de derechos personales. El derecho a la intimidad solo puede ser solicitado por un ser humano ya que no cabe contar con la vida sexual de una empresa.
- Otra distinción que se puede establecer sobre estos dos derechos es con respecto al consentimiento; en lo que respecta al derecho a la intimidad, hay un aspecto de lo íntimo que aparece determinado por la sociedad, pero puede existir variaciones, producto del consentimiento de su titular. A diferencia, el derecho al honor no depende del consentimiento del titular, simplemente, es el desprestigio producido a una persona por la conducta constitucionalmente reprochable.
- Con respecto a la intención, en el derecho a la intimidad la intención puede ser buena o mala, ella no depende de eso porque solo la simple divulgación de la noticia privada atenta contra este derecho; en cambio, en el derecho al honor, de la intención que asuma una persona, depende que información neutral se conviertan en deshonrosas.

2.4. EL DERECHO A LA LIBERTAD DE INFORMACIÓN

Es preciso que, antes de conocer sobre este derecho, se realice un análisis de lo que es la información y su evolución dentro de nuestra sociedad.

La palabra información viene del latín "forma" y, como tal, la información ha sido catalogada como el conjunto de datos transmitidos desde una fuente emisora hasta una fuente receptora; pero, estos datos deben tener sentido para que gocen de un significado cognitivo.

No se puede concebir una sociedad democrática sin el libre acceso a la libertad de información. *"La posibilidad de investigar, recibir y difundir información es un derecho humano que ayuda a moldear al hombre en su dimensión social"*.[40]

La información llegó a poseer un gran auge en las últimas décadas del siglo XX por lo que la UNESCO publico un informe el 16 de agosto de 1976, en el que decía: *"Mientras que la comunicación interpersonal fue la única forma de comunicación humana, el derecho de la libertad de opinión era el único derecho de la comunicación. Más adelante con la invención de la imprenta se añadió el derecho a la libertad de expresión. Y más tarde aún, a medida que se desarrollaban los medios de comunicación, el derecho a buscar, recibir e impartir información pasó a ser la preocupación fundamental"*.[41]

Es, de esta manera, cómo la expresión del hombre se convirtió en pilar fundamental de desarrollo, pues, cada cultura ha crecido a través de registros lingüísticos y grafológicos que han permitido mantener costumbres y alcanzar un alto nivel cultural, económico y político.

Así, grandes pensadores como Hegel consideraba que: *"para que una cultura pudiera desarrollar un pensamiento filosófico era necesario que en el contexto social se tuviera la*

[40] Rodríguez Villafañe "Periodismo e Información judicial en Argentina", Revista Contribuciones, Buenos Aires, p. 63.
[41] UNESCO; Informe 19c/93 de 16 de agosto de 1976, p. 56.

libertad de expresión como la facultad humana que permita el desarrollo del pensamiento".[42]

Jurídicamente, el desarrollo de la libertad de expresión se inicia con el Código de Manú, que consagra, por primera vez, la libertad de pensamiento, pero, con el desarrollo del pergamino y de las técnicas de escritura, se dio grandes limitaciones a éste derecho, debido a que atentaba contra los poderes políticos constituidos por la monarquía. En Roma, la libertad de expresión llegó a ser censurada ya que tan solo las personas consideradas como ciudadanos romanos podían hacer uso de la misma.

Más tarde, en el mundo oriental, la información tuvo su auge con el papel y la imprenta, y posteriormente, con el nacimiento del industrialismo se dio paso a un proceso de socialización de los derechos fundamentales, de tal manera, que el individuo dejó de ser la médula de atención; el foco de importancia se mudó a la colectividad.

El reconocimiento de la importancia de la información se generó con la declaración de los derechos humanos en 1948; aquí, la libertad de expresión se convirtió en un derecho reconocido constitucionalmente; el artículo 19 de éste cuerpo legal sostiene: "*Todo individuo tiene derecho a la libertad de opinión y expresión; este derecho incluye el de no ser molestado a casusa de sus opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".*[43]

De esta manera, la libertad de opinión y expresión fue reconocida a nivel mundial y, en nuestro País, no existió excepción alguna ya que la Constitución Política actual la registra dentro de su artículo 66, numeral 6, la cual manifiesta que reconoce y garantiza a las

[42] Hegel; W.G.F.; Lecciones Sobre la Historia de la Filosofía; p. 52/ 56. Citado por Carlos Márquez Escobar, El Delito Informático, Bogotá, Edit. LEYER, 1999, p. 26.

[43] Declaración Universal de los Derechos del Hombre, en la Constitución Política de Colombia; citado por Carlos Márquez Escobar, El delito Informático, Bogotá, Edit. LEYEER, 1999, p. 31.

personas*: "El derecho a opinar y expresar su pensamiento libremente y en todas sus formas y manifestaciones"*.

2.4.1. Libertad de Expresión y el Derecho a la Información

Generalmente, la libertad de expresión y la libertad de información han sido catalogadas como dos conceptos iguales ya que se sintetizan a través de una misma realidad práctica: la comunicación; pero, la doctrina distingue estos dos derechos. Tres son las teorías que delimitan la relación existente entre la libertad de expresión y la libertad de información:

a. Consentir que ambas componen un mismo derecho.
b. Comprender que ambas nacen de una misma base, pero se diferencian en cuanto al régimen jurídico de cada país.
c. Admitir que son dos derechos distintos.

En principio, se considera que la libertad de expresión abarca a la libertad de información, es decir, constituye la base de todo acto comunicativo posible, inclusive, se concibe a la libertad de información y al derecho a la comunicación como un área específica dentro de dicho derecho.

Sin embargo, con el desarrollo social, otros doctrinarios consideran que la libertad de información es diferente a la libertad de expresión, en cuanto al objeto de cada derecho, debido a que el primero protege la transmisión de datos y hechos ciertos, información veraz, mientras que el segundo, protege la emisión de juicios de valor y opiniones.

Se debe aclarar que pueden existir ambos derechos, siempre que estén expresados de manera específica en la constitución.

En nuestro País, la Constitución expresa dentro del artículo 66, numeral 6, que se reconocerá y se garantizará a las personas*: "el derecho a opinar y expresar su pensamiento libremente y en todas sus formas y manifestaciones"*.

Se Reconoce, de esta manera, que la libertad de expresión es un derecho fundamental inherente a todo ser humano, del cual emerge el Estado porque, como expresa el catedrático Joaquín Urías: *"Sin la libertad de expresión hubiera sido imposible terminar con el antiguo régimen y pasar a la primacía del Estado constitucional. En este sentido fue un prius para el reconocimiento de muchos otros derechos"*.[44] Es un derecho que garantiza la libertad de opinión personal frente a las mediaciones del Estado.

En cuanto a la libertad de información, nuestra Carta Magna, también, hace referencia dentro de la sección tercera de la Comunicación e Información, en su artículo 18 numeral 1, que sostiene: *"Todas las personas, en forma individual o colectiva, tienen derecho a:*

Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y proceso de interés general y con responsabilidad ulterior".[45]

Nuestra Carta Magna garantiza es una comunicación libre dentro de la sociedad, donde exista un intercambio de noticias y que cualquier ciudadano espontáneamente conozca la información emitida por los distintos medios de comunicación y se forme su propia opinión, lo que posibilitará la existencia de una verdadera soberanía popular. Cabe manifestar, también, que la información, para que cumpla con las finalidades que establece la Constitución, tiene que ser veraz; serán los Tribunales de Justicia los encargados de probar si los hechos descritos realmente existieron o no.

[44] Lecciones de Derecho de la Información, Op. Cit. p. 53.
[45] Constitución de la República del Ecuador, Op. Cit. p. 21.

2.4.2. La Obtención Legítima de Información

La información se transmite en tres fases: la recolección de los datos, su trasformación en información por el receptor y su difusión o esparcimiento.

Para que se cumpla con la misión de nuestra Constitución, se debe, proteger las tres fases de la información, destacando que la fase de mayor importancia es la publicación porque es aquí donde se consume el derecho y se llega a determinar si la información afecta o no a los demás derechos.

Ahora bien, es preciso expresar que tampoco cabe que, en la fase de obtención de información, una persona adquiera información privada o secreta y que la Constitución lo permita, ya que se estaría violentando con los derechos garantizados en ella por lo que, dentro del derecho a la libre expresión y libre información hay que tener presente el hecho de obtener información de manera veraz y legítima.

Es importante reconocer que toda persona es capaz de recopilar información acerca de algún suceso; pero, en realidad, esta tarea constantemente la realiza el periodista como parte de su labor. El periodista tiene derecho a investigar y recibir información de cualquier persona, siempre y cuando, esta se adquiera lícitamente, es decir, que no se haya cometido ningún delito ya que el derecho de obtener información no le exime del cumplimiento de la ley. Es por esto, que ninguna persona que recopile información no puede exigir a otra que posee el conocimiento, que lo suministre, ni cabe que la obtenga por medio de amenazas, de interferencias telefónicas, de incautación de documentos privados o por cualquier otra forma antijurídica.

Además, el ciudadano, que conozca que un periodista está averiguando sobre su vida, no puede impedir dicha investigación tan solo debe esperar la publicación de la información

para poder reclamar alguna lesión en contra de su derecho a la intimidad o de su derecho al honor.

La obtención de información de los poderes públicos resulta más eminente, ya que es imprescindible conocer sobre el funcionamiento de las instituciones del Estado. Por tanto, al momento de adquirir información con respecto al Estado, este debe facilitar la libertad de investigación sobre asuntos públicos e, incluso, tiene que informar periódicamente sus actividades. Este es un derecho que puede ser ejercido por los medios de comunicación al igual que por cualquier ciudadano.

De otra parte, hay ciertos intereses constitucionalmente protegidos; así por ejemplo, el derecho a la intimidad, que predomina frente al derecho de información. Por lo tanto, al momento de acceder a informaciones públicas que perturben la intimidad de terceras personas, se estaría irrespetado un derecho superior establecido en nuestra Constitución. Es así, como la libertad de información se ve limitada por ciertos valores e intereses reconocidos constitucionalmente como primordiales.

2.5. CONFLICTO ENTRE DERECHOS: EL DERECHO AL HONOR, LA INTIMIDAD Y LOS LÍMITES DE LA LIBERTAD DE INFORMACIÓN

Al ser los derechos fundamentales inalterables en su contenido constitucional y al estar amparados por todos los poderes del Estado, parecería ser que no existe conflicto alguno entre estos, pero, en la mayoría de las ocasiones esto no es así.

En principio podría explicarse que los derechos fundamentales funcionan en conjunto de forma perfecta debido a que cada derecho encaja exactamente en un conflicto y por esto no

puede concurrir dos derechos a la vez para regular una misma actividad, es decir, los derechos jamás colisionan entre sí.

Lo descrito sería una visión constitucional ideal acerca de los derechos fundamentales; pero, como casi siempre ocurre, la realidad es muy diferente. Se genera, por lo tanto, auténticos conflictos normativos en el que resulta muy oscuro reconocer y proteger dos derechos a la vez; es aquí donde nos encontraos en un conflicto de derechos. Los conflictos más frecuentes y los que en nuestro estudio importan se originan entre la libertad de información y los derechos al honor y la intimidad.

Así, si una persona ha reunido información de otra y se le recrimina que ha vulnerado el derecho al honor y a la intimidad, se deberá demostrar que la información almacenada es veraz, que no contiene ofensas, que la obtuvo de manera legítima y que es relevante públicamente, es decir, que tiene trascendencia para el desarrollo social; de esta manera, no existiría conflicto alguno con la libertad de expresión y el derecho al honor y la intimidad.

La mayoría de conflictos se solucionan a través de la verificación del cumplimiento de cada uno de los requisitos que conciernen a cada derecho. Es por esto que se dice que la libertad de información ha de ocuparse solamente de temas públicamente importantes; esto porque se quiere dar protección a la intimidad, puesto que lo íntimo es lo que no es públicamente importante. De igual manera, al indicar que la información obtenida debe ser veraz e indiscutible es porque se busca proteger el honor y evitar el descenso de la consideración ajena a través de informaciones calumniosas o injuriosas.

Sin embargo, existen situaciones en las que dos derechos, a pesar de reunir sus requisitos, se enfrentan entre sí porque la protección de uno implica el sacrificio del otro. En este caso, hay que tener presente la importancia de ambos derechos y analizar las circunstancias

de cada caso y valorar los perjuicios que se ha ocasionado en cada derecho para llegar a una resolución razonada y constitucional.

No se puede hablar que un derecho es superior a otro, es decir, que el derecho a la intimidad y el derecho al honor son superiores al derecho de libertad de expresión o a la libertad de información; lo que se trata de deducir es que cada derecho debe ser respetado y considerado con igual grado de importancia dentro del marco Constitucional; y que todo derecho debe ser minuciosamente valorado antes de decidir qué derecho será sacrificado.

Para concluir con lo que respecta al conflicto entre derechos es importante señalar que la libertad de información centra su objetivo en la veracidad para evitar lesiones en el honor; pero, esta veracidad siempre estará supeditada a la actividad del informador y su profesionalismo, es decir, puede suceder que una información veraz resulte luego ser distinta a la verdad judicial. Así, si una persona ha sido acusada de asesinar a un allegado y esta noticia, luego, es desmentida, en juicio, se estaría lesionando el honor de esa persona. Lo que se trata de explicar es que para llegar a comprobar la veracidad, muchas de las veces, es necesario lesionar el derecho al honor de las personas.

En lo que respecta a la intimidad, esta es muy distinta al honor; aquí, lo que importa no es la veracidad, sino si la información es notable o no, es decir, si afecta a lo íntimo o no, por lo que la única forma legítima de resolver el conflicto es a través de una investigación exhaustiva de la posible ofensa a la intimidad por parte del informador; no importa si la información es verdadera ni tampoco si se ha afectado al honor porque, si se llega a comprobar que el derecho a la intimidad ha sido lesionado, es innecesaria tal consideración y lo único que queda por hacer es proveerle de razón al afectado.

2.6. LÍMITES DE LA LIBERTAD DE INFORMACIÓN

La información en nuestros días ha alcanzado un gran adelanto y esto se debe al inmenso desarrollo tecnológico, que ha permitido al ser humano vivir de forma diferente, puesto que la comunicación, en nuestros días, es inmediata y precisa. Es normal charlar con el amigo de clases, que radica en otro continente, por medio de la red e, incluso, enviarle postales de felicitación o cartas confidenciales por medio del correo electrónico. Todas estas situaciones en las que intercambiamos parte de nuestra vida merecen tener un toque de seguridad y privacidad, frente a la intromisión de terceras personas. Es así como se ha impuesto ciertos limitantes a la libertad de información con el objetivo de impedir que se vulneren las prohibiciones establecidas en nuestro ordenamiento jurídico. Evidentemente, dentro de la libertad de expresión y de información, se debe exceptuar de manera absoluta los insultos ya que nuestra Constitución no protege las informaciones de tipo injurioso.

La razón de la existencia de un elemento informativo es la de anunciar o denunciar irregularidades teniendo en mira un solo objetivo que es el de mantener a los ciudadanos, miembros de un Estado, totalmente informados de lo que ocurre dentro de su marco social; pero, cuando la libertad de expresión o la información se fusionan con la opinión, se generan los inconvenientes.

Puede, muchas de las veces, que la información vertida sea veraz y que se cuente, incluso, con pruebas contundentes de lo narrado o que la información sea relevante públicamente; sin embargo, si en la información se ha difundido opiniones injuriosas no puede hablarse de libertad de expresión o información. Tanto informadores como editores pueden presentar, dentro de sus informaciones, criterios de valoración sobre cualquier conducta y esta valoración puede ser negativa como positiva; pero, en ningún momento, se aprueba insultos

o ponencias injuriosas que deshonren o desacrediten a una persona. Con los insultos, no hay libertad de información practicada de forma lícita.

Cabe manifestar que, cuando se habla de noticias insultantes, se prioriza la intención; así, el llamar a alguien ignorante o bestia implica una intención de descalificación. El uso de estos calificativos no pueden estar amparados por la libertad de información, incluso, si la persona, en realidad, carece de cultura. Además, si la noticia se encuentra plagada de expresiones que degradan a una persona, más que anunciar una situación de importancia social, se estaría lesionando el derecho al honor y es, aquí, donde cabe explicar la Doctrina de la Real Malicia, que tuvo su origen en los Estados Unidos, en el año de 1964, a partir de conocido caso: "New York Time Vs Sullivan". Con esta teoría, se ha pretendido dar solución al antagonismo de tres derechos reconocidos en nuestra Constitución como fundamentales: la honra del agraviado, la libertad de expresión y el derecho que tienen la sociedad de una información veraz[46]. Por lo tanto, el comunicador o articulista que haya cimentado una información que ofenda a un funcionario público, a un particular o a una figura pública será responsabilizado por dicho agravio; siempre y cuando, se llegue a comprobar que el periodista conocía de la falsedad de la información o que manejó informaciones secretas al conocimiento público, con dolo y descuido temerario en la comprobación de la verdad.

Dicha comprobación la tiene que realizar la persona que se sienta ofendida, es decir, en esta doctrina, se impone la carga de la prueba a quien lo alegue; por lo tanto, los periodistas que han sido acusados penalmente o civilmente por perjuicios ocasionados por noticias,

[46] Es necesario hacer una distinción entre verdad y veracidad; la primera es la adhesión del entendimiento humano con la realidad, cuando una persona tiene la verdad es porque no existe duda alguna sobre lo que conoce o cree conocer, mientras que la segunda es la simple creencia de que estamos en posición la verdad. La certeza no necesariamente coincide con la verdad.

crónicas, opiniones o informaciones inexistentes serán inculpados el momento que los agraviados o demandantes prueben que dichas noticias o informaciones estaban emitidas de manera imprudente y a sabiendas de su falsedad.

Si el periodista actúa a sabiendas de la falsedad de la información, se incurre en un dolo directo, es decir, el periodista actúa con total conciencia y voluntad de lesionar el honor de la persona hasta llegar a cometer el delito de injuria.

Si se emite una información sin la investigación necesaria, se estaría frente a un dolo eventual, que constituye la frontera entre el dolo y la culpa consciente; aquí se produce el "no no querer" que se vuelve querer según el análisis de la doctrina alemana. "*En el dolo eventual no hay una aceptación del resultado como tal, sino su aceptación como probabilidad o posibilidad"*.[47]

Al analizar este aspecto, es necesario precisar que, dentro de la Doctrina de la Real Malicia, existe elementos, que proporcionan un mayor conocimiento.

- La información debe ser equivocada, con lo que se lesiona el derecho al honor y a la intimidad de una persona.
- La persona lesionada o perjudicada, que goce de connotación pública: Sujeto Pasivo.
- La persona que comunique o el periodista: Sujeto activo.
- El conocimiento de la falsedad de la noticia y el descuido temerario por parte del periodista de conocer si era o no verdadera la información publicada: Elemento subjetivo del tipo.

[47] Raúl Zaffaroni, Manual de Derecho Penal Parte General, Buenos Aires, Edit. Sociedad Anónima Editora, Comercial, Industrial y Financiara, 2001, p. 416.

- La inversión de la carga de la prueba; se invierte el *onus probandi* correspondiéndole a la figura pública, en este caso, probar que la información era falsa y que el periodista conocía de dicha falsedad.

Estos son los requisitos de la Real Malicia, de ahí que el periodista, al no estar seguro de la información que va a emitir, preferiblemente, debería utilizar un tiempo prudencial para averiguar e investigar sobre cualquier accionar del funcionario público, figura pública o particular con connotación pública, evitando responsabilizarse por la inexactitud o falsedad de lo que se publica.

Al tener claridad sobre el actuar correcto de los funcionarios públicos, figuras públicas o particulares con connotación pública, respecto de las informaciones falsas vertidas en su contra, es necesario manifestar cual debe ser el proceder de los simples ciudadanos. Estos tienen derecho a presentar las demandas que consideren pertinentes, con el fin de acreditar únicamente la falsedad o la negligencia impartida por el periodista. Esto se basa en la debilidad de los particulares frente a las personas con vínculos públicos ya que, estos últimos, tienen la posibilidad de acceder a los medios de comunicación para defender su honor frente a la sociedad.

De esta manera, no se puede hablar de un derecho a la información de forma total ya que siempre tiene que limitarse a la veracidad de lo que se informa para no menoscabar otros derechos como el honor o la intimidad. Toda persona tiene derecho a una vida intima que no solo comprende su esfera doméstica, constituida por la familia y los amigos, sino otros aspectos que deben permanecer en reserva frente a la indiscreción ajena.

Otro límite importante, dentro del derecho a la libertad de información, que merece un interés especial, es la protección a la infancia. Aunque no se le trate a la protección infantil

como un derecho fundamental, nuestra Constitución dentro de la sección V, sobre las niñas, niños y adolescentes, en su artículo 46, numeral 7, sostiene:

> *"El Estado adoptará, entre otras, las siguientes medidas que aseguren a las niñas, niños y adolecentes:*
> *Protección frente a la influencia de programas o mensajes, difundidos a través de cualquier medio, que promuevan la violencia o la discriminación racial o de género. Las políticas públicas de comunicación priorizarán su educación y el respeto a sus derechos de imagen, integridad y los demás específicos a su edad. Se establecerán limitaciones y sanciones para hacer efectivos estos derechos.* [48]

Como se puede observar, la Constitución da una especial prioridad a la infancia frente a la influencia de ciertos programas o medios de comunicación que impartan noticias violentas o discriminatorias puesto que la etapa infantil implica un proceso de creación personal en el que el niño o niña va madurando su personalidad y conciencia. De este modo, es coherente sostener que las influencias externas provocadas por cualquier medio informativo pueden atentar en contra del desarrollo de la personalidad del niño.

Las informaciones referidas a un menor en las que se divulgue hechos propios o de sus familiares y que impliquen una connotación negativa o perjudiquen a su crecimiento social, constituyen lesiones a su integridad, por lo que la información estaría atentado el desarrollo integral de los niños o de las niñas. Es por tal motivo, que nuestra Constitución busca restringir ciertas informaciones tendientes a desorientar la formación del niño, con sanciones, y, más aún, si las informaciones atentan en contra de su honor o de su intimidad.

[48] Constitución de la República del Ecuador, Op. Cit. p. 31.

CAPÍTULO III

DELITOS QUE VIOLAN LA INTIMIDAD: ANÁLISIS DEL ARTÍCULO 202.1 y 202.2 DEL CÓDIGO PENAL ECUATORIANO

CAPITULO III

3. DELITOS QUE VIOLAN LA INTIMIDAD: ANÁLISIS DEL ARTÍCULO 202.1 y 202.2 DEL CÓDIGO PENAL ECUATORIANO.

Dentro del conjunto de delitos protegidos por nuestro Código Penal ecuatoriano, encontramos en el Capítulo V: De Los Delitos Contra La Inviolabilidad Del Secreto, algunas nuevas conductas, las que no se encontraban tipificadas en el anterior Código Penal. Este nuevo conjunto de normas fue incorporado a partir de la creación y aprobación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos dentro del Registro Oficial número 557 del 17 de abril del 2002. Esta Ley en su primer artículo regula: *"los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas"*. [49] Y es que, sin lugar a dudas, en la actualidad todo tipo de contrato se lo puede efectuar por medios electrónicos; es así, que se adquieren títulos valores sin necesidad de poseerlos físicamente e, inclusive, se efectúa una compraventa de bienes y servicios y se genera una prueba legal valida.

Esta ley considera a los mensajes de datos como si fueran documentos escritos; además de reconocer su confidencialidad y discreción, la firma electrónica, también, es reconocida con los mismos efectos de la firma manuscrita, siempre que cumpla con los requisitos establecidos en esta ley.

Es por esta razón que nuestro Código Penal ha sufrido reformas fructíferas, logrando tipificar las infracciones informáticas ejecutadas en contra de claves o sistemas de

[49] Cámara de Comercio de Quito; Boletín Jurídico número 195, de marzo del 2002.

seguridad para acceder o destruir información protegida o secreta, ya sea, por medio de la apropiación ilícita, de la obtención no autorizada de información o por medio de la falsificación electrónica.

El Código Penal ecuatoriano expresa dentro del artículo 202.1, sobre los delitos contra la información protegida, lo siguiente:

> *El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.*
>
> *Sí la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.*
>
> *La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.*
>
> *Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, estas serán sancionadas con pena de reclusión menor de seis meses a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.* [50]

Para hacer un análisis es preciso definir los elementos estructurales del tipo.

Sujeto Activo: Es cualquier persona que puede llegar a cometer este tipo de delitos es indeterminada; es decir, cualquier persona es capaz de realizar el delito. Pero, nuestro Código hace hincapié en que, si los autores de estos injustos son personas encargadas de la

[50] Código Penal Ecuatoriano; Op. Cit. p. 79 y 80.

custodia o la utilización de la información, la pena aumentará y será de seis meses a nueve años y la multa, de dos a diez mil dólares.

Sujeto Pasivo: Es la persona perjudicada con la divulgación de la información protegida.

El Objeto Material del Tipo: Es la información protegida, secreta o privada. Entendiendo la palabra secreto como *"todo aquello que se mantiene ignorado del conocimiento de los demás y cuyo poseedor lo debe conservar en esa situación, ya sea por decisión propia o por exigencia legal".*[51]

El Verbo Rector: Es la palabra Violentare ya que la persona que violenta algo lo hace sin la autorización del dueño o a través de medios forzosos. En este caso, el generador del ilícito violenta claves o sistemas de seguridad que son métodos de protección de archivos, de bases de datos o software.

El Fin del Injusto: Consiste en vulnerar la seguridad, el secreto, la confidencialidad y la reserva. En definitiva, es el acceder u obtener la información protegida.

El Modus Operandi: Es la ejecución a través del medio informático, electrónico o afín. Entendiendo siempre que la electrónica *"es la ciencia que estudia dispositivos basados en el movimiento de los electrones libres en el vacío, gases o semiconductores, cuando dichos electrones están sometidos a la acción de los campos electromagnéticos".*[52]

Cabe hacer alusión que, a medida que, la infracción se va agravando, la pena y la multa, también, van ascendiendo. Así, el segundo inciso expresa que si la información se refiere a asuntos de seguridad nacional o secretos comerciales o industriales, la pena será de uno a

[51] Jorge Zavala Baquerizo, Delitos Contra la Propiedad; Tomo II, Guayaquil: Edit. Edino, 1998, p. 43.
[52] Efraín Torres Chaves, Breves Comentarios a la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos; Quito: Edit. Corporación de Estudios, 2006, p. 92.

tres años de prisión y la multa, de mil a mil quinientos dólares ya que los asuntos de seguridad nacional hacen mención a la soberanía, tanto interna como externa, de la República.

En cuanto al penúltimo inciso, el artículo se refiere al uso ilícito de la información obtenida que hace el autor del injusto. Aquí, la divulgación o la utilización de la información secreta es lo que predomina como núcleos del tipo ya que divulgar es publicar o poner al conocimiento de los demás la información; y utilizar sería emplear la información para algún fin determinado.

Y, por último, el artículo en mención expresa que existirá mayor pena y multa, si la información secreta, es divulgada o utilizada de manera fraudulenta por personas encargadas de manera legítima de la información.

Sin duda, a estos delitos los podemos llamar informáticos; puesto que el objeto material del injusto es la información y, en este caso, la información debe ser secreta. Además, los medios de comisión de este ilícito son informáticos porque para que exista divulgación es necesario de intermediarios que, en este caso, serían las redes de cómputo, la internet, etc. En cambio, el artículo 202.2 de nuestro Código Penal expresa lo siguiente: *"La persona o personas que obtuvieren información sobre datos personales, a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años o multa de mil a dos mil dólares de los Estados Unidos de Norteamérica"*[53].

[53] Código Penal Ecuatoriano, Op. Cit. p. 80.

En lo que respecta al análisis de este artículo, se podría anotar que la información manipulada es de tipo personal, es decir, está en extrema vinculación con el derecho a la intimidad.

La Ley de Comercio Electrónico define a los datos personales como aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley. Con lo que manifiesta que los datos personales de un individuo pueden ser autorizados por la persona titular de la información o por cualquier organismo que así lo consienta. La obtención fraudulenta de la información es castigada con prisión de dos meses a dos años y multa de mil a dos mil dólares.

En la actualidad, con el desarrollo de los medios de comunicación, los datos personales se han visto afectados, tanto así, que se podría decir que se encuentran en una cuerda floja debido a que la nueva "sociedad de la información" abre múltiples caminos de acceso a datos que corresponden a una esfera íntima de las personas. Es por tal motivo, que cabe analizar la importancia que presenta el derecho a la intimidad dentro la internet.

3.1. EL DERECHO A LA INTIMIDAD EN LA INTERNET

La situación tecnológica, económica, social y jurídica ha sufrido grandes cambios dentro de una sociedad en la que la información es eje fundamental e, incluso, influye en los cambios que surgen dentro de las conductas jurídicas.

Lamentablemente, el nuevo fenómeno informático al que asistimos, con la presencia de la internet, se enfrenta con varias fluctuaciones jurídicas, producto de una realidad moderna que no es contemplada en la normativa actual. Por lo tanto, es necesario añadir cierta reglamentación que regule y equilibre el mundo real con el mundo virtual ya que el uso de

la internet implica riesgos que atentan contra el derecho a la intimidad, al manejar datos que, incluso, sin el consentimiento de los afectados pueden ser almacenados por terceros.

En el mundo moderno, tanto la intimidad como la protección de las comunicaciones, derechos reconocidos por nuestra Constitución , se ven inmersos en retos novedosos, fruto de que las nuevas tecnologías de la información que permiten no solo nuevas formas de comunicación, sino, también, ofrecen la posibilidad de interceptar las comunicaciones.

En relación con lo expresado, el profesor Álvarez Civantos señala: *"Hay veces en la que uno piensa perderse en un lugar en el que nadie pueda localizarle, sin dar más explicaciones. Esto que pudiera ser cosa fácil, hoy día puede calificarse de prácticamente imposible, aún cuando creamos que no le hemos comentado a nadie nuestro paradero. Más allá de nuestra familia, novia o amigos de confianza, siempre hay alguien que conoce donde estamos, aunque nosotros no seamos conscientes de ello".* [54] Según el profesor Álvarez Civantos, el banco sería una de esas personas a que no le hemos expresado nuestro destino, pero que, sin embargo, lo conocen por varias razones ajenas a nuestra voluntad. Afirma, además: *"Sea cual fuere el lugar del mundo en el que nos encontremos nuestro banco conocerá nuestra situación desde el mismo momento en el que utilicemos nuestra tarjeta de crédito, medio de pago que más que usual se ha convertido en imprescindible compañero de viaje. Al hacer un cargo con nuestra tarjeta, nuestro banco conocerá no solo el lugar del mundo en el que nos encontramos, sino, también, lo que hacemos; eso sí, nosotros seguiremos creyendo que nadie lo sabe".* [55]

[54] Oscar José Álvarez Civantos, Normas para la Implantación de una Eficaz Protección de Datos de Carácter Personal en Empresas y Entidades, Granada: Edit. Comares, 2001, p. 1-3.
[55] Ibídem.

Y, en efecto, nuestro banco es una entidad que conoce nuestra vida íntima más que nuestros propios amigos o familiares, puesto que sabe lo que nos agrada comprar y en donde lo adquirimos; sabe qué tipo de revista nos agrada cada vez que nos suscribimos, a qué escuela van nuestros hijos; conoce si nos agrada realizar o no algún ejercicio, si tenemos deudas; en fin, conoce una multiplicidad de situaciones que tienen implicación con lo económico.

A esta realidad no solo se suma el banco, pues existen otras entidades a las que cedemos nuestros datos sin darnos cuenta. Así pues, al momento que pasamos a formar parte de una cuenta de correo electrónico tenemos que ingresar, de manera previa, nuestros datos personales como nombres y apellidos, dirección, país en el que vivimos o nacimos, profesión, edad, aficiones, hobbies, etc., incluso, muchas ocasiones, llenamos formularios para formar parte de diversas páginas web y, al no leer todas las cláusulas del contrato por falta de tiempo y previsión, aceptamos que nuestros datos sean tratados con fines publicitarios o cedidos a terceras personas o empresas.

De esta manera, tan ingenua, nos convencemos que adquirimos un servicio gratuito y provechoso, sin percataros que estamos dejando nuestra vida privada al alcance de cualquier persona, es decir, perdemos lo más valiosos que es nuestra intimidad y discreción, en esta época tecnológica donde más prudencia debemos tener en el uso de nuestros datos.

Por tal motivo, la Comisión Europea ha publicado en marzo del 2004[56] los resultados de sus últimas encuestas sobre la protección de datos en la Unión Europea, centrándose en la visión que los ciudadanos europeos tienen sobre la protección de datos personales por

[56] Valentín Carascosa López, "Memorias del X Congreso Iberoamericano de Derecho e Informática" Op. Cit. p. 225.

organizaciones, tanto públicas como privadas; concluyendo que el más del 60% de europeos se manifiestan preocupados por la protección de su privacidad. Además, centran su interés en el deseo de ser informados sobre el tratamiento de sus datos personales y las cesiones que de los mismos se pueden realizar.

No cabe duda que necesitamos de la creación de ciertas normas que permitan el control del uso de nuestros datos personales por terceras personas, empresas o corporaciones. Para hacer respetar el derecho a la intimidad y a la privacidad que tiene toda persona.

3.2.FORMAS DE VIOLAR EL DERECHO A LA INTIMIDAD EN LA INTERNET

La Carta de Derechos Fundamentales de la Unión Europea firmada en Niza, el 7 de diciembre del 2000, ha incorporado dentro de sus artículos, el derecho a la protección de datos de carácter personal. Con ello, la privacidad ha marcado territorio dentro de los derechos humanos ya que, al ser un derecho inherente a la persona, necesita de un marco legislativo que lo respalde. Así, la profesora Llácer Matacás explica que: *"El tratamiento informático de aspectos parciales de nuestra persona, como los gustos y las aficiones, los hábitos de comprar o el poder adquisitivo, es una fuente de información que, en manos de terceros, puede perjudicar el libre desarrollo de la personalidad o provocar la denegación de derechos"*. [57]

Por lo tanto, se busca crear un marco de seguridad en el cual se proteja al conjunto de datos personales que, por sus características y al ser tratados por medios informáticos, pueden llegar a proyectar el perfil de una persona y lesionar sus derechos.

[57] María Rosa Llácer Matacás, "La Protección de los Datos Personales en Internet", en La regulación del comercio electrónico, Madrid: Edit. Dikynson, 2003, p. 158.

En la actualidad, existen en la internet, mecanismos con los cuales se puede violar el derecho a la privacidad; estos recogen información del usuario con su aprobación o sin ella. Hay, por tal motivo, que distinguir entre las herramientas que recogen la información del usuario con su consentimiento de las invisibles, que recogen la información sin él.

Las Herramientas Visibles de Datos

Estas aplicaciones de la internet de las que se puede extraer los datos de un usuario con su voluntad son las siguientes:

- Los grupos de noticias.
- El correo electrónico.
- Las guías web.
- Los formularios y cuestionarios.

1. Los Grupos de Noticias: Conocidos, también, como “news” o como “newsgroups”, permiten a los usuarios de la internet intercambiar, de manera voluntaria, sus ponencias o criterios sobre temas diversos, con personas de todo el mundo. En definitiva, son grupos de personas que envían y reciben mensajes de otros con la finalidad de expresar sus opiniones.

Generalmente, la información de las personas que forman parte de estos grupos de noticias es capturada por los distintos identificadores de los usuarios: nombre, contraseña, dirección electrónica, grupo de noticias e, incluso, a través de los mensajes que ha enviado, los cuales permanecen guardados durante meses.

2. El Correo Electrónico (e-mail): Es la forma de comunicación que ha suplantado a la correspondencia postal. El correo electrónico es una forma de recibir y enviar mensajes entre los diversos usuarios de la internet de manera más rápida y económica; los usuarios, únicamente, tienen que adquirir una dirección de correo que será exclusiva para cada individuo.

No cabe duda que el *e-mail* se ha convertido en una herramienta de comercialización a nivel mundial puesto que, en múltiples ocasiones, nos encontramos con correos de personas desconocidas, que presentan anuncios y publicidad. A estos mensajes, generalmente, se los conoce como "correo basura", "chatarra" o "spam", ya que son enviados de manera permanente y paulatina.

Estos correos basura nacieron hace trece años con Laurence Canter y su esposa y, desde su creación, han causado más de 200.000 mil dólares de pérdidas anuales en recursos y tiempo. Más de 8.700 millones de correos electrónicos no personalizados (correos basura) han sido enviados a diario por la red el año pasado; lo que supone entre el 45% y el 60% de los *emails* enviados, cada día, en todo el mundo.

En la actualidad, se requiere de mecanismos para frenar los *spams;* así, en España, el frente anti-spam que ésta representado por la Ley de Servicios de la Sociedad de la Información –LSSI–[58] ha incorporado multas graves entre 30.000 y 150.000 euros por el envío de más de tres comunicaciones comerciales no solicitadas en un año. Esta normativa basa sus argumentos en el principio de "consentimiento previo" y de que es ilícito camuflar o

[58] http//europea.eu.int/comn/internal_market/en/dataprot/index.htm.

disimular la identidad del emisor; además, de que todos los correos deben mencionar una dirección de respuesta válida, donde el abonado pueda oponerse al envío de mensajes posteriores. Asimismo, todos los mensajes enviados a direcciones sin el consentimiento de su titular se consideran ilegales y cada Estado miembro de este frente anti-spam puede implantar las multas que considere pertinentes.

Lo que se busca, sin duda, es erradicar estos correos chatarra desde su origen ya que podría perjudicar al *email* que es el motor de la internet e, incluso, un gran número de usuarios se verán obligados a abandonar el correo electrónico y a sus beneficios debido a los mensajes basura.

3. Las Guías Web: Son páginas *web* que se dedican a difundir, por medio de la red, guías de alumnos profesionales miembros de asociaciones o de cualquier persona; lo que preocupa es el tratamiento que se den a los datos que forman parte de estas guías y que, sin duda, pertenecen a lo privado de cada persona ya que a estas guías *web* se puede acceder sin mayor inconveniente.

4. Los Formularios de la Internet: Un gran número de personas, todos los días, llenan formularios para formar parte de ciertas páginas *web* por lo que dan a conocer todos sus datos personales; así por ejemplo: los portales de internet que ofrecen servicios gratuitos y no emiten una política clara de protección de los datos personales que han sido suministrados por el usuario.

A. Herramientas Invisibles de Datos

Al referirnos a las herramientas invisibles de datos hacemos alusión a todos aquellos datos personales que, sin la aprobación del usuario, han sido arrebatados por la red. Las formas de retener estos datos son las siguientes:

- Los datos de conexión o archivos LOG.
- Las Cookies.

1. Los Datos de Conexión o Archivos LOG: Se generan cuando el proveedor de acceso al internet hace un uso no deseado de "los archivos log", los mismos que muestran: dirección IP del emisor, dirección IP del destinatario; fecha, hora y duración del servicio, y tipo de servicio. Las personas que hacen uso de estos archivos almacenan automáticamente los mensajes enviados, perdiendo, de esta forma, la confidencialidad de los mismos.

"Los 'archivos log' en posesión del proveedor de acceso constituyen, por tanto, un yacimiento de datos indirectamente nominativos que genera importantes problemas de protección de datos de carácter personal, en la medida en que internet permite pasar de la prospección en masa a la prospección orientada llamada 'one to one', es decir, directamente adaptada al perfil del comportamiento de una personas.".[59]

2. Las Cookies: Son escrituras que se acumulan de forma temporal en la memoria del disco duro del ordenador del usuario cuando este accede a distintas páginas *web* por lo que se lleva un margen de control sobre las conexiones que tiene un individuo, durante un margen de tiempo, mostrando, de esta manera, información sobre los anuncios consultados,

[59] Carascosa López, Valentín; Memorias del X Congreso Iberoamericano de Derecho e Informática, Op. Cit. p. 232.

las rutinas de compras, las páginas visitadas, y todos los movimientos que por red puede realizar el internauta.

Es así, como el uso del internet implica la pérdida del derecho a la intimidad en la sociedad moderna actual, en nuestro País, no existe un marco normativo que regule este tipo de inseguridad jurídica. Existe una masa de usuarios de la red que, sin conocimiento alguno, incorporan sus datos personales, los mismos que pueden ser almacenados por terceras personas y utilizados de manera provechosa e ilícita.

Podemos palpar como la tecnología viola nuestra intimidad y reserva sin que existan mayores esfuerzos, en nuestro País, por frenar los riesgos inducidos a nuestros derechos, los cuales se encuentran protegidos por la Carta Magna.

Seguramente, para que exista una verdadera protección de la privacidad, se necesite no solo de la construcción de un marco legal, sino, también, de la participación consciente de los usuarios; así, por ejemplo, una forma de aplacar el *spam* podría ser las llamadas "*Listas Robinson"*, que son aquellas en las que pueden inscribirse las personas que no estén dispuestas a recibir publicidad vía *e-mail* o aquellas que, por el contrario, acepten a diario la publicidad en su correo. Es importante recordar que somos los ciudadanos los defensores de nuestros derechos; por lo tanto, la responsabilidad se encuentra en nuestras acciones. Debemos ser cautelosos a la hora de suministrar datos dentro de la red y más todavía, si lo que queremos es que se proteja nuestra intimidad.

Además, es conveniente que los mensajes de texto no guarden información trascendental ya que a través de *softwars* de búsqueda, se puede acceder a esta información y violar el derecho al secreto de las comunicaciones, que se encuentra protegido como un derecho

independiente en nuestra Constitución, dentro del Capítulo Sexto, sobre los Derechos de Libertad en el artículo 66, numeral 21, el mismo que expresa:

> Art. 66*: Se reconoce y garantizará a las personas:*
>
> *21.- El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; esta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto a los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otra forma de comunicación.*[60]

Pero no solo la Constitución ecuatoriana hace mención a este derecho, el Código Penal ecuatoriano, también, en su artículo 202.1, anteriormente analizado, nos da a conocer su vital importancia. Y es que se trata de un derecho emparentado con el de la intimidad por lo que las comunicaciones secretas, que sean víctimas de intervención ajena, serán reprimidas por el Estado.

Generalmente, el campo de acción de estos injustos se da a través de mecanismos como el correo, el teléfono, la internet, etc.

Con un ejemplo se puede comprender mejor la forma en la que se viola el secreto en los medios de comunicación:

> *En hora no determinada de la mañana del 23 de abril de 1990, el director del periódico La Crónica del Sur, hizo uso en su despacho de un aparato especialmente apto para captar y obtener la audición de comunicaciones practicadas por medio de telefonía móvil automática, y localizó así una conversación privada que en ese momento mantenía Juan Asensio Rodríguez, empresario, y Rafael Montoya Martínez, funcionario, hablando el primero desde un teléfono inalámbrico instalado en su automóvil detenido en las inmediaciones de las instalaciones del periódico; el acusado, al identificar las voces de quienes hablaban, dado que las conocía, procedió a copiar cuanto oía, no consta si lo hizo por escritura o*

[60] Constitución de la República del Ecuador, Op. Cit. p. 44.

> *utilizando una grabadora, con el propósito de publicar en la edición del periódico del día siguiente. Horas después, ya por la tarde, el acusado, aprovechando de que había localizado la frecuencia correspondiente al teléfono móvil de Juan Asensio, procedió con igual técnica a escuchar las comunicaciones que pudieran llevarse a cabo a través del mismo y, de este modo, captó una breve conversación, también privada, que Juan Asensio Rodríguez mantuvo con el periodista del diario Ideal, Miguel Ángel Blanco Martín, conversación que el acusado captó, también, con la idea de publicarla. Al día siguiente por decisión del acusado ambas conversaciones fueron publicadas en la página 7 del periódico La Crónica del Sur.* [61]

Como se puede apreciar, en este ejemplo, el autor del injusto lo hizo de manera voluntaria y consciente, es decir, con dolo porque, muchas veces, podemos escuchar una conversación sin que exista la voluntad de hacerlo sino de forma casual. Además, el guardar la conversación, ya sea con grabadora o por escrito, demuestra la intención de apropiarse de ella para, luego, utilizarla con fines beneficiosos para su periódico. Incluso, al tratarse de una información privada, se puede ver como se atenta contra el derecho a la intimidad de las personas, cuyas líneas telefónicas fueron captadas.

Sin duda, en este ejemplo, sí existe la violación al secreto de las comunicaciones puesto que este es algo ajeno y que no se puede divulgar. Aquí, se realizó la interceptación de la línea telefónica sin el consentimiento de sus titulares y la obtención de la información fue de manera voluntaria e ilícita.

Hay que tener presente que la interceptación de las comunicaciones se comete el momento que, por actos ilegítimos, la conversación se desvía hacia una tercera persona que, en este caso, sería el autor del injusto ya que es él, quien se apropia de la información secreta.

[61] Joaquín Urias, Lecciones de Derecho de la Información Op. Cit. pág. 86. (STC 34/1996)

Así, también, cuando una carta dirigida hacia una persona y, por equivocación, llega a manos de otra, la violación del secreto se da el momento en que la persona ajena a la información del documento lo abra para enterarse de su contenido. De igual manera, si una persona recibe una postal emitida por un extraño, la violación al secreto se da el momento que decida fotocopiarla.

El artículo 197 del Código Penal ecuatoriano hace insinuación a este tipo de conductas producidas por la violación de la correspondencia y manifiesta:

Art. 197:" Serán reprimidos con prisión de dos meses a un año y multa de seis a dieciséis dólares de los Estados Unidos de Norteamérica, los empleados o agentes del Gobierno y los del servicio de estafetas y telégrafos que hubieren abierto o suprimido cartas confiadas al correo, partes telegráficos, o que hubieren facilitado su apertura o supresión".[62]

Se puede apreciar, entonces, como nuestra ley protege la correspondencia y la información que se encuentra dentro de esta. Así como, también, castiga a las personas que, de manera voluntaria, facilitan su apertura o su supresión.

Cabe manifestar que no solo los empleados de las oficinas del correo, los agentes del gobierno o los empleados del servicio telegráfico pueden ser los autores de este tipo de delitos, sino cualquier persona que, de manera ilícita, despoje una carta confiada al correo.

En cuanto a la violación del secreto en las comunicaciones hay que tener presente que no solo se castiga la retención y exploración de los datos que tienen el carácter de secretos, sino, también, la difusión de estos. Para que el delito se consuma, es necesario que el autor sea consciente de que la información obtenida y divulgada ha sido adquirida de manera

[62] Código Penal, Op. Cit. p. 78.

ilegitima, es decir, el periodista debe difundir una información ajena y prohibida. Básicamente, es una información de la que no se cuenta con la autorización judicial ni con el consentimiento de los participantes.

3.3.LA INVIOLABILIDAD DE LOS DATOS DE CARÁCTER PERSONAL

El alcance del derecho a la intimidad no solo se centra en ser un derecho garantista, es decir, de defensa frente a cualquier invasión de la esfera privada, sino, también, es un derecho controlador de la creciente oleada de informaciones que se concentran en bancos de datos y que afectan a cada sujeto.

Esta ampliación del contenido de la intimidad ha generado un mayor control de las informaciones que se encuentran, hoy en día, dentro de los registro de las computadoras y que pueden estar al alcance de todos. Y es que, gracias al uso de la computadora, la sociedad informatizada pierde su privacidad ya que las bases de datos se van ligando a otras con lo que se obtiene información se con facilidad. Dicha información puede ser utilizada como herramienta a favor o en contra de la persona a la que le pertenece.

Una vez identificada a la intimidad con el concepto de vida privada, se puede comprender que la divulgación de cierta información y ciertas circunstancias personales no pueden, bajo ninguna causa, llegar al dominio de los demás, es decir, de lo público. Y es que la doctrina ha adoptado a la intimidad bajo dos dimensiones: como secreto y como libertad.

Concebida como secreto, atenta contra la intimidad todas aquellas divulgaciones ilegítimas de hechos de la vida privada o familiar, incluso, las investigaciones ilícitas de acontecimientos propios y reservados de una persona. Concebida como libertad, la

intimidad se centra en el derecho que tiene toda persona a tomar decisiones dentro de su vida íntima con el propósito de desarrollar su propia personalidad.

Cada persona, en su intimidad, puede actuar de la forma que desee, aun yendo en contra de la moral vigente, siempre y cuando, su actuar no sea calificado como ilícito por la ley penal o lesione los intereses jurídicos del Estado, de la sociedad o de los demás seres humanos.

En cuanto a la inviolabilidad, el derecho a la intimidad se ve ligado con el derecho fundamental al buen nombre y a la buena reputación y con el derecho a no ser molestado. La penetración en la vida privada, las averiguaciones ilícitas sobre esta y la curiosidad indiscreta son conductas injustas, pues, con estas maneras de actuar, se deduce agravio al patrimonio íntimo e, incluso, psicológico de las personas, atentando contra su dignidad.

El derecho a la intimidad, concebido como inviolable, impone tanto al Estado como a los demás miembros de una sociedad, un deber negativo, que se sustenta en abstenerse de toda intromisión dentro del espacio privado de cada individuo, salvo, que exista una razón válida para hacerlo. Toda injerencia es ilegal cuando está prohibida por la ley.

Cabe manifestar que la inviolabilidad de la vida privada no siempre es absoluta y definitiva. El derecho a mantener salvo el ámbito privado, en ciertos casos, puede ceder ante las exigencias del bien común. Así, por ejemplo, cuando el Estado recauda los impuestos puede, de manera legítima, penetrar en una zona privada para evitar la evasión de impuestos. Se debe recordar que todo acceso a la esfera de lo íntimo debe estar motivado o justificado y previsto de modo expreso por la ley.

Existe en la ley ciertos casos en los cuales les es lícito a las autoridades inmiscuirse en la vida privada de las personas; así se puede mencionar:

- El allanamiento, tanto a domicilio propio, como ajeno, para detener al delincuente sorprendido en delito flagrante.
- El allanamiento del inmueble, nave o aeronave donde se encuentre una persona contra la cual exista orden de captura.
- El allanamiento de un lugar no abierto al público donde se lleve a cabo un delito.
- La retención y apertura de la correspondencia de un imputado.
- La interceptación de comunicaciones telefónicas, etc.

Como se puede apreciar el derecho a la intimidad, en estas circunstancias, se ve menoscabado por la potestad judicial; pero, siempre, en beneficio de la colectividad y con el propósito de impedir un daño grave en los derechos y valores de la sociedad. Respecto a ese tema, el tratadista Rivera Llano manifiesta:

> *Nadie discute hoy en las sociedades democráticas que el derecho a la intimidad y al honor, al igual que todo otro derecho humano, no puede ser ilimitado o absoluto, haciéndose, desde luego, la salvedad de que nada puede justificar medidas que estén en contradicción con la dignidad física, mental, intelectual o moral de la persona humana. Las limitaciones necesarias para equilibrar los intereses del individuo con aquellos otros individuos, grupos y el Estado varían según el contexto en que se busque aplicar el derecho a la intimidad y el honor. El interés público exige a menudo que las autoridades, para poder intervenir en la esfera privada del individuo, cuenten con más facultades que las que sería aceptable dar a individuos o grupos y las circunstancias en que puedan ser otorgadas tales facultades a una autoridad pública, quedaron estipuladas en la Convención Europea para la Protección de los Derechos Humanos y Libertades Fundamentales y son aquellas en que las injerencia en la esfera privada se hace necesaria en una sociedad democrática para defender los intereses de la seguridad del Estado, la seguridad pública o el bienestar económico de la Nación, para impedir el desorden o el crimen, para proteger la salud o la moral pública o los derechos y las libertades de los demás, pero es esencial que los casos en que se*

> *permite la interferencia sean definidos con precisión. De ahí los denominados estatutos de prensa, radio y televisión; así como las correspondientes normas procesales en materia penal.*[63]

Como acertadamente sostienen el tratadista Rivera, la inviolabilidad del derecho a la intimidad no conseguiría ser incondicional siempre porque se violaría algunos derechos fundamentales reconocidos por nuestra Constitución y se protegería lo menos por lo más, es decir, se renunciaría a velar por los intereses de la comunidad o del Estado por salvaguardar un interés individual. De este modo, se puede apreciar la diferencia entre una sociedad democrática y una sociedad oprimida o totalitaria.

3.4.EL DERECHO A LA INTIMIDAD Y EL HÁBEAS DATA

Es importante comenzar este tema señalando la finalidad del hábeas data, el mismo que recae en la protección a la persona humana en su intimidad, es decir, en su dignidad e integridad; procurando, de esta manera, que la información obtenida por medio de los ordenadores sea cierta y no contenga circunstancias privadas, pertenecientes al conocimiento íntimo de la persona.

Marie Claude Mayo nos dice respecto al tema que:

> *La regla fundamental de la protección de la privacidad de los datos está configurada por dos extremos que por el bien de la sociedad se desea compatibilizar: el derecho del que gozan los sujetos de la información de tener acceso a sus datos personales y a corregir aquellos que sean erróneos e impertinentes, pero con la limitación que tal prerrogativa no llegue a coartar la libertad de recolección, es decir, sobre bases que no perturben ni entraben el avance de la ciencia y la tecnología.* [64]

[63] Abelardo Rivera Llano, La protección de la Intimidad y el Honor y la Informática, Publicado en Estudios Penales, Edit. Temis, 1984, p. 54.

[64] Marie Claude Mayo, Informática Jurídica, Chile: Edit. Jurídica de Chile, 1991, p. 95.

Y es que con el desarrollo de la tecnología que, para muchos es un elemento peligroso, se ha marcado una forma de uso de la información a través de los ordenadores que nos ha convertido en sus dependientes. La información de una persona puede ser almacenada en una máquina y manejada por el ordenador con una eficiencia puntal; pero, con el riesgo eminente de que estos datos sean transmitidos y reproducidos a pedido de cualquier persona e, incluso, sean objeto de falta de veracidad.

Es precisamente, en esta dirección por dónde camina el hábeas data para garantizar el derecho a la intimidad que, como ya se ha anotado, es el derecho a gozar de la vida dentro de un ámbito totalmente privado, que no debe ser perturbado por terceros ni por el propio Estado para alcanzar el desarrollo de la personalidad en libertad.

Con respecto a este tema, el Dr. Juan Larrea Holguín puntualiza:

> *Hay hechos, modos de ser, creencias, costumbres, características de la persona y de su familia que pueden no tener ningún aspecto peyorativo, mucho menos delictivo o contrario a la moral que, sin embargo no tienen por qué ser del conocimiento del público ni pueden aprovecharse o tomarse como motivo para una inculpación pública o para las discusiones de índole político, en una palabra, no tienen porqué darse a la publicidad por personas extrañas. Este es el respeto a la intimidad personal y a la intimidad familiar.* [65]

El derecho a la intimidad es tan importante que, a más de ser expuesto en nuestra Constitución, dentro de los llamados derechos personalísimos, se ve, también, protegido por el Código Penal (capítulo V de los delitos contra la inviolabilidad del secreto) y por el Código de Procedimiento Penal; en el cual se salvaguarda la inviolabilidad del domicilio (con las excepciones que dentro del propio cuerpo legal se plantean) puesto que se entiende al domicilio como la residencia de una persona donde la intimidad encuentra el

[65] Juan Larrea Holguín, Nueva Estructura Constitucional del Ecuador, Quito: Edit. Corporación de Estudios y Publicaciones, 1969, p. 79.

mayor grado de seguridad. Esta imposibilidad de allanar el domicilio, sin contar con una orden judicial, etc. es la forma de proteger a la intimidad, tanto personal como familiar.

Pero, este resguardo a la intimidad se ve amenazado por la tecnología, al punto de considerar a la privacidad como un problema social de nuestra época. La capacidad de la computadora de procesar y almacenar datos de un particular es tan grande que se pierde fácilmente la noción del tipo de información que en ella se encuentra.

Ahora bien, es importante en este capítulo hacer alusión de lo que significa el hábeas data para luego analizar el ámbito de su aplicación. La palabra "hábeas" ha sido tomada del derecho inglés, que se ha generalizado y forma parte de muchos idiomas, incluso, del nuestro. Por otro lado, la palabra "data" significa dato, cuya fuente es el idioma inglés; es así como la denominación de "hábeas data" hace referencia al derecho que posee cada individuo para acceder a los datos que sobre sí constan en los registros.

Constituye una figura jurídica que goza de características propias y está contenida en la Constitución ecuatoriana, dentro del Capítulo Tercero, sobre las Garantías Constitucionales, artículo 92, que expresa:

> Art. 92: *Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Así mismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.*
>
> *Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.*

> *La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, esta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.*[66]

La Constitución con esta disposición da paso a que la información personal llegue a formar parte de los datos inmersos en un computador, lo que genera pérdida de privacidad; además, que reconoce el derecho que tiene cada persona de conocer y verificar sus datos; así como, de rectificar, actualizar, anular o eliminarlos. Por lo tanto, esta norma constituye una garantía al derecho a la intimidad ya que cubre los riesgos que descienden del registro de datos personales. El hábeas data no constituye la única forma jurídica para proteger el derecho a la intimidad; esto se debe a que no solo el registro de datos personales puede afectar a la intimidad de una persona; sino también puede verse afectada por las injerencias del Estado.

El Dr. Nahim E. Emén Kalil con respecto a este tema señala:

> *Un ejemplo clásico de la manera en que puede afectarse la intimidad por parte del Estado, respecto a la que no existe protección legal explícita y suficiente, la constituyen los excesos o abusos en las medidas de seguridad en las visitas o comunicaciones penitenciarias o en la aplicación del propio régimen penitenciario, en el que de acuerdo con el Código de Ejecución de Penas y rehabilitación Social, debe aplicarse la individualización del tratamiento, lo que involucra un conocimiento profundo y forzado de la personalidad de cada individuo.*[67]

Por otra parte, lo esencial del hábeas data es el derecho de acceso que posee cada individuo sobre sus datos, los cuales se encuentran dentro de registros ajenos. Este derecho posibilita

[66] Constitución de la República del Ecuador, Op. Cit. p. 59.
[67] Emén Kalil Nahim, El hábeas data en el Ecuador, Quito: Edit. EDINO, 1997, p. 95.

a la persona para conocer el uso y el origen de sus datos, así como el destino y el tiempo de vigencia de los mismos. En conclusión, se puede decir que el hábeas data es una acción, que faculta a la persona a provocar *"la actividad jurisdiccional del Estado"*,[68] esto expresado en sentido técnico procesal.

3.5. ESFERA DE APLICACIÓN DEL HÁBEAS DATA

El hábeas data es un recurso creado para proteger los derechos de los particulares y con ello poner en vigencia los derechos humanos; el Dr. Cesar Trujillo señala al respecto:

> *En la Convención Americana sobre Derechos Humanos, el Ecuador se comprometió a conceder a sus habitantes un recurso sencillo y rápido o cualquier otro recurso efectivo ante los jueces o tribunales competentes para obtener amparo contra cualquier posible amenaza de violación, o, desde luego, contra cualquier violación de los derechos fundamentales.* [69]

Como podemos observar, en nuestro País, tanto la Constitución como los tratados internacionales, a los cuales nos hemos adherido, defienden la acción del hábeas data que constituye un derecho adjetivo con gran relación al derecho sustantivo de la intimidad al cual resguardan.

Es, con tal finalidad, que este recurso debe aplicarse sin limitación alguna; es decir, tanto a las personas jurídicas como a las personas físicas ya que, el excluir a las personas jurídicas originaría una discriminación debido a que gran parte de las entidades concentran sus datos en empresas de gran magnitud o, incluso, en establecimientos bancarios por lo que no sería justo que dichas instituciones no puedan acceder a sus datos. Así, también, existen

[68] Enciclopedia Jurídica Omeba; Tomo I; pág. 207.
[69] Julio Cesar Trujillo, "Teoría del Estado en el Ecuador"; citado por Nahim E. Emén Kalil; El hábeas data en el Ecuador, Op. Cit. p. 97.

empresas pequeñas, conformadas por una o dos personas físicas, cuyos datos a pesar de formar parte de las personas jurídicas para efectos fiscales, siempre se ven relacionados con los datos de las personas físicas, que sin la amplitud dada por el recurso no podrían acceder a los mismos.

La defensa al derecho a la intimidad no se puede suministrarla solo al individuo, excluyéndolo de los grupos sociales a los que se adhieren y en los que desarrollan su personalidad. Es por tal motivo, que la protección de la privacidad debe ser absoluta como, también, debe serlo el control sobre los bancos de datos.

Fue la antigua República Federal Alemana, la que dictó la primera y novedosa ley sobre la protección de datos, el 7 de octubre de 1970; la misma que se encontraba limitada al control de la administración pública. Esta ley presentaba algunas ingeniosas normas, pues instauraba un centro de control adecuado para la protección de datos. Luego, esta ley fue sustituida por otra, que se originó en el marco de la informática, la misma que incluía la obligación de registrar los bancos de datos, de extenderlos a los sistemas manuales y la limitación del control jurídico de los datos personales.

Al respecto, Vittorio Frosini comenta que *"la primera ley realmente orgánica y completa sobre la protección de la intimidad y sobre el control de los bancos de datos, públicos y privados, fue dictada por el parlamento sueco, el 11 de mayo de 1973"*.[70] A esta ley se la puede considerar como ejemplo de las demás ya que constituye el punto de referencia para todas las posteriores.

[70] Vittorio Frosini, Informática y Derecho, Bogotá: Edit. Temis, 1998, p. 114.

Pero, fue realmente la época del nacimiento de la computadora y el avance informático en Estados Unidos, que desató el surgimiento de varias comisiones de protección a la privacidad y de la ley "Privacy Act.", en el año 1972; la cual se creó con la finalidad de proteger la vida privada de personas físicas contenidas en los registros manuales y automáticos del gobierno federal. La mencionada ley sostiene que solo los datos que guarden relación con los fines que persiguen las entidades púbicas pueden ser llevados en registro; caso contrario se estaría violando con la intimidad de las personas. Además, estos datos tienen que estar actualizados y disponibles a su titular.

Cabe afirmar que esta ley ha creado algunas limitaciones con respecto a los registros llevados por el FBI, la CIA o los servicios de inmigraciones y tráfico de drogas ya que a este tipo de información no se puede tener acceso directo, sino que se tiene que cumplir con varios requisitos para poder acceder a ella.

En el continente europeo, la mayoría de países han cimentado leyes con respecto a este derecho. Así Francia, España, Dinamarca, Austria, Noruega y muchos más han enunciado el principio: tanto las personas físicas como las jurídicas tienen derecho de conocer sus datos personales recopilados en los bancos de datos y su utilización; así como, también, de pretender su actualización y corrección. Además, han instituido niveles de control sobre el manejo de la información, para prevenir su mal uso, con lo que se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Países como Argentina y Brasil, también, han adoptado dentro de sus constituciones el derecho de acceso a la información; así el artículo 43 de la Constitución de la Nación Argentina, sostiene: *"Toda persona podrá interponer esta acción para tomar conocimiento*

de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".[71]

En lo que corresponde a nuestro país, Ecuador, en el año de 1996, se implantó, por primera vez, en nuestra Constitución, el derecho de acceso o hábeas data para la protección de datos personales y de entidades tanto públicas como privadas. Anteriormente, solo se protegían los documentos calificados, es decir, aquellos documentos reservados por razones de Seguridad Nacional por lo que el individuo quedaba totalmente desprotegido.

Es por tal motivo que, de manera precisa, surgió el derecho al hábeas data sin ninguna distinción para las personas jurídicas como para las personas físicas. Esto involucra la capacidad que tiene cada individuo para prevenir los distintos manipuleos en la información personal o en la difusión de actividades o actitudes que solo pertenecen al dueño de la información, con la finalidad de impedir que los datos recogidos se usen para reprimir libertades y derechos.

En lo que corresponde al trámite del hábeas data, la ley señala que toda persona natural o extranjera puede solicitar, ante el juez de primera instancia del domicilio del poseedor de la información, el cumplimiento de este derecho. Incluso, el defensor del pueblo puede promover o patrocinar el recurso. Una vez que se ha recibido la petición, se convoca a una Audiencia para la que se tiene el plazo de 8 días, luego del cual se tiene 2 días para dictar la resolución.

[71] Emén Kalil Nahim ,El hábeas data en el Ecuador, Op. Cit. p. 109.

El juez, en la resolución, puede ordenar la eliminación, la rectificación o la no divulgación de la información; así, como, también, dar la prestación de la información con todos los datos y las certificaciones de que se eliminó o rectificó, dentro de los ocho días. En caso de que la petición sea incumplida puede pedirse la verificación directa y el funcionario público será destituido.

En caso de que el juez considere que la información no afecta al honor, a la intimidad o no puede irrogar daño moral al recurrente, el recurso puede ser negado. De igual manera, el juez puede manifestar que no procede el recurso cuando este afecte al sigilo profesional, obstruya la acción de justicia o cuando se trate de documentos reservados por seguridad nacional. Será, sin duda, el Tribunal Constitucional el que conozca las resoluciones que denieguen el recurso.

Todo lo antes manifestado se crea con el objeto de obtener del poseedor una información completa, clara y verídica que sea rectificada y no divulgada; así como, también, se debe conocer el uso que se le haya dado o que se le va a dar a dicha información para exigir las respuestas y el cumplimiento de las medidas cautelares, con la intención de salvaguardar la reserva de cada individuo.

CAPÍTULO IV

LOS DELITOS INFORMÁTICOS Y LA LEGISLACIÓN EXTRANJERA

CAPITULO IV

4. LOS DELITOS INFORMÁTICOS Y LA LEGISLACIÓN EXTRANJERA

Es innegable, que en materia informática, los países desarrollados han originado un progresivo marco jurídico para sancionar drásticamente el auge de los delitos informáticos y esto debido al indudable nivel de perfeccionamiento informático que ha existido en los países norteamericanos como europeos.

En nuestro País, la informática, lamentablemente, ha abierto una grieta descomunal dentro del marco legislativo porque ha rezagado al Código Penal e, inclusive, a las leyes que se han modificado recientemente. Y es que si se legisla, en materia informática, en nuestro País, se lo hace de forma leve e incluso desordenada, sin manifestar mayor preocupación por las nuevas formas delictivas que se llevan a cabo a través de mecanismos informáticos. Las pocas leyes que regulan sobre este tema, para muchos tratadistas son consideradas como "*leyes pre- informáticas*", es decir, que abarcan temas variadísimos, como los servicios de procesamiento de datos, transmisión y recepción de información codificada y ciertos programas informáticos.

Por tal motivo, es imprescindible que nuestro órgano legislativo se organice y cree leyes tan avanzadas como los sistemas informáticos, es decir, verdaderas leyes que se incorporen al Código Penal y se adecuen a los cánones internacionales vigentes.

Al hablar de normas extranjeras y de los delitos informáticos no se puede dejar de analizar la legislación norteamericana, europea e, incluso, la latinoamericana. En lo que respecta al derecho estadounidense, cuyo sistema jurídico es el consuetudinario, se ha conseguido establecer una normatividad equivalente al desarrollo del sistema informático. Se han

dictado leyes como la *"Counterfeit Access Device and Abuse Act"*, que protege a las computadoras del gobierno federal, los bancos y establecimientos de crédito contra el acceso de personas no autorizadas, excluyendo de esa protección a las computadoras privadas; así, también, han incorporado normas en contra de copias de programas e, incluso, de todos los abusos cometidos por medio de las tarjetas de crédito, estableciendo multas que sobrepasan los 100.000 dólares y penas hasta de veinte años de prisión.

El único inconveniente que se presenta es que cada País ha implantado su respectiva normatividad, por lo que para un Estado puede ser un delito para otro, puede ser un delito menor. Es por tal motivo, que existen valoraciones diferentes en los Tribunales o Cortes de cada nación. Las normas en contra de los *Computer-Crimes* se presentan muy completas, sobre todo, en los Estados de California y Pensylvania.

Por otro lado, la legislación europea ha considerado conveniente modificar los tipos penales ya existentes y, de esta manera, adecuar las nuevas conductas delictivas de tipo informático. Y es que, sin duda, los europeos han dado mayor importancia a este tipo de conductas que se van incorporando a la sociedad a través del desarrollo tecnológico y de la innovación.

La Comunidad Europea, conformada por países desarrollados, se ha preocupado por problemas relacionados con la piratería, los virus informáticos y, en general, contra cualquier infracción cometida en el sector de la información automatizada. Así, también, la Comunidad Económica Europea ha emitido una Recomendación sobre la criminalidad en relación con los ordenadores; en la que se incrementa la lista de infracciones como el fraude informático, los daños que afectan los datos y programas, el sabotaje informático, el

acceso no autorizado, la alteración de datos y programas, la utilización no autorizada de ordenadores y de programas informáticos protegidos.

En España, los delitos informáticos se han dividido en tres grupos: el primero tiene que ver con el manipuleo de los datos; el segundo, se basa en la obtención y divulgación de secretos industriales, comerciales o personales con la finalidad de producir resultados perjudiciales y el tercer grupo abarca todo lo referente a la obtención de programas sin la autorización de su titular.

Dentro de su Constitución el Art. 18, apartado 4, manifiesta lo siguiente: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. [72] Con lo cual busca proteger a la intimidad como derecho fundamental del individuo.

En Francia, en cambio, se ha originado la Ley 88-19, que crea un capítulo nuevo dentro del Código Penal francés, llamado: *"Sobre Ciertas Infracciones en Materia Informática"* sancionando así: el sabotaje informático, la destrucción de datos, la falsificación de documentos, el acceso fraudulento a un sistema de elaboración de datos, el uso de documentos informatizados falsos e, incluso, el entorpecimiento o falsedad en el funcionamiento de un sistema, la tentativa y asociación para delinquir. Las sanciones impuestas a estos ilícitos son variadas, pues van desde la privación de la libertad hasta la incautación de los materiales que fueron utilizados por el sujeto activo para delinquir.

En lo que respecta a Italia, Alemania, Dinamarca y Austria, se ha incorporado, en cada país, normas que frenan los delitos de tipo informático por lo que se ha reformado el Código

[72] Gustavo Aboso y María Zapata, Cibercriminalidad y Derecho Penal, p. 185.

Penal existente e, incluso, se han adherido a nuevos convenios internacionales sobre el tema. En especial, se sanciona el robo de información, el uso abusivo de tarjetas magnéticas y hasta la utilización de redes informáticas para perpetrar delitos económicos. En Alemania, particularmente, se trata de frenar las manipulaciones informáticas que pueden ser de tipo bancario hasta el uso abusivo de las telecomunicaciones.

Para culminar, es importante estudiar la legislación latinoamericana, la cual se ha visto retardada frente a los crecientes desarrollos tecnológicos. La situación, en la mayoría de países de Latinoamérica, es crítica ya que la impunidad es casi total, debido a la falta de organización para lograr reformar las normas de derecho penal.

En Chile, se ha presentado un proyecto de ley para aplacar los delitos informáticos; así, la persona que utilice o ingrese de manera maliciosa a sistemas de computadores o a cualquier parte de la misma con el propósito de alterar, obstaculizar o suprimir información será castigada con pena de presidio menor, en su grado medio o máximo.

A su vez, se señala que la persona que, a sabiendas y de forma maliciosa, intercepta, interfiere, daña, usa o destruye una computadora, un sistema o red de computadoras con el fin de defraudar u obtener dinero, será sancionado con una pena máxima.

Como se puede apreciar, estos delitos no reclaman la existencia de una condición especial dentro del sujeto activo por lo que pueden ser ejecutados por cualquier persona y se los puede incluir dentro de los denominados delitos comunes. Además, en este tipo de injustos no se puede hablar de dolo eventual ya que al manifestar que son realizados de forma maliciosa, y, a sabiendas se está considerando que son cometidos con conciencia y

voluntad, es decir, de forma dolosa. El bien jurídico que se busca proteger es, sin duda, la información.

En Perú, al igual que en México, los Códigos Penales han sido reformados para prevenir los diversos ataques producidos a través de los sistemas informáticos. Entre los artículos que se han incorporado, encontramos aquellos que previenen la penetración ilícita a los equipos informáticos y la alteración o destrucción de datos informáticos. La protección penal, incluso, se extiende a las instituciones financieras y la pena original se agrava en caso de que la infracción sea producida por algún empleado o trabajador que forme parte del sistema financiero.

En lo que respecta a Argentina, no existe una legislación específica sobre los delitos informáticos por lo que se busca crear un proyecto de ley que frene los denominados delitos informáticos como son: el sabotaje informático, la violación de secretos, la alteración o destrucción de datos y equipos informáticos. En lo que respecta a delitos en contra de la intimidad y el honor, el Código Penal Argentino se ha reformado penando a todos aquellos actos que infrinjan la confidencialidad de la información; contenida en documentos, medios electrónicos o magnéticos, discos, microfilms, etc. Lamentablemente, esta reforma solo protege un pequeño campo de los denominados delitos informáticos, puesto que se limita a la protección de los datos públicos o privados destinados a suministrar información, sin llegar a contemplar la gran gama de casos que afectan a bienes jurídicos de igual o mayor importancia.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

Al finalizar la presente monografía sobre los "Delitos Informáticos: Conflicto entre el Derecho al Honor y la Intimidad y el Derecho a la Información" me permito señalar algunas conclusiones.

- Con la creación de los sistemas informáticos, se puede apreciar que la humanidad ha llegado a obtener altos niveles de desarrollo en las comunicaciones y en el comercio mundial; pero, este importante progreso informático no ha conseguido resguardar la seguridad y la privacidad de la cual goza la persona como un derecho fundamental, debido a que se ha generado nuevas formas delictivas, cometidas a través de medios informáticos poco comunes.
- Se puede apreciar la variedad de conceptos y clasificaciones que existe sobre los delitos informáticos, quedando varias interrogativas sobre cuál es el concepto más acertado y pertinente para definir a estos delitos y cuál es la clasificación más completa para abordar el tema de los mismos. En lo que corresponde a los sujetos que intervienen en esta clase de injustos, se puede considerar que gozan de ciertas características, tanto intelectuales como económicas; por lo que, son conocidos como delitos de "cuello blanco".
- Dentro de los tipos de delitos informáticos, se observa que se puede cometer varias manipulaciones, tanto en los datos de entrada como en los de salida, lo que genera la sustracción y eliminación de información perteneciente a un ordenador, con la

finalidad de obtener beneficio propio o de perjudicar a un tercero. Este tipo de injustos se realiza por medio de las computadoras. Sin embargo, hay otros delitos en los cuales las computadoras son el instrumento adecuado para ejecutarlos como es el caso de la estafa informática, el hurto informático y la falsedad informática.

- Al analizar el derecho a la intimidad, el honor, el buen nombre y el derecho a la libertad de expresión se observa la importancia jurídica de la que ellos gozan, ya que son considerados por nuestra Constitución como derechos fundamentales, es decir, son derechos inherentes a cada individuo y el objetivo del Estado es hacer respetar y protegerlos.
- Al hablar del honor se habla de los valores personales de cada individuo por lo que se debe tener presente la estima que cada persona tiene de sí misma y el aprecio que los demás tienen sobre ella, dentro de un entorno social determinado. Este derecho busca resguardar la buena reputación de una persona. En cambio, la intimidad es todo aquello que un individuo señala como interno o exclusivo; para, de esta manera, frenar las injerencias por parte de terceros dentro de su vida privada. Generalmente, depende, del titular del derecho, el límite de la privacidad por lo que se puede apreciar que el honor y la intimidad, a pesar de ser considerados derechos fundamentales y personales, no gozan de las mismas características ya que el primero se ejerce dentro de las relaciones sociales, mientras que el segundo, se ejerce dentro de la esfera privada.
- La libertad de expresión permite al hombre poner de manifiesto sus propias ideas y emitir criterios diversos de acuerdo con su forma de pensar; en definitiva, ayuda al desarrollo intelectual de una persona dentro de lo social. Toda expresión u opinión

debe ser manifestada con total responsabilidad y con apego a la verdad con la finalidad de no menoscabar los derechos de los demás.

- El respeto que se debe tener a la vida privada de una persona se ve plasmado en nuestra Constitución ya que impide la intromisión de cualquier persona a informaciones catalogadas como confidenciales. Es así como la libertad de información se ve limitada por el derecho a la intimidad; pero, es necesario aclarar que las personas encargadas de recopilar información, como es el caso de los periodistas, tienen todo el derecho de investigar y recopilar información siempre que la misma sea obtenida de forma lícita y, al momento de su publicación, no engendre perjuicio alguno a terceros.
- Es preciso que la libertad de información posea límites para evitar que surjan opiniones injuriosas que desacrediten a una persona; se busca evitar son los insultos y los informes humillantes por parte de los informadores. Además, la libertad de información limita su actuar al momento de impartir informaciones que perjudiquen o desorienten el desarrollo integral de los niños y niñas.
- La Doctrina de la Real Malicia nos permite conseguir un equilibrio entre la prensa y los derechos a la honra, el honor y el buen nombre, que hubiesen sido afectados por comentarios lesivos a funcionarios públicos, objeto de información.
- Esta doctrina de origen anglosajón es muy disímil a nuestro ordenamiento jurídico; lo que hace poco efectiva su aplicación. Y es que la aplicación de esta doctrina contraviene muchos principios que deben ser respetados como son el de presunción de inocencia, el de igualdad jurídica, que hace referencia al derecho que tenemos todos de no recibir un trato discriminatorio, y el derecho a probar un hecho

negativo, razón por la cual la inversión de la carga de la prueba resulta contraria al ordenamiento jurídico.

- En cuanto a la violación del secreto en las comunicaciones, hay que tener presente que no solo se castiga la retención y exploración de los datos que tienen el carácter de secretos; sino, también, la difusión de estos. Para que el delito se consuma, es necesario que el autor sea consciente de que la información obtenida y divulgada ha sido adquirida de manera ilegítima, es decir, el periodista debe difundir una información ajena y prohibida.
- La importancia del hábeas data radica en la posibilidad del individuo de poder acceder a los datos que sobre sí, constan en los registros. Este derecho constituye una garantía al derecho de la intimidad ya que resguarda los riesgos que descienden del registro de los datos personales. Este derecho debe aplicarse sin ninguna limitación, es decir, tanto a las personas físicas como a las jurídicas.
- El uso de la internet implica la pérdida del derecho a la intimidad, lastimosamente en nuestro País, no existe un marco normativo que regule este tipo de inseguridad jurídica; en cambio, en materia informática, los países desarrollados han originado un progresivo marco jurídico para sancionar drásticamente el auge de los delitos informáticos y esto debido al indudable nivel de perfeccionamiento informático que existe en los países norteamericanos como europeos.
- Es importante prevenir a todos los usuarios de la red sobre el riesgo y la protección de sus datos personales ya que éstos pueden ser almacenados por terceras personas y utilizados de manera provechosa e ilícita.

- Se puede palpar como la tecnología viola nuestra intimidad y reserva sin que existan mayores esfuerzos, en nuestro País, por tratar de frenar los riesgos inducidos a nuestros derechos, los cuales se encuentran protegidos por nuestra Carta Magna. Es por tal motivo, que deberíamos concientizarnos y promover un ordenamiento jurídico más dinámico que regule todas las situaciones que se van generando a diario, sin olvidar que las nuevas leyes deben garantizar una vida en sociedad tranquila y pacífica.
- Es indudable la falta de interés e información que tenemos sobre los temas de relevancia social por lo que se debería promover un mayor involucramiento en la problemática para convertirnos en sujetos activos de su posible solución.

BIBLIOGRAFÍA

ÁLVAREZ CIVANTOS, Oscar José; Normas para la Implantación de una Eficaz Protección de Datos de Carácter Personal en Empresas y Entidades, Granada: Edit. Comares, 2001.

BECCARIA, C; De los Delitos y de las Penas; Madrid: Edit. Imprenta Nacional, 1986.

BERDUGO GÓMEZ DE LA TORRE; Honor y Libertad de Expresión; Madrid; 1987.

BERDUGO GÓMEZ DE LA TORRE; Revisión del Contenido del Bien Jurídico Honor; Madrid: Anuario de Derecho Penal y Ciencias Penales, 1984.

CARASCOSA LÓPEZ, Valentín; Memorias del X Congreso Iberoamericano de Derecho e Informática; Santiago de Chile: Edit. LOM, 2004.

FROSINI, Vittorio; Informática y Derecho; Bogotá: Edit. Temis, 1988.

HEGEL; W.G.F.; Lecciones sobre la Historia de la Filosofía; Tomo I; México: Fondo de la Cultura Económica, 1977.

LARREA HOLGUÍN, Juan; Nueva Estructura Constitucional del Ecuador, Comentario Jurídico de la actual Constitución; Quito: Corporación de Estudios y Publicaciones, 1969.

LLÁCER MATACÁS; María Rosa, La Protección de los Datos Personales en Internet, en La regulación del comercio electrónico; Madrid: Dykinson, 2003.

MAYO; Marie Claude; Informática Jurídica; Santiago de Chile: Edit. Jurídica de Chile, 1991.

NAHIM E., Emén Kalil; El Hábeas data en el Ecuador; Quito: Edit. EDINO, 1997.

PEÑA Helen, PALAZUELOS Silvia y ALARCÓN Rosalita, Delitos Informáticos, División de Estudios de Posgrado, Facultad de Derecho; México: Universidad Autónoma de México, 1999.

RIVERA LLANO, Abelardo; La Protección de la Intimidad y el Honor y la Informática; Trabajo publicado en Estudios Penales; Edit. Temis; 1984.

RODRÍGUEZ VILLAFAÑE, Miguel; Periodismo e Información Judicial en Argentina; Revista Contribuciones, Publicación trimestral de la Konrad-Adenauer Stiftung A.C.- Centro Interdisciplinario de Estudio sobre el Desarrollo latinoamericano; Argentina; 2001.

ROMERO, Coloma; De Los Bienes y Derechos de la Personalidad; Madrid: Edit. Lavel, 1985

SALT, Marcos, Delitos Informáticos de Carácter Económico; Buenos Aires:Edit. del Puerto,1994.

TORRES CHAVES, Efraín, Breves Comentarios A La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; Quito: Edit. Corporación de Estudios y Publicaciones, 2006.

UNESCO; Informe 19c/93 de 16 de agosto de 1976.

URIAS, Joaquín; Lecciones de Derecho de la Información; Madrid: Edit. Tecnos (Grupo ANAYA, S.A.) 2003.

VIDAL MARÍN, Tomás; El Derecho al Honor y su Protección desde la Constitución Española; Madrid: Centro de Estudios Políticos y Constitucionales y Boletín Oficial del Estado, 2001.

ZAFFARONI, Raúl Eugenio; Manual de Derecho Penal; Parte General; Buenos Aires: Edit. Sociedad Anónima Editora, Comercial, Industrial y Financiera, 2001.

ZAVALA BAQUERIZO, Jorge, Delitos Contra la Propiedad Tomo II; Guayaquil: Edit. Edino, 1998.