UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE DERECHO

"DELITOS CONTRA EL HONOR DE LAS PERSONAS A TRAVÉS DEL INTERNET"

TESIS PRESENTADA PARA OPTAR EL GRADO DE LICENCIATURA EN DERECHO

POSTULANTE : ***LUIS ALBERTO DEL CARPIO GONZALES***

TUTOR : ***Dr. RAMIRO BARRENECHEA ZAMBRANA***

LA PAZ - BOLIVIA

2003

DEDICATORIA

DEDICO EL PRESENTE TRABAJO A MI QUERIDA MADRE ELBA R. GONZALES O. LA CUAL SIEMPRE FUE MI IMPULSO Y RAZÓN DE VIVIR Y A LA CUAL DEBO MIS LOGROS Y TRIUNFOS EN LA VIDA.

ASÍ MISMO A MIS HIJOS VANNIA ROSSELY, ELBITA, GABRIEL, LUIS G. Y ARAMYS ALBERTO.

AGRADECIMIENTOS

AGRADEZCO A MI TUTOR DR. RAMIRO BARRENECHEA Z. LA COLABORACIÓN, BIBLIOGRAFÍA Y GUÍA, CON CUYO APOYO Y CONCURSO LA PRESENTE TESIS LLEGO A BUEN FIN .

DE LA MISMA MANERA A MI HERMANO JORGE EDWING DEL CAPIO GONZÁLES

INDICE GENERAL

CAPITULO I

METODOLOGÍA DE LA INVESTIGACIÓN

CAPITULO II

ANÁLISIS JURÍDICO DE LOS DELITOS CONTRA EL HONOR EN LA LEGISLACIÓN BOLIVIANA

CAPITULO III

EL INTERNET

CAPITULO IV

LA CRIMINOLOGÍA Y EL DELITO INFORMÁTICO

CAPITULO V

DELITOS CONTRA EL HONOR DE LAS PERSONAS A TRAVÉS DEL INTERNET

ÍNDICE DE CUADROS

ABSTRACT

Los constantes avances tecnológicos en materia informática han propiciado la aparición de nuevos conceptos, a nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, las investigaciones, la seguridad, el Derecho etc. son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

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

Debido a lo anterior se desarrolla el presente documento que contiene una investigación sobre la temática de los Delitos Contra El Honor De Las Personas a Través Del Internet , de manera que al final pueda establecerse una relación con el cambio y transformación del Derecho Penal.

Para lograr una investigación completa de la temática se establece la conceptualización respectiva del tema, generalidades asociadas al fenómeno, estadísticas regionales y continentales sobre delitos informáticos, y el desarrollo del Internet, como poder minimizar la amenaza de los delitos a través de la seguridad, aspectos de legislación informática, y por último se busca establecer el papel del Estado boliviano frente a los delitos informáticos.

Al final del documento se establecen las conclusiones pertinentes al estudio, en las que se busca destacar situaciones relevantes, Legislación comparada, Estadísticas, etc.

INTRODUCCIÓN

La mayoría de las sociedades enfrenta hoy en día una revolución de la informática, ya que esta nueva tecnología ha venido a reemplazar algunas de las funciones intelectuales desarrolladas por el hombre, construyéndose así la llamada "sociedad de la información" la cual ha determinado que los avances tecnológicos logrados por las computadoras se conviertan en una de las fuerzas más poderosas de la sociedad actual, posibilitando su uso tanto a nivel de grandes organizaciones, como en los mismos hogares.

En las tecnologías de la información se puede observar que se deriva una energía intelectual, que constituye una forma de poder. Por lo que la información significa poder, poder que puede ser objeto de dominio y de control sobre quien no lo detenta. Y es aquí donde hacemos referencia y será el tema central de nuestra ponencia el hecho de que no está fuera de los conocimientos de nadie los grandes beneficios que los medios de comunicación y el uso de la Informática han aportado a la sociedad actual, pero en la otra cara de la moneda tenemos que este desarrollo tan amplio de las tecnologías informáticas ofrece a su vez un aspecto negativo el cual radica en el hecho de que ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar.

Todo esto tiene su fundamento en el hecho de que los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales. Y es aquí donde hace su entrada triunfal los llamados "delitos informáticos" los cuales no son cometidos

por la computadora, sino que es el hombre quien los comete con ayuda de aquella o más bien a través de ésta.

En ese entendido, nuestro trabajo se dirige al análisis de las posibles soluciones, ya sean de carácter administrativo o penal que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de infracciones o delitos, alcance los niveles de peligrosidad que se han dado en muchos países.

Al iniciar esta ponencia, encontramos que no existe un consenso en cuanto al concepto de delito informático, y que estudiosos del tema lo han definido desde diferentes puntos de vista como son el criminógeno, formal, típico y atípico, etcétera; dando lugar a que la denominación de esta conducta haya sufrido diferentes interpretaciones, las que hemos recogido en este trabajo.

Además hemos señalado los sujetos; activos y pasivos, clasificación y los tipos de delitos informáticos. Seguidamente, realizamos un estudio de los métodos utilizados comúnmente para la comisión de este tipo de delito, y por último para finalizar el presente trabajo, hacemos unas conclusiones y dentro de éstas unas propuestas, sustentada en el estudio comparativo tratando de adecuar a la realidad existente en la mayoría de los países latinoamericanos, pero previendo que no estamos exentos de la velocidad del desarrollo tecnológico y de los vicios que éste genera.

CAPITULO I

METODOLOGÍA DE LA INVESTIGACIÓN

CAPITULO I

METODOLOGÍA DE LA INVESTIGACION

1.1 IDENTIFICACION DEL PROBLEMA.

A principios de la segunda mitad del siglo XX, una novedosa forma de automatizar, guardar y transmitir información se apodera de todo el mundo, trayéndole beneficios incalculables y adelantos hasta el presente inimaginables. Esta nueva forma se denomina informática. Pero no todo es socialmente útil, el hombre siempre ha sabido valerse de la tecnología para perfeccionar sus actos contrarios a los fines de la sociedad. Ayudado de este adelanto los delincuentes han perpetrado con mejora sus delitos y entre los muchos , aquellos contra el honor de las personas a través del Internet. Es verdad que en Bolivia como País pobre y en vías de desarrollo no debería preocuparse por estos aspectos pero lo paradójico es que el Internet se ha introducido en todas las áreas, es así que en la actualidad se lo utiliza para los negocios, contactos comerciales, búsqueda de información, comunicación, distracción, compra venta y todo lo que uno se pueda imaginar, como así en el campo Jurídico a evolucionado grandemente puesto que jamás hubiéramos pensado en un Notario de fe Publica cibernético pues ahora y actualmente lo hay, al hacer la identificación del problema supra citado veremos en el desarrollo la producción de los primeros delitos contra el honor de las personas a través del Internet , en nuestro país, es así que la problemática fundamental reside en la carencia de una normativa legal y especifica que regule esta situación puesto que a

mayor crecimiento de usuarios de Internet habrá un índice mayor de delitos de este orden, que afecten el Honor de las Personas.

1.2 DELIMITACIÓN DE LA TESIS.

1.2.1 DELIMITACION TEMÁTICA

Los delitos contra el Honor de las personas que usan como medio ejecutivo el Internet.

1.2.2 DELIMITACION TEMPORAL

Pondremos como parámetros los años 1997 a 2002, puesto que a partir del año citado se ha producido un ingreso masivo del Internet a nuestros hogares, Ciber Cafes, Instituciones publicas, privadas y otros.

1.2.3 DELIMITACIÓN ESPACIAL

Tomaremos como ámbito espacial de la presente investigación la ciudad de La Paz.

1.3 FUNDAMENTACION E IMPORTANCIA DE LA TESIS

En los últimos años el desarrollo de la información en especial la amplia difusión de Internet, ha tenido una influencia social de tal grado que las practicas tradicionales de las diversas disciplinas del

conocimiento se han modificado sustancialmente tal es el caso del Derecho y por que no también aplicado en todos los campos profesionales, en fin, el Internet implica un cambio en el paradigma tradicional del intercambio de información y aun de las diferentes formas de la relación de nuestras sociedades, permitiendo con ello una reestructuración social acorde con la globalización en la que nos encontramos inmersos en este nuevo milenio.

Por todo esto para cualquier persona relacionada con el campo del derecho surge la pregunta de cómo se ve afectada nuestra disciplina por la aparición de estas tecnologías, por lo que se podría dar tres respuestas. Primero que ahora la rama jurídica se ha visto trastocada, por la aparición de nuevos delitos que en otra época eran tal vez impensados. Segundo, siendo el derecho una ciencia que se encuentra en constante cambio y transformación, debido a su flexibilidad. Y Tercero aquí surge la imperiosa necesidad de desarrollar, cambios en nuestra legislación adecuada a las innovaciones y coyuntura de nuestra sociedad, a fin de que no exista impunidad por delitos cometidos a través del Internet.

1.4 OBJETIVOS DEL TEMA DE LA TESIS

1.4.1 OBJETIVOS GENERALES

- Se demostrara la existencia de conductas delictivas ejecutadas a través del Internet, que dañan el Honor de las personas.

- Demostrar la comisión y creciente ola de delitos informáticos en países que cuentan con Servicio de Internet.

1.4.2 OBJETIVOS ESPECÍFICOS

- Establecer la impunidad en nuestro país de los delitos contra el honor de las personas vía Internet.
- Fundar la insuficiencia regulatoria de tipos penales que no protegen el honor de las personas a través del Internet.

1.5 MARCO TEÓRICO REFERENCIAL

1.5.1 MARCO HISTÓRICO

En 1997 en fecha 25 de abril se promulga el D.S. 24582, Que reglamenta específicamente la parte de la informática tal como lo dispone el art. 66 inc 1 de la ley 1322 que contiene en sus nueve capítulos el reglamento de software, protección de Derechos de Autor , de las medidas precautorias y jurisdiccionales y los medios probatorios, soporte lógico banco de datos y procedimiento administrativo de conciliación y arbitraje tomando en cuenta el Acuerdo de Cartagena decisión 251, los ADPIC (Acuerdo sobre los Derechos de Propiedad Intelectual relacionados con el Comercio) y el convenio de Berna protege la expresión creativa del Intelecto Humano finalmente en julio de 1997, se publica el proyecto de la Ley de Ciencias y Tecnología que fue presentada a la Camara de Senadores para su tramite legislativo el 4 de marzo como propuesta de la Vice presidencia de la Republica del

anterior gobierno y del consejo nacional de Ciencias y Tecnología (CONACYT).

También el Código Penal antes de ser modificado considera su capitulo décimo, los delitos contra el Derecho de Autor y el art. 363 la Violación de Privilegio de Invención, ambas figuras tipificadas como delitos , están plenamente sancionadas.

El 10 de marzo de 1997 , se emite la ley 1768 " Ley de Modificaciones al Código Penal, esta ley en el numeral 57 dispone la inclusión de un capitulo, el XI dependiente del capitulo XII, del Libro Segundo del Código Penal, a los Delitos Informáticos, incluidos dentro de los arts. 363 Bis y 363 Ter., cuyas tipificaciones son manipulación Informativa y alteración, acceso y uso indebido de Datos Informáticos respectivamente.

El art. 362 referido anteriormente ha sido sustituido por el numeral 59 que de ser la figura Violación de Derecho de Autor actualmente es Delitos Contra la Propiedad Intelectual.

1.5.2 MARCO TEÓRICO

La realidad social actual ha impuesto una serie compleja de objetivos que el hombre debe alcanzar. El advenimiento del nuevo siglo ha creado modos de trasmisión de la información que permite que delitos inveterados, se ejecuten haciendo uso de este beneficio, los delitos contra el honor de las personas no escapo de esta nueva forma, que utiliza la tecnología informática del Internet para generarse.

En este sentido que vemos la urgente necesidad de que el derecho actual, responda con regulaciones jurídicas, para prevenir y posteriormente sancionar a los autores de la difamación, injurias y calumnias vía Internet. El problema se torna dificultoso y vamos a analizarlo descubrir y explicarlo, con ayuda del Conocimiento científico, propuesto por el Positivismo Jurídico, que escruta todo fenómeno social con la apreciación empírica de los hechos para contrastarlos con la norma jurídica. Este contraste nos permitirá concluir sobre si los delitos contra el honor de las personas a través del Internet estas suficientemente regulados o si carecen de normatividad para su control. Por tratarse de un problema con preponderancia de elementos técnicos creemos que no existe un mejor instrumento de examen que el positivismo Jurídico.

1.5.3 MARCO JURÍDICO

La era de las comunicaciones, la materialización de la idea del mundo como una aldea global, el ciberespacio y las cyberculturas, y el impacto de las tecnologías de la información han implicado una transformación en la forma de convivir en sociedad.

Dentro de este marco de transformación, el cambio producido por el mal uso de la informática ha hecho que surjan nuevas conductas merecedoras del reproche social que, sin embargo, no siempre son fáciles de tipificar. Así, han surgido modalidades delictivas relacionadas con la informática.

Una primera reflexión surge en relación al concepto informático. De la relación entre delito e informática, surgen entonces dos tipos de

ilícitos, los delitos computacionales y los delitos informáticos. Cuando un delincuente de delitos tradicionales comienza a utilizar como medio específico de comisión a las tecnologías de la información, se produce una informatización de los tipos tradicionales, naciendo el delito computacional, que en realidad se trataría solo de ilícitos convencionales que ya están regulados en el Código Penal. Sin embargo, también se crean conductas nuevas, no contempladas en los ordenamientos penales por su especial naturaleza, lo que hace necesario crear nuevos delitos, llamados delitos informáticos.

Es así como entendemos por delito informático a 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. Por lo tanto, 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 sólo delitos computacionales que no ameritan la creación de un nuevo ilícito penal.

Aún no es fácil conceptuar los delitos informáticos por su novedad. Una primera idea al respecto la señala el profesor mexicano Julio Téllez Valdés, quien lo conceptualiza desde dos ópticas. Nos dice que desde un punto de vista atípico son *"actitudes ilícitas en que se tiene al computador como instrumento o fin"*, y desde uno típico son "conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como medio o fin".

Esta primera idea es común en los textos del área, asi por ejemplo, Nidia Callegari define al delito informático *como "aquel que se da con la ayuda de la informática o de las técnicas anexas."*

Para Carlos Sarzana, el delito informático *"es cualquier comportamiento criminogéneo en que la computadora está involucrada como material, objeto o mero símbolo."*

En fin, podemos resumir las posturas diciendo que *"delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas."*

1.5.3.1 CONSTITUCIÓN POLÍTICA DEL ESTADO

Art. 6.- Todo ser humano tiene personalidad y capacidad jurídicas, con arreglo a las leyes. Goza de los derechos, libertades y garantías reconocidos por esta Constitución, sin distinción de raza, sexo, idioma, religión opinión política o de otra índole, origen, condición económica o social, u otra cualquiera.

La dignidad y la libertad de la persona son inviolables. Respetarías y protegerlas es deber primordial del Estado.

En este articulo la dignidad de la persona es protegida por nuestra Constitución Política del Estado, pues la dignidad, entendida como sustantivo de la palabra honor, que es el bien jurídicamente protegido por las leyes y en especial el articulo precedente.

1.5.3.2 CÓDIGO CIVIL

Art. 12. (PROTECCIÓN DEL NOMBRE).

La persona a quien se discuta el derecho al nombre que lleva o sufra algún perjuicio por el uso indebido que de ese nombre haga otra persona, puede pedir judicialmente el reconocimiento de su derecho o la cesación del uso lesivo . El juez puede ordenar que la sentencia se publique por la prensa. (Arts. 473 Código. de Comercio , Arts. 9, 999 Código. Civil)

Art. 16. (DERECHO A LA IMAGEN).

I. Cuando se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por la ley, que el juez haga cesar el hecho lesivo.

II. Se comprende en la regla anterior la reproducción de la voz de una persona.

Art. 17.- (DERECHO AL HONOR).

Toda persona tiene derecho a que sea respetado su buen nombre. La protección al honor se efectúa por este Código y demás leyes pertinentes.

Art. 18.- (DERECHO A LA INTIMIDAD).

Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos

por la ley.

Art. 21.- (NATURALEZA DE LOS DERECHOS DE LA PERSONALIDAD Y SU LIMITACION).

Los derechos de la personalidad son inherentes al ser humano y se hallan fuera del comercio. Cualquier limitación a su libre ejercicio es nula cuando afecta al orden público o a las buenas costumbres.

Art. 22.- (IGUALDAD).

Los derechos de la personalidad y otros establecidos por el presente Código, se ejercen por las personas individuales sin ninguna discriminación.

Art. 23.- (INVIOLABILIDAD).

Los derechos de la personalidad son inviolables y cualquier hecho contra ellos confiere al damnificado la facultad de demandar el cese de ese hecho, aparte del resarcimiento por el daño material o moral. (Art. 16, 32 Const. Pol. del Estado)

1.5.3.3 CÓDIGO PENAL.

TITULO IX
DELITOS CONTRA EL HONOR
CAPITULO UNICO
DIFAMACION, CALUMNIA E INJURIA

ARTICULO 282.- (Difamación).

El que de manera pública, tendenciosa y repetida, revelare o divulgare un hecho, una calidad, o una conducta capaces de afectar la

reputación de una persona individual o colectiva, incurrirá en prestación de trabajo de un mes a un año o multa de veinte a doscientos cuarenta días.

Concordancias
c.c. 17-c. p. m. 212-c. p.- 285-286 - 289-290-c.p. m.- 214 -

ARTICULO 283.- (Calumnia).

El que por cualquier medio imputare a otro falsamente la comisión de un delito, será sancionado con privación de libertad de seis meses a dos años, y multa de cien a trescientos días.

Concordancias
L. imp. 27-c. p. m. 213 - 214 - c. p. 168 285 - 286 -287 -290 -

ARTICULO 284.- (Ofensa a la memoria de difuntos).

El que ofendiere la memoria de un difunto con expresiones difamatorias o con imputaciones calumniosas, incurrirá en las mismas penas de los dos articulos anteriores.

Concordancias
c.p. 285 -

ARTICULO 285.- (Propalación de ofensas).

El que propalare o reprodujere por cualquier medio los hechos a que se refieren los artículos 282, 283 y 284, será sancionado como autor de los mismos.

Concordancias
c.p. 282 - 283 - 284 - 290 -

ARTICULO 286. (Excepción de verdad).

El autor de difamación y calumnia no será punible si las imputaciones consistieren en afirmaciones verdaderas, pero el acusado sólo podrá probar la verdad de la imputación:

1) Cuando se trate de ofensas dirigidas a un funcionario público y con referencia a sus funciones.
2) Cuando el querellante pidiere la prueba de la imputación, siempre que tal prueba no afecte derechos o secretos de tercera persona.

Concordancias
c.p. 162-165 - 282 - 283 - 288 -

ARTICULO 287.- (Injuria).

El que por cualquier medio y de un modo directo ofendiere a otro en su dignidad o decoro, incurrirá en prestación de trabajo de un mes a un año y multa de treinta a cien días.

Si el hecho previsto en le Art. 283 y la injuria a que se refiere este artículo fueren cometidos mediante impreso, mecanografiado o manuscrito, su autor será considerado reo de libelo infamatorio y sancionado con multa de sesenta a ciento cincuenta días, sin perjuicio de las penas correspondientes.

Concordancias

L.imp. 27 - 30 c. pm. 210 - 211 c. p. 132 - 162 -283 - 290 -

ARTICULO 288.- (Interdicción de la prueba).

No será admitida la prueba sino en los casos señalados en el articulo 286.

Concordancias

c.p. 286 -

ARTICULO 289.- (Retractación).

El sindicado de un delito contra el honor quedará exento de pena, si se retractare antes o a tiempo de prestar su indagatoria.

No se admitirá una segunda retractación sobre el mismo hecho.

Concordancias

c.p. 282 y s.

ARTICULO 290.- (Ofensas recíprocas).

Si las ofensas o imputaciones fueren reciprocas, el juez podrá, según las circunstancias eximir de pena a las dos partes o a alguna de ellas.

Concordancias

c.p. 282 - 283 - 285 - 287 -

ARTICULO 162.- (desacato).

El que por cualquier medio calumniare, injuriare o difamare a un funcionario público en el ejercicio de sus funciones o a causa de ellas,

será sancionado con privación de libertad de un mes a dos años.

Sí los actos anteriores fueren dirigidos contra el Presidente o Vicepresidente de la República, Ministros de Estado o de la Corte Suprema o de un miembro del Congreso, la sanción será agravada en una mitad.

1.6 HIPÓTESIS DEL TRABAJO

"El avance Tecnológico e informático a nivel a mundial a generado la probabilidad de que los delitos contra el honor de las personas realizados a través del Internet queden impunes situación que repercute con mayor intensidad en Bolivia por su atraso técnico jurídico "

1.7 MÉTODOS

1.7.1 MÉTODOS GENERALES

Se utilizara el análisis y la síntesis, de la misma manera el método inductivo y deductivo.

1.7.2 MÉTODOS ESPECÍFICOS

Para analizar las normas penales especificas sancionadoras de los delitos contra el honor de las personas a través del Internet, usaremos el método exegético.

Para contrastar los conceptos de daño, honor, patrimonio, moral, etc. Utilizaremos el método de las construcciones lógicas.

Si proponemos soluciones con la generación de nuevos cuerpos legales o artículos utilizaremos el método sistemático del derecho.

1.8 TECNICAS

Utilizaremos como técnicas en el presente trabajo la entrevista, cuestionarios, encuestas y de la misma manera para obtener resultados se hará muestreo de datos, aprovechando la estadística como medio empírico de contrastación de datos.

CAPITULO II

ANÁLISIS JURÍDICO DE LOS DELITOS CONTRA EL HONOR EN LA LEGISLACIÓN BOLIVIANA

CAPITULO II

ANÁLISIS JURÍDICO DE LOS DELITOS CONTRA EL HONOR EN LA LEGISLACIÓN BOLIVIANA

2.1 EL CODIGO PENAL

El Código Penal Recopilado y copiado del Código español de 1922, contenía una esencia superior en cuanto al desarrollo social de aquella sociedad en comparación con la nuestra, pues claramente se veía una brecha en el aspecto socio jurídico e histórico este hecho es asumido pues *"no existía otro derecho"* tal cual comenta el autor Latinoamericano Juan P. Ramos[1] .

Nuestro Código Penal elevado a rango de ley y modificado por la ley No. 1768 de 10 de marzo de 1997, ideológicamente se asienta en el Derecho Penal Liberal, que sustenta el principio de legalidad y admite aunque limitadamente la teoría peligrosista o defensita, que permite regular junto a los medios represivos (penas), los de carácter preventivo (medidas de seguridad), para enfrentar la defensa de la sociedad contra la delincuencia. Dando un sentido moderno a las sanciones ,e incorpora el personal judicial, suspensión condicional de la pena, detención domiciliara y otras medidas positivas y actualizadas.

[1] Ramos, Juan P
Los Delitos Contra el Honor
Abeledo Perrot, Buenos Aires, Argentina 1958, Pag 136

En lo sistemático, su contenido supera al código de 1834, pero coincidimos con que aun existen aspectos que pueden ser mejorados tomando en cuenta la extraordinaria dinamicidad de nuestra sociedad boliviana y los cambios y transformaciones que naturalmente inciden no solo en el aspecto social, sino también jurídico.

2.2 EL SUJETO ACTIVO DEL DELITO EN LA LEGISLACIÓN PENAL

El sujeto activo en los delitos contra el honor en nuestra legislación penal ofrece aspectos no bien aclarados, aunque ciertamente discutibles.

Quienes deben responder por un ataque contra el honor están sujetos a las reglas generales del derecho penal, pero existen casos en los que aun hoy existen controversias.

El delincuente es aquel que infringe una norma penal y es una persona a quien Raymundo Del Río en sus *"elementos de derecho penal"*[2] define como *"El individuo a quien es posible responsabilizar legalmente pro un atentado cometido en contra de una norma jurídica de carácter legal"*. Sin embargo de esta definición consideramos que aun hay controversias en torno a, si los sujetos activos de estos delitos son solo los imputables o los inimputables y que sanciones se aplican a los inimputables que atentan por si o por otros delitos contra el honor de las personas. Por otra parte, también es discutible la situación de las

[2] DEL RIO, Raymundo.
Elementos del Derecho Penal
Ed. 1939. Santiago de Chile Pag. 230

personas jurídicas, ya que surge una pregunta ¿ serán sujetos activos en los delitos contra el honor las personas jurídicas?

La criminología que hoy versa sobre el delincuente y la victima poco a aportado en torno a complejos mecanismos causales sobre el delincuente en este terreno.

La literatura consignada en torno al delincuente difamador calumniador o injuriador, apenas refiere a ese como a una persona que con *"animus injuriandi"*comete estos delitos.

Por nuestra parte, consideramos que se trata de un delincuente que obedeciendo a causas sociales, biológicas y psicológicas , comete este tipo de delitos en contra del honor, la dignidad, el decoro y la reputación de otros y cuya explicación es multicausal y multi explicativa, si bien con predominio de una de las causas de un momento dado.

De estas causas, a modo de factores precipitantes, son de alto valor las psicológicas debido a obsesiones, delirios de grandeza o paranoicas situaciones reactivas ante la frustración, estados de ansiedad, estrés, complejos de superioridad e inferioridad, sentimientos de amor, odio, envidia y otros. También debemos destacar que los factores sociales tienden a ser factores desencadenantes de los delitos contra el honor, otorgando a la familia, educación, religión, factores económicos y la influencia de los medios de comunicación, un relieve no despreciable.

2.3 EL SUJETO PASIVO DEL DELITO EN LA LEGISLACIÓN PENAL

En cuanto a la victima, la legislación boliviana no solo reconoce a las personas vivas sino también a los muertos considerándolos como sujetos pasivos. Otras legislaciones niegan alguna titularidad sobre bienes jurídicos tutelados. En realidad *"lo que la ley entiende por honor en caso de los muertos es su memoria"* [3] y si tenemos en cuenta que la ley civil considera a los herederos como continuadores de la personalidad de los difuntos, ellos vendrían a ser las victimas.

La victimólogia disciplina científica que ha logrado adelantos notables en los últimos años y que aun permanece bajo el manto protector de la criminología también ha logrado muy pocos avances, pese a que en ella confluyen no solo consecuencias victimológicas sino también efectos civiles que en casos precipitan a conductas depresivas, neurosis de angustia, ansiedad, sin descontar la implantación de complejos sentimientos negativos para su futuro desarrollo, reacciones de agresividad, autismo y otros que juzgaremos no deben ser desdeñados y que consideramos merecen mayor atención por parte de nuestra legislación. Capitulo aparte, merece la situación de las personas jurídicas los menores, los enajenados mentales, las personas deshonestas y deshonradas como sujetos pasivos o victimas de los atentados contra el honor, que por los limites del presente trabajo no abordamos en detalle, pero que si constituyen consideraciones validas y necesarias en este terreno tan delicado de los delitos contra el honor.

[3] MIGUEL, Harb, Benjamin
Código Penal Boliviano(Comentado)
La Paz-Bolivia, Ed. Los Amigos del Libro, 1979 2da Ed. Pag. 307

2.4 DIFAMACIÓN

Si revisamos el contenido de este articulo inserto en el Titulo IX Delitos Contra el Honor, Capitulo único, observamos :

Art. 282.- " El que de manera publica, tendenciosa y repetida, revelare o divulgare un hecho, una calidad, o una conducta capaces de afectar la reputación de una persona individual o colectiva, incurrirá e prestación de trabajo de un mes a un año o multa de veinte a doscientos cuarenta días "

En la interpretación del presente articulo se debe tener mucho cuidado puesto que muchas veces se confunde las instituciones Injuria y calumnia, a falta de una adecuada definición.

La palabra *DIFAMAR*, etimológicamente deriva del griego, aunque no indicaba la idea que hoy se le atribuye "quitar la fama", sino el de "divulgar cualquier cosa".

La difamación comúnmente es confundida con la injuria aun por quienes poseen una cultura media, por ello consideramos necesario su delimitación y alcance. Entre otros aspectos la difamación es también considerada como un aspecto particular de la injuria pudiéndose diferenciar como el genero y la especie.

Legislaciones como la nuestra la consignan específicamente , además de los códigos de Brasil, Republica Dominicana, Haití, Paraguay, Perú, Puerto Rico, Uruguay, Venezuela y México.

Por otra parte tienen definiciones bastante acertadas Brasil Uruguay, Venezuela, y México, siendo a nuestro juicio la mas pertinente la de , México, que en su articulo 350 indica:

"Art.350.- El delito de difamación se castigara con prisión hasta de dos años o multa de cincuenta a trescientos pesos o ambas sanciones a juicio del juez .

"La difamación consiste : en comunicar dolosamente a una o mas personas la imputación que se hace a otra persona física o personal moral en los casos previstos por la ley de un hecho cierto o falso determinado o indeterminado, que pueda causarle deshonra, descrédito perjuicio o exponerlo al desprecio[4]*"*

Si bien gramaticalmente, significa desacreditar a uno respecto a terceras personas, la difamación implica un ataque a la fama o reputación, rebajando a alguien frente a los demás, este hecho es muy frecuente en nuestro medio no es valorado en sus reales alcances sociales ni jurídicos en nuestro código, por cuanto no incluye claramente algunos aspectos importante del mismo, así lo señalan algunos de sus elementos, que conforme como lo expresaba Carrara son: Conducta dolosa, ausencia del imputado, imputación de un hecho determinado *" bien sea inmoral o criminoso"* y comunicación o divulgación de lo alegado o imputado.

En nuestro código no se menciona claramente la necesidad del dolo en la conducta como no aparece clara la exigencia de la ausencia del difamado, ni tampoco el que la difamación sea cometida a través de

[4] MÉXICO, Código Penal, para el Distrito Federal, México
Ed Porrua S.A. 1980, 33 Ed Pag 109

un medio informático, vía Internet, donde una agravante mas es la gran cantidad de usuarios que tienen acceso a esa información, mas estos aspectos consideramos que deberían estar subsanados en nuestra legislación a objeto de evitar malas interpretaciones, distorsiones y representan un vació jurídico, que disminuyen el valor de este articulo.

Si muy bien es posible, tanto teórica como prácticamente admitir que la difamación puede ser culposa o consideramos que su aclaración bien podría ser subsanada en la ley de imprenta , ya que en los países anglosajones la responsabilidad culposa es altamente considerada y atendida. Así lo demuestran muchos casos, en que publicaciones de ciertos hechos personales o sensacionales de personalidades o celebridades de la política el deporte el cine etc. Sirven para fines publicitarios y da lugar a casos innumerables de difamación culposa. Por otra parte no faltan personas que sirviéndose de la ley buscan indemnizaciones como medio de chantaje. Este aspecto creemos que debería ser considerado en nuestra legislación no solo como medio preventivo educativo, sino también como una forma de evitar que este delito sea reprimido, ya que va cobrando peligrosamente muchas victimas.

Por otra parte el gran adelanto de los medios de comunicación, la publicidad y propaganda , justifican que la difamación sea atendida con mucho cuidado y rigurosidad en nuestras disposiciones legales escuetamente expuestas en nuestro código sin tomar en cuenta previsiones que es necesario atender dado que en nuestro medio la impunidad del difamador es de alta frecuencia.

La difamación como dijimos " *consiste en revelar o divulgar un hecho, una calidad o una conducta aunque sea cierto pero que su conocimiento no tiene por que llegar a oídos de terceros y que tiene por finalidad afectar la reputación de una persona que pueda ser física o colectiva o las llamadas morales*"[5] debe necesariamente expresar que al acusado de difamación no se le admitirá ninguna prueba para acreditar la verdad de su imputación salvo en los casos ya consignados en el código mexicano que son :

I. Cuando aquella se haya hecho a un depositario o agente de la autoridad o a cualquier otra persona que haya obrado con carácter publico, si la imputación fuere relativa al ejercicio de sus funciones.

II. Cuando el hecho imputado este declarado cierto por sentencia irrevocable y el acusado obre por motivo de interés publico o por interés privado, pero legitimo y sin animo de dañar.

"En estos casos se librara de toda sanción al acusado, si probare su imputación"[6]

Convendría incluir en nuestra legislación boliviana, al igual que en la mexicana que no se aplicara sanción alguna como reo de difamación (ni de injuria), al que manifieste técnicamente su parecer sobre alguna producción literaria, artística, científica, o industrial. Tampoco al que manifieste su juicio sobre la capacidad instrucción, aptitud o conducta

[5] MIGUEL , Harb, Benjamin.
Código Penal Boliviano (comentado)
La Paz, Ed. Los amigos del libro 1979, Pag. 307
[6] MEXICO. Ob. Cit Pag 109

de otro si probase que obro en cumplimiento de un deber o por interés publico, o que con la debida reserva, lo hizo por humanidad o por prestar un servicio a persona con quien tenga parentesco o amistad dando informes que se le hubieren pedido, sino lo hiciere a sabiendas calumniosamente y el autor de un escrito presentado en un discurso pronunciado en los tribunales, pues hiciera uso de alguna expresión difamatoria o injuriosa, los jueces, según la gravedad del caso le aplicaran medidas disciplinarias que la ley le autorice.

Ciertamente que en nuestro código, en su articulo 286, se consigna la excepción de verdad y no esta de mas indicar con muchos autores, que la "*ratio essendi*" del delito de difamación, al igual que la calumnia, es la falsedad, por tanto es excepción de no punibilidad el derecho a probar la verdad de al imputación "*exceptio veritatis*".

Curiosamente el Código Penal Peruano admite la prueba de la verdad cuando la imputación difamante se ha cometido en defensa propia, aspecto que nosotros y junto a otros autores , consideramos inadmisible e injustificado.

En cuanto a la propalación de ofensas consignado en nuestro Código Boliviano en su art. 285 que a la letra dice:

" Art. 285.-(propalación de ofensas) el que propalare o reprodujere por cualquier medio hechos a que se refieren los artículos 282, 283 y 284, será sancionado como autor de los mismos ".

Consideramos que es adecuada su inclusión por cuanto no, pocos comunicadores sociales en nuestro medio arguyen consideraciones

éticas o de "secreto profesional", para justificar actos, hechos, y omisiones en las que incurren.

Debemos de hacer hincapié en este tipo de delitos que dañan y mellan, el honor, honra y reputación de las personas, pues muchos juristas en pleno ejercicio le dan muy poca relevancia, y pues contrariamente merece atención y consideración por parte de la sociedad y los administradores de justicia, ya que esta jurídicamente protegido por un cuerpo sustantivo penal.

2.5 CALUMNIA.

Analizando cuidadosamente este articulo de nuestro Código Penal podemos concluir lo siguiente:

" Art. 283.-(Calumnia) el que por cualquier medio imputare a otro falsamente la comisión de un delito será sancionado con privación de libertad de 6 meses a tres años multa de cien a trescientos días " .

Este delito que tiene como característica esencial la falsedad de la imputación, dando como cierto un hecho inexistente ya que el delito en la realidad no ha sido cometido o la atribución del hecho cierto no es delito y al qu4e se lo describe como tal, involucra para algunos autores una mayor gravedad , por cuanto al imputar, es decir atribuir a luna persona determinada conducta comisiva, constituye un ataque mas grave al honor, la honra o el crédito ajeno.

Algunos autores , con los que no compartimos criterios , manifiestan que la calumnia no es un delito contra el honor , ya que

poro su medio se sancionan tan solo las denuncias falsas que se hicieran ante los órganos de justicia. Este criterio que reduce la calumnia a lo dispuesto por el articulo 166 y siguientes del Código Penal, a nuestro juicio no es adecuado por cuanto esta tendencia se adecuaría directamente al la figura de la acción recriminatoria y no así a lo preceptuado por nuestro código que indica claramente la imputación de un delito por cualquier medio siendo este ultimo una cita general y no particular como la de otros autores que restringen indicando "ante los órganos de justicia".

El Código Penal Boliviano de 1834 como muchas legislaciones en la actualidad , precisaba que la imputación delictiva debía ser de un delito considerado publico. Nuestro código actual solo estipula que sea de un delito, sea este prescrito, entendiéndose que no hace distinciones, aunque debe ser delito o delito determinados. Este delito siempre es doloso , tanto por el dolo indirecto, directo o eventual como se puede apreciar la descripción del tipo penal en nuestro código es demasiado restringida y podría dar lugar a confusiones controversias e interpretaciones erróneas que deben ser evitadas .

Si analizamos el Código Penal Español de 1822, encontramos en el una definición muy aceptable de la calumnia en acepción amplia: *"es la imputación voluntaria de un hecho falso del que , si fuere cierto, podría resultar alguna deshonra, odiosidad o desprecio en la opinión coman, o algún otro perjuicio"*.

De acuerdo a esta definición, los elementos o requisitos inmersos en el mismo son: denuncia o propalación; falsedad de la imputación; y mala fe del propalador o denunciante.

En esta situación en particular no existe tentativa por que significaría el pensamiento o propósito no exteriorizado o manifestado, por lo tanto esta libre de toda sanción en el entendido y aplicación de un principio de derecho que dice que la sola intención no causa efectos de derecho.

Si pasamos a analizar que muchos individuos están dispuestos a sacrificar incluso su vida en caso de ver mellados su honra, honor y reputación, que constituye un patrimonio moral, será fácil concluir que existe sobrada razón para la protección jurídica de este " *bien* " (el honor) , en este entendido nuestra justicia no debe limitar recursos pues con una imputación falsa a una persona honorable se la denigra comparándola o tomándola como si se tratara de un delincuente.

Ante posibles confusiones y mal entendidos en contra de representantes del Ministerio Publico y administradores de Justicia que por su actuar podrían adecuar su conducta a este tipo penal se sugiere que el articulo motivo de análisis debería consignar que quienes por mandato legal ejerzan la función judicial no cometen el delito de calumnia pues su labor es el de coadyuvar, a la justicia.

2.6 OFENSA A LA MEMORIA DE DIFUNTOS

" Art. 287.- (ofensa a la memoria de difuntos) El que ofendiere la memoria de un difunto con expresiones difamatorias o con imputaciones calumniosas, incurrirá en las mismas penas de los dos artículos anteriores ".

Este articulo de nuestra legislación vigente, consideramos que contiene dos aspectos que deben ser tomados en cuenta.

Si muy bien con la muerte se extingue los derechos y llega al fin la personalidad, quienes por derecho de representación tienen la potestad de hacer respetar el honor de la persona fallecida son los herederos o descendientes del mismo.

El segundo aspecto reside en la imposición de la pena, pues tratándose de una persona la cual no puede asumir defensa además que sacude las fibras mas intimas del sentimiento del ser querido fallecido, hablando de los herederos, consideramos que el presente articulo deba considerarse como un agravante por las circunstancias que envuelven al hecho.

Entorno al presente articulo existen diferentes posiciones, por tanto hay autores tratadistas y legislaciones que no conciben este tipo penal, en particular el tesista no se adhiere a las precitados.

2.7 PROPALACIÓN DE OFENSAS

" Art. 285.- (propalación de ofensas) El que propalare o reprodujere por cualquier medio los hechos a que se refiere los artículos 282, 283 y 284, será sancionado como autor de los mismos ".

En este articulo, creemos que resalta otro grado de agravación de la pena por cuanto el que repite una difamación, una calumnia o una ofensa a la memoria de un difunto deberia ser considerado no solo como coautor, sino que además le añade su "*animus injuriandi*" y propala o difunde la imputación a otra persona o personas. En consecuencia se impone la agravación de la pena.

2.8 INJURIA

De la revisión en torno al presente articulo y su contenido observamos lo siguiente:

" Art. 287.- (injuria) El que por cualquier medio y de modo directo ofendiere a otro en su dignidad o decoro, incurrirá en prestación de trabajo de un mes a un año y multa de treinta a cien días "

" Si el hecho previsto en el artículo 283 y la injuria a que se refiere este articulo, fueren cometidos mediante impreso, mecanografiado, o manuscrito, su autor será considerado reo de libelo infamatorio y sancionado con multa de sesenta a ciento cincuenta días; sin perjuicio de las penas correspondientes".

La injuria a merecido múltiples y variadas consideraciones doctrinales y legislativas. Así ha sido conceptualizada en la doctrina como *"la atribución de cualquier hecho o circunstancia agraviante siempre que no se trate de delitos falsos"* y en el código español es considerada como tal *" toda expresión preferida o acción ejecutada en deshonra, descrédito o menosprecio de otra persona "* .

Diversos tratadistas han efectuado análisis sobre la injuria que podríamos haberlas glosado, sin embargo los limites de la presente tesis.

La definición de injuria insertada en el articulo 384 del Código Penal Mexicano, nos parece adecuada y creemos que debería ser insertada en nuestro código por cuanto contiene elementos

indispensables del tipo: *"injuria es toda expresión proferida o toda acción ejecutada para manifestar desprecio a otro, con el fin de hacerle una ofensa"*[7]

En la injuria se consideran los siguientes animus como causa de justificación :

a) **El animimus corrigendi aut emendandi.-** Esta causa de justificación consiste en corregir o instruir para enmendar , obrando en ejercicio de un derecho.
b) **El animus consulendi.-** Consiste en el informe o consejo para guiar la conducta ajena.
c) **El animus narrandi.-** Es la causa de justificación por la cual una persona relata hechos deshonrosos con el propósito de esclarecimiento.
d) **El animus jocandi.-** Esta justificación es una broma picara, la mofa o la diversión inocente, la burla jocunda, el dibujo o la caricatura traviesa.
e) **El animus defendendi.-** Que es la legitima defensa del patrimonio moral para prevenir o defenderse de agresiones.
f) **El animus retorquendi.-** Consiste en devolver una injuria por otra parte para salvaguardar el patrimonio moral.

Según el profesor Carrara "*en la doctrina , en el foro y en las legislaciones contemporáneas, se han venido manifestando la división de delitos de injuria en tres especies : la difamación, la contumelia y el libelo infamatorio*".[8]

[7] MEXICO, Código Penal para el Distrito Federal. México, Ed. Porrua, 1980. Pag. 108
[8] CARRARA, Francesco.
Programa de Derecho Criminal, Parte Especial

Carrara indica cuando las palabras ofensivas se pronuncian en presencia de la persona contra la cual se dirigen, la injuria se distingue con el nombre de contumelia. En este delito el daño es mínimo, por cuanto el injuriado puede volver, puede devolver o refutar o desmentir la injuria y desbaratar la maldad del ofensor.

En cuanto al libelo infamatorio, de mayor gravedad por el modo escrito, y que muchos autores conocen como pasquín, se halla previsto en nuestra legislación en forma por demás escueta y no de acorde con los nodos y medios con que actualmente pueden ser difundidas injurias.

Si revisamos la legislación Anglo Norteamericana, observaremos la presencia de dos conceptos de libelo : El libel y el slander, cuyos conceptos son mas amplios que el de los delitos contra el honor de las legislaciones latinoamericanas, ya que sancionan todo lo que puede atacar y afectar la reputación de los individuos. Es mas, la influencia de la radio y la televisión son muy tomadas en cuenta, por que pueden afectar mucho mas que cualquier medio escrito y esta contemplado en la Difamation Act de 1952 (Inglaterra) además de otras disposiciones que amplían el concepto del libel.

Infortunadamente en nuestro país pese a contar con una ley de imprenta, no se ha previsto su plena vigencia y equiparación o adecuación a modernas tendencias y en los hechos a creado un sentido vació que seria adecuado abordar . volviendo a la legislación anglo

Vol. III 5 Pag. 17. Bogota Colombia

norteamericana del libel , observamos que tres acciones son ejecutadas por los particulares :

a) Acción de carácter criminal por libelo
b) Acción civil de daños y perjuicios
c) Acción especial por libelo, cuando el libelo perjudique de alguna manera una empresa negocio, profesión u oficio.

El slander no tiene acción criminal, pero en el, debe probarse el perjuicio. En el libel es requisito esencial la difusión, ya que como bien decía Newel *" es una publicación por escrito, por impresión, por dibujos, por imágenes o por cualquier medio que pueda ser visto".*

Estos últimos aspectos de la legislación anglo americana, consideramos que deben ser asimilados e nuestra legislación, bien sea en el legislación penal, ley civil, ley de imprenta o en todos, según sea conveniente y adecuado, por que son causa de no pocos hechos delictivos en nuestro medio.

En referencia a las ofensas reciprocas insertadas en el articulo 290, consideramos que ellas son adecuadas y en buena parte de la legislación extranjera se procede de igual forma.

2.9 RETRACTACIÓN EFECTOS

En lo referente a la retractación nuestra legislación indica :

"Art.289 (retractación)El sindicante de un delito contra el honor quedara exento de pena si se retractare antes o a tiempo de prestar su indagatoria.

No se admitirá una segunda retractación sobre el mismo hecho."[7]

Como podrá observarse en este articulo. La retractación opera en nuestras disposiciones como excusa absolutoria , no obstante que los delitos contra el honor son de peligro y hasta de daño. Busca inútilmente a nuestro juicio conjurar y reparar el perjuicio, pero sin considerar que el delito ya esta consumado y realizado. Es mas consideramos que esta practica viciosa en nuestro medio, no deja a salvo la dignidad ni la reputación y menos tutela el Carbo moral del imputado.

La retractación a nuestro buen entender debería ser parte de la sanción y no una acción para eludir la acción penal como actualmente se lo hace en la practica. No consideramos que este singular y benévolo recurso para valido para el sujeto activo del delito contra el honor, que además confiesa su ligereza error o mentira quede en la impunidad bien sea antes o a tiempo de prestar su indagatoria, pues el delito esta perpetrado y merece sanción o pena.

Por mucho que se quiera no repara en su totalidad el delito cometido y en muchos casos ni siquiera es motivo inhibitorio pues quien esquiva de este modo la pena encuentra mayor estimulo para repetirlo. Si bien la retractación implica desdecirse de lo aseverado o revocar lo imputado nunca se llega al desmentido inequívoco. Algo mas muchas veces, la retractación provoca mayor difusión de los ataques

[7] BOLIVIA Código Penal Cochabamba Bolivia
Ed Serrano, 1984 Pag. 113

contra el honor y en algunos casos el remedio es peor que la enfermedad.

Otro argumento en contra de la retractación, expuesta en los términos del art. 289, es el que ciertas injurias escapan a la retractación, ya que un golpe con el que frecuentemente están asociados estos delitos, no se desdicen, la fotografía no se desmiente, el dibujo no se borra.

2.10 EXCEPCIÓN DE VERDAD

" Art. 286.- (excepción de verdad) *El autor de difamación* ***el autor de*** *difamación y calumnia no será punible si las imputaciones consistieren en afirmaciones verdaderas, pero el acusado solo podrá probar la verdad de la imputación.*

1. *Cuando se trata se ofensas dirigidas a un funcionario publico y con referencia a sus funciones.*
2. Cuando el querellante pidiere la prueba de la imputación siempre que tal prueba afectare derechos o secretos de tercera persona"[10]

Como podrá observarse, este articulo se nuestra legislación concede al acusado, autor de difamación y calumnia, la facultad de probar sus afirmaciones o imputaciones y no ser punible si estas son verdaderas, en los siguientes casos:

a) Cuando scan dirigidas a un funcionario publico y con referencia al ejercicio de sus funciones.

[10] BOLIVIA, codigo penal Cochabamba Bolivia Ed. Serrano, 1984. Pag. 112

b) Cuando el sujeto pasivo o victima convertido en querellante , pida la prueba de la imputación, en tanto no afecta derechos o secretos de otras personas.

Esta excepción concedida en esos casos, no es una excusa absolutoria, ya que es una ausencia de antijuricidad como bien afirma José Maria Rodríguez Devesa[11].

Es mas en la difamación y la calumnia lo esencial es la falsedad y *"el derecho a probar la verdad de la imputación es excepción de no punibilidad, (exceptio veritatis), pues es excluyente del dolo, resta tipicidad, otros consideran como excusa absolutoria"*

[11] RODRÍGUEZ, Devesa, Jose Maria; Derecho Penal Español, Madrid – España Parte General y especial II 8v. Ed 1980-1981 Pag.244 y ss.

CAPITULO III

EL INTERNET

CAPITULO III

EL INTERNET

3.1 COMO NACE EL INTERNET.

La palabra misma es muy inquietante, pues la revolución informática, conjuntamente con el desarrollo de nuevas tecnologías, que nos permiten en fracción de segundos tener acceso a veinte millones de usuarios, así mismo a información, intercambio de ideas, rompiendo obstáculos en el entendido que; por la comunicación, escrita, oral y hasta audiovisual, se pasa por encima cualquier barrera social, administrativa o financiera Internet la red precursora de la supercarretera de la información, es una nueva herramienta para el computo y la comunicación, además de un poderoso vehículo para el crecimiento económico.

A fines de la década de los sesenta, el departamento de defensa de los Estados Unidos, creo la ARPA (Advance Reserch Project Agency)[1] con la finalidad de llevar a cabo el objetivo estratégico, todavía sencillo, de asegurar el envío de la orden de abrir fuego desde el centro de control a las bases de misiles aun después o, mejor dicho y de hecho especialmente si las redes de comunicaciones hubieran quedado en parte destruida por un ataque. Esta misión se extendió con rapidez para

[1] HANCE Oliver y DIONNE BALZ Suzan
" Leyes y Negocios en Internet"
1ra edición, Ed. Mc Graw-Hill p.40

incluir acceso y para poder compartir todos los recursos de computo de los Estados Unidos. La Nueva red se denomino ARPAnet.

Al establecer una red en cadena a los centros de computo mas importantes y al usar información dividida en paquetes " autónomos ", fue posible configurar una estructura flexible, independiente del tipo de computadoras utilizadas. El uso de protocolos TCP/IP, que adoptaron con mucha rapidez el servicio militar en una red independiente (MILnet) y las Universidades, se fortaleció en 1984 cuando la National Science Foundation (NSF), los selecciono al crear cinco importantes centros de calculo equipados con super computadoras, con el fin de permitir a toda la comunidad cientifica tener acceso a la información almacenada entonces, cada centro universitario importante estableció una conexión con la red constituida, por la NSF, la cual fungió como un "esqueleto" o (Circuito Principal), para todo el trafico de esas subredes. De ahí en adelante fue posible ingresar a cualquier punto de la red desde cualquier sitio universitario conectado.

Con el fin de administrar e incrementar la capacidad de la red de la NSF se garantizo un contrato con MERIT NETWORK INC.,IBM Y NCL[2] en 1987. desde 1992, la NSF ha retirado su inversión, dejando asi la puerta abierta a otros tipos de financiamiento y por lo tanto a otros usos.

Internet es una federación de redes que esta en constante desarrollo y que en la actualidad es de acceso general. Después de los investigadores universitarios y de los empleados de instituciones

[2] R. RESNICK Y D. TAYLOR
" The Internet Bussines Guide: Riding the Information Superhighway to Profit"
Sams Plubishing, 1994, p. XXV

publicas, las compañias privadas y los individuos han visto ahora los beneficios que se pueden obtener viajando a través de las redes. Antes prohibido, el uso comercial se ha ido desarrollando con firmeza en los últimos años, contrariamente al espíritu inicial de Internet inspirado en sus pioneros. Hoy en día Internet experimenta un crecimiento exponencial. Mantiene unidas alrededor de 25.000 redes por el mundo y el numero de usuarios de estima alrededor de 40 millones[3].

Expuesto en el lenguaje mas simple , Internet se compone de una infraestructura compartida (Internet, la red de redes), constituida por todas las partes "hablando el mismo lenguaje (los protocolos TCP/IP) y enlazando computadoras esparcidas por todo el mundo, lo cual permite que estas computadoras se comuniquen de distintas formas (diferentes aplicaciones).

La infraestructura establecida conjunta varios medios de telecomunicaciones (desde cable telefónico hasta comunicaciones vía satélite)cada parte (universidad, institución gubernamental, proveedor de acceso, usuario final, etc, etc) es responsable del establecimiento de su red y de cubrir el costo de la conexión con otras redes. luego entonces, los usuarios independientes o empresas privadas se conectan a Internet por medio de un proveedor de acceso y ellos mismos pagan los costos de la linea telefónica para enlazarse a ese proveedor, lo mismo que los costos de suscripción al provedor, el cual esta conectado a Internet y cuyo trabajo es proporcionar acceso, es conveniente hacer una diferenciación entre los proveedores de acceso, que ofrecen un servicio de telecomunicaciones y ciertos servicios de computo y los

---

3 HANK I. ,
" Traffic Rules on Canada's information, highway : the regulatory framework for new cable and telphone services" , developpinp multimedia Products, Toronto, 2001

varios servidores en Internet, sean profesionales o no, que difunden la información por Internet.

Internet por su propia naturaleza, al estar abierta al publico en general y al utilizar protocolos de telecomunicaciones no protegidos , en ciertas aplicaciones, como el desarrollo de transacciones comerciales o el suministro de servicios de información privada, plantea problemas referentes a la confidencialidad del intercambio y al monitoreo del acceso.

Aunque el problema general se puede resolver técnicamente empleando herramientas para encriptar los datos intercambiados, esta lejos de ser insignificante, ya que en términos de seguridad y análisis de riesgo, nunca será posible lograr una situación "sin riesgos".

3.2 DETALLES TÉCNICOS

Los servicios a los que se puede tener acceso van desde la simple consulta o transferencia de documentos (FTP, Gopher, Web, ETC, ETC.)[4], hasta el uso de herramientas que permiten interactividad, mediata o inmediata, entre usuarios (correo electrónico, charla viva, etc.).

Independientemente del tipo de enlace, siempre se accede a Internet por medio de una conexión a una de las numerosas redes que la constituyen. Para usuarios individuales y empresas, esto significa, como indicábamos entrar a través de un proveedor de acceso a Internet,

[4] "The Net Investor" http://www.pawws.secapl.com/invest.html
Banknet Electronic Banking Service http://www.henix.net/mns

el cual mediante a una suscripción, proporciona acceso a su red, la cual esta, a su vez conectada a otras redes, todas las cuales constituyen Internet.

En términos prácticos, esta conexión al proveedor de acceso puede establecerse por una línea telefónica convencional (analógica o digital), mediante conexiones especiales mas apropiadas para transmisión de datos o en el caso de requerimientos mayores y mas duraderos, mediante conexiones permanentes (líneas telefónicas).

una vez conectado a la ramificación de la red, el usuario tiene acceso a los varios servicios y aplicaciones disponibles en Internet[5]. Mas aun los usuarios de Internet pueden tener acceso a sistemas telemáticos privados, algunos de los cuales implican un costo, aun que otros no. Estos sistemas son conocidos como Bulletin Board Systems (BBS) o en español Sistemas de Boletines Electrónicos. Por lo General constan de una computadora y de varios módems. Los BBS o sistemas de boletines electrónicos los utilizan tanto los usuarios individuales que desean difundir información especifica como importantes sistemas comerciales, como Compu Serve.

A continuación pasaremos a detallar ocho de las aplicaciones mas usuales dentro de lo que significa el uso del internet, en la supercarretera de la información:

[5] " The National Trade Bank "disemina alrededor de 300.000 documentos y casi 130 programas de información sobre comercio y economía. http.//www.stat.usa.gov/BEN/Service/ntdbhome.html.

3.2.1 Correo electrónico.

El correo electrónico o (e-mail), permite a los usuarios con una dirección electrónica, comunicarse entre si de la misma manera que lo hacen a través del servicio postal convencional. En términos prácticos, el mensaje del emisor de correo electrónico se envía al servidor de correo electrónico[6], (para un usuario o una compañía pequeña), por lo general, el proveedor de acceso a internet), el cual a su vez lo envía por la red al servidor del correo electrónico, del destinatario, quien a su vez abre su servidor de correo, consulta su buzón electrónico y recibe su mensaje.

Al igual que el servidor postal convencional, esta en una comunicación privada dirigida desde un punto geográfico, a otro, dentro de cierto periodo; la diferencia es que el correo electrónico llega al servidor del destinatario aproximadamente en quince minutos, después de haber sido despachado(incluso el correo electrónico enviado de París a Nueva York), y los usuarios pueden abrir su buzón varias veces al día si así lo desean . El correo erróneamente enviado puede extraviarse, pero lo común es regresa automáticamente al servidor del emisor, quien lo recupera al abrir su buzón.

Cada segundo se envían al rededor de cuatro mil mensajes por internet.

[6] http.www.latinmail.com
http.www.usanet.com

3.2.2 World Wide Web (www o Web).

Es una de las herramientas mas amigables al usuario, para la busque da y difusión de datos en Internet, fue creado por el CERN, hace cinco años y permite hacer una consulta simple de recursos gracias a los enlaces de hipertexto insertados en el texto por el autor. El enlace de hipertexto que casi siempre esta indicado en por una palabra subrayada, , enmarcada o en un color diferente, apunta a una zona distinta del servidor, o a un servidor diferente algunas veces a una distancia de 10.000 Kilómetros, en el cuerpo de un texto sobre propiedad intelectual en el marco legal, francés , por ejemplo la palabra subrayada " Copyright " puede proyectar a quien hace "clic " en ella hacia el servidor en América que aborda el mismo tema. El Web es entonces una aplicación particularmente amigable para el usuario, pues permite " navegar " en Internet, mediante saltos, de un servidor a otro en un par de segundos. El usuario puede navegar entre servidores, con la mayor flexibilidad, revisando textos, imágenes sonidos e incluso secuencias animadas. Además puede usar motores de búsqueda compuestas de enlaces de hipertexto a palabras clave que hacen referencia a otros servidores Web[7].

Desde el punto de vista del servidor este método de divulgación de datos, es muy similar a editar una revista de compra venta de muy amplia circulación, con la diferencia de que todos los usuarios pueden crear fácilmente sus servidores Web y actualizarlos en forma constante.

---

[7] P.J. BENEDICT, O'MAHONEY,
" Web Issues", Copyright Website
http.www.bendict.com/webiss,

Existen varios cientos de miles de sitios Web en el Internet y esta cantidad esta creciendo exponencialmente.

3.2.3 Telnet .

Telnet es menos amigable pero mas poderoso ; permite la emulación de terminal por la red, la cual posibilitara a una computadora tomar el control total o parcial de una computadora remota. Una computadora en Tokio puede, por Ejemplo estar controlada desde Berlín. Aun Que comúnmente se usaba para trabajo de larga distancia en la primera etapa de internet, en la actualidad se utiliza en forma esporádica, excepto por los servicios que desean poner disponibles en Internet sistemas de información que operen sobre la base de otros sistemas de búsqueda (por ejemplo la biblioteca del congreso de los Estados Unidos, Agencia de Bancos, etc., etc.)[8]

En la mayoría de los caso el uso de Telnet, esta confinado al uso de consulta de información textual.

3.2.4 FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos).

FTP es una versión reducida de Telnet. Puede utilizarse para transferir archivos de texto o de programas, entre computadoras distantes . Si el usuario tiene la autorización necesaria puede conectarse a un servidor FTP a fin de recuperar archivos, descargarlos,

first Publication, Inc. v. Rural tel. Serv. Co. Inc.

[8] WRIGHT. B.
" The Law Electronic Comerce" E.D.I. Email and Internet Technology Proof and Liability, 2da. Ed. Boston Brown & Cie, 1995

pero también para colocarlos, (cargar). Un usuario en América conectado a un servidor FTP, en Europa, puede por lo tanto con toda facilidad descargar cualquier archivo de este servidor, (una obra de Shakespeare, o un programa de software de navegación por ejemplo), o colocar cualquier archivo (sujeto a autorización del servidor) que otros usuarios pueden descargar, gracias a la aplicación FTP, amigables al usuario, esta operación es tan sencilla tanto a si como la transferencia de una unidad de HD Disco duro a un Floppy o Disco Flexible, Los Servidores FTP, por lo general incluyen una sección " Privada " [9] a la cual el acceso solo esta permitido a quienes poseen una contraseña.

3.2.5 Gopher

Entre los servidores FTP (de los cuales evolucionaron en parte) y los servidores Web, los servidores GOPHER constituyen el primer intento para integrar varios recursos de red. No obstante, aquí no lo estudiaremos pues fueron diezmados por la tormenta de la Web , Telnet, FTP y Gopher, las primeras herramientas que permitieron la constitución de " Bibliotecas electrónicas " a la disposición de bibliotecas a disposición de los usuarios mas extenso posible, están siendo gradualmente sustituidas por la web que integra y extiende las características de cada una de ellas.

3.2.6 Listas de Correo.

Una lista de correo es, valga la redundancia, una lista de usuarios que desean intercambiar ideas o información sobre temas

---

9 BENYEKHLEF, K.,
" La Protection de la Vie Privée Dans les Echanges Internationaux D'informations"
Montreal, Themis, 1992.

específicos, cualquier usuario puede crear este tipo listas. Por analogía la lista de correo es un foro para la colección y difusión de información enviada por usuarios desde sus hogares " sin tener que desplazarse ". En términos prácticos , el usuario debe suscribirse a la lista que desee, enviando un correo electrónico, estándar al administrador de la lista, indicando su deseo de suscribirse. El principio en el que descansan estas listas es muy simple : cada mensaje enviado por el correo electrónico a la lista se distribuye automáticamente a la dirección electrónica de todos los demás suscriptores ; por lo tanto , es un correo dirigido a un gran auditorio. El usuario por supuesto , es libre de iniciar correspondencia privada mediante correo electrónico común con un usuario con quien tenga contacto mediante la lista.

3.2.7 Grupos de Discusión.

El propósito de los grupos de discusión, también conocidos como foros o grupos de interés, es similar al de las listas de correo: intercambiar información e ideas sobre un tema en particular. Cualquier usuario puede crear un grupo de estos. Por analogía, un grupo de discusión es un foro de convivencia como una cafetería donde el publico asiste a conversar . No obstante la platica no ocurre en tiempo real entre los participantes. Asi podemos imaginar usuarios que van y vienen desde el mismo lugar pegando sus mensajes en la pared y leyendo los que dejaron los otros usuarios.

A diferencia de las listas de correo , los grupos de discusión no implican el correo electrónico para enviar o recibir información publica.

A lo que los usuarios tienden a referirse con el termino grupos de interés esta fuera del contexto de Internet y constituye una enorme red de información paralela pero interconectada con la mayoría de los servicios telemáticos incluyendo los de Internet.

No existe un servidor de noticias (mensajes) central ; en su lugar hay varios miles de computadoras que mantienen una copia de las noticias e intercambian sus respectivas contribuciones utilizando procesos muy complejos . Estos servidores son sincronizados varias veces en un dia sobre la base de diagramas de flujo de información manejados por administradores de sitios.

Independientemente del software utilizado, la consulta en los grupos de discusión se basa en los principios simples. Desde la lista de todos los grupos de discusión , el usuario selecciona los de su interés y se suscribe a ellos. Esta suscripción permite que el software mantenga un registro de las consultas de los usuarios . En cada una de las suscripciones , el usuario, por lo tanto , solo debe atender nuevos mensajes que le interesan . en consecuencia puede leer mensajes, agregar replicas a las noticias o responder directamente enviando correo electrónico a los autores de estas , o formular sus propias preguntas .

3.2.8 La Función de Charla IRC.

A diferencia de los grupos de discusión, la comunicación por la charla se lleva a cabo directamente entre las computadoras interconectadas y por lo tanto , solo pueden acceder a ella quienes estén conectados durante la sesión.

3.3 IMPORTANCIA DEL INTERNET EN LA ACTUALIDAD

Internet, la red de redes basada en el uso de un lenguaje de computación común o, mas precisamente en el uso de la propia familia de protocolos que permite a millones de computadoras " comunicarse entre si, que anticipa el futuro de las comunicaciones electrónicas.

No cabe duda que la apariencia y sobre todo el desarrollo de las comunicaciones electrónicas mundiales, que algunas veces se describe alegóricamente como " aldea global" " o Ciberespacio", altera sustancialmente las comunicaciones, métodos y otras características de nuestras futuras comunicaciones sin cambiar radicalmente nuestras relaciones con los demás o con el conocimiento, estos cataclismos tecnológicos que cuidadosa y rápidamente denominamos sociedad de la información ya no mas " mercado de la información " perdiendo la vista después de este paso, el hecho de que una sociedad de la comunicación" podría haber sido mas prometedora que una sociedad de la "información", no debería ser menospreciada.

Internet ya ofrece la oportunidad de ingresar a una cantidad asombrosa de información pero no ofrece conocimiento ética ni respuestas, "preprogramadas a preguntas humanas, morales o científicas. Entre la información y la decisión ; el conocimiento o la elección de vida, debe existir cierto análisis, juicio o intuición humana. Felizmente lo mas impresionante de las redes es que no nos priva de estas funciones únicas que nos permiten distinguir hasta cierto grado del reino animal y que probablemente nos confiera una misión especifica en relación a nuestro ambiente – de otras personas y como un mismo

genero desde un punto de vista pragmático, cada uno de nosotros ya puede tener acceso a tanto información como podamos clasificar, comprender, analizar, clasificar e interpretar entonces, mas necesaria que nunca es nuestra capacidad, de análisis y reflexión con el fin de procesar y "utilizar" esta información en la mayoría de nuestras esferas de actividad.

La esfera profesional tiene una necesidad vital de personas capaces de reflexionar e interpretar la información como instrumento de acción y de construcción de un destino comercial. En la esfera social, la información sigue siendo la materia prima del conocimiento colectivo, cuya elaboración requiere que el hombre en el presente como en el pasado muestre pruebas no solo de inteligencia sino también de intuición y ética. La esfera educacional también refleja esta realidad – ahora mas que nunca, es necesario enseñar a los jóvenes a asimilar, a procesar, información y sobre todo a mantener cierto grado de objetividad con respecto a la información que recibe sin ningún tipo de análisis o con un análisis parcial, si es que no cercenado.

En otras palabras, interpretar información es y seguirá siendo mas importante que recolectarla un acto que es el mas seguro en la garantía de nuestra dignidad como seres con capacidad de raciocinio.

Dado que Internet puede cumplir este papel, se ha restringido a estado de vehículo un proveedor de información en las tres esferas antes mencionadas. Por supuesto, la red debe ser capaz de ofrecer un sistema estructurado de acceso a la información, confirmando así el valor de los varios en Internet (índices, sitios altamente desarrollados en términos de enlaces de hipertexto) pero además la sociedad u la ley deben, por

medio de su intervención, ser capaces de asegurar que el sistema sea confiable tanto para aquellos que desean publicar como para los usuarios pasivos de la red, para propósitos privados u comerciales.

Hasta ahora la situación quizá parezca alarmante para los no iniciados. De hecho la mayoría de los círculos legales, y de medios ahora tienden a reclamar que no existen normas ni reglas legales, aplicables a Internet.

Sin embargo el presente trabajo no llegaría a abarcar todo el campo que abarca el campo del Internet, pues siguen existiendo áreas sombrías que necesitan ser escudriñadas.

Las leyes aplicables a Internet, contienen puntos de referencia fijos que, cuando se estudian con lógica y rigor, ofrecen soluciones a los problemas cotidianos encontrados en la red de redes, sea muy claro este punto en el entendido que existen muy pocas lagunas legales en le Derecho en Internet, pero existe un enrome vació jurisprudencial que se puede atribuir a la relativamente reciente explosión de la red.

Nunca se pierda de vista el hecho de que vivimos en un mundo en constante movimiento y nada estático, en especial la ley, por fortuna la ley que rige Internet existe; esta en completo desarrollo y se confirmara.

3.4 BOLIVIA EN EL INTERNET.

Hasta la década de los 80, el Estado era el principal administrador de los servicios básicos de la población y contaba con una importante participación en la administración de empresas productivas de bienes y servicios.

En 1985, Bolivia cambió de modelo económico y el Estado dejó de participar activamente en la economía. En este sentido, una de las principales reformas de este proceso fue la promulgación de diversas leyes como las de Capitalización y del Sistema de Regulación Sectorial (SIRESE), la modificación de la Ley Impositiva y diversas leyes sectoriales como las de Electricidad, Telecomunicaciones, Hidrocarburos, entre otras.

El cambio más significativo se produjo a partir de la promulgación de las leyes de Capitalización (del 21 de marzo de 1994) y del Sistema de Regulación Sectorial (SIRESE), Ley No. 1600 del 28 de octubre de 1994, cuyo objetivo era regular, controlar y supervisar aquellas actividades pertenecientes a los sectores de servicios básicos, entre esos, el de telecomunicaciones.

Entre los objetivos de la Capitalización en Bolivia estaba el de constituir sociedades anónimas incrementando el capital social de las empresas estatales, mediante aportes de capitales privados, con el fin de mejorar la producción y el desarrollo económico del país. Como consecuencia del proceso de capitalización, el sector de las telecomunicaciones ha experimentado importantes cambios en los últimos años.

La Empresa Nacional de Telecomunicaciones (ENTEL), principal proveedor de servicios de telecomunicaciones en Bolivia se privatiza en el año 1995, en virtud de la Ley de Capitalización. En este proceso, el grupo italiano STET adquirió el control de la gestión de ENTEL, así como el 50 por ciento de sus acciones. Con ello se han mejorado los servicios de telecomunicaciones, al promover la modernización de las redes públicas y locales y de los servicios celulares.

La Ley No. 1632 de Telecomunicaciones otorga monopolios regionales a los proveedores de servicios. En función a esta última ley ENTEL adquiere derechos exclusivos con respecto a los servicios de telecomunicaciones de larga distancia e internacionales para el periodo 1995 – 2001.

3.5 ESTRUCTURA INSTITUCIONAL DE LAS TELECOMUNICACIONES EN BOLIVIA

La formulación de políticas en el sector de las telecomunicaciones en Bolivia corresponde al Ministerio de Desarrollo Económico a través del Viceministerio de Transportes, Comunicaciones y Acronáutica Civil. La supervisión del sector es tarea de la Superintendencia de Telecomunicaciones (SITTEL), creada por Ley No. 1600 de 1994 en el marco del SIRESE.

Las principales responsabilidades de SITTEL son la utilización del espectro electromagnético, la elaboración de normas técnicas para la explotación y mejora de los servicios de telecomunicaciones, la adopción de decisiones con respecto a las normas de contabilidad aplicables a los servicios de telecomunicaciones básicas y la aprobación de tarifas, entre

otros aspectos.

3.6 BOLIVIA Y LA LIBERALIZACIÓN DE LOS SERVICIOS EN LA ORGANIZACIÓN MUNDIAL DE COMERCIO (OMC).

En el marco de la Organización Mundial de Comercio (OMC), Bolivia participó en las negociaciones sobre servicios de telecomunicaciones básicas y presentó una lista de compromisos en esta materia. Entre los más importantes están los compromisos sobre telecomunicaciones locales, de larga distancia e internacionales, con respecto a los cuales Bolivia acordó no imponer limitaciones al acceso a los mercados o trato nacional.

3.7 LA APERTURA DEL MERCADO DE TELECOMUNICACIONES EN BOLIVIA.

Tanto por los compromisos adquiridos en la Ley de Telecomunicaciones como por los asumidos ante la OMC, a partir del 28 de noviembre del año 2001, el mercado de servicios locales en Bolivia queda plenamente abierto a la competencia, donde ya no existe monopolios. El objetivo es alcanzar el servicio universal en las áreas urbanas y rurales, mejorar la calidad del servicio y disminuir las tarifas en todas las áreas. La competencia libre y legal, con el menor costo regulatorio posible será el instrumento a través del cual se obtendrán dichas mejoras.

El Plan de Apertura para el mercado de telecomunicaciones en Bolivia - aprobado mediante Decreto Supremo 26005 – autoriza a SITTEL a aplicar el procedimiento de otorgación directa de concesiones para la prestación de los siguiente servicios: telecomunicaciones locales; larga distancia nacional; larga distancia internacional; teléfonos públicos; distribución de señales y, transmisión de datos.

Este Plan establece el acceso irrestricto de nuevos operadores con la finalidad de crear una competencia abierta que derive en una mayor cobertura de los servicios de telefonía e Internet a precios bajos.

La apertura del mercado también posibilitará el ingreso de tecnología de punta. Los operadores deberán cumplir con parámetros técnicos que serán evaluados por la Superintendencia de Telecomunicaciones. Las empresas que ofrecen telefonia local, larga distancia nacional e internacional, a partir de la apertura de las telecomunicaciones rebajarán el costo de las llamadas.

La apertura de las telecomunicaciones y transformación tecnológica facilitará el acceso a Internet. Cada operador esta obligado a aportar el 3,5 por ciento de sus ingresos brutos anuales con la finalidad de lograr un acceso universal a la telefonía. Con estos fondos se posibilitará el acceso comunitario a los telecentros donde se instalará una terminal para teleducación y telesalud.

3.8 LA RED DE FIBRA ÓPTICA EN BOLIVIA

ENTEL cuenta con una red de fibra óptica[10] que se encuentra

[10] La fibra óptica apareció en 1951. Luego de 20 años la compañia Corning Glass fabricó un tipo de fibra que no presentaba pérdidas. En la de los años 80 se obtuvo una fibra con una pérdida cinco mil veces menor a

instalada en siete departamentos de los nueve que conforman la República de Bolivia. Esta conexión ha permitido ampliar las comunicaciones, no sólo al interior del país sino también al exterior del país.

ENTEL ya tiene construida su red de fibra óptica con una extensión de 3.200 kilómetros que conecta a las ciudades de La Paz, Cochabamba, Santa Cruz, Sucre, Tarija, Potosí y Oruro. En los departamentos de Beni y Pando no habrá conexión de fibra óptica debido al elevado costo que ésta significa. En estas dos regiones no existe un mercado significativo que justifique dicha inversión. Sin embargo, estas dos regiones están comunicadas vía satélite.

Bolivia, a través de ENTEL, se conecta por fibra óptica con Tambo Quemado y Chile. Este país a su vez se conecta con el cable Panamericano en sistema Modo de Transferencia Asincrónica (ATM)[11] y éste permite conectar al país con el resto del mundo.

Actualmente, frente a la apertura de las telecomunicaciones, ENTEL se disputa el negocio de las conexiones en Bolivia con la empresa americana AES.

---

la que fue creada en 1951. La materia prima para la fabricación de la fibra óptica es la arena de cuarzo, de la cual se obtiene el vidrio que es procesado en forma análoga al laminado de metales, hecho de un cristal de alto grado de transparencia. El proceso permite obtener hilos muy finos que requieren un recubrimiento. Las fibras ópticas son múltiples, es decir, un solo cable está conformado por varias fibras. Tiene muchas ventajas, entre ellas: elevado ancho de banda con lo que se puede llevar mucha información por una sola fibra. Inmunidad ante las tormentas electromagnéticas. Aislamiento eléctrico, ya que la fibra no es conductora de electricidad. Protección de la información que se envía por la fibra.

La fibra óptica es un conductor, un vidrio que utiliza la luz como medio de transmisión y no sufre interferencia electromagnéticas. Es un cable transmisor de luz. La luz viaja por medio del vidrio a 300.000 kilómetros por segundo, convirtiéndose éste en un perfecto medio de transmisión óptico de informaciones tales como datos, voz y sonido.

[11] ATM - Sistema que transporta datos, imagen y sonido en tiempo real

AES Communications Bolivia[12] se constituye en la primera competidora de la Empresa Nacional de Telecomunicaciones (ENTEL) en la oferta de telefonía de larga distancia nacional e internacional. Esta empresa comenzará a operar en telefonía de larga distancia a partir del 28 de noviembre del 2001, cuando el mercado de telecomunicaciones de Bolivia se abra a la libre competencia.

La empresa AES ha proyectado instalar 1.900 kilómetros de fibra óptica entre Corumbá, Santa Cruz, Cochabamba, La Paz y Tambo Quemado. Esta red unirá al océano Atlántico con el Pacífico y entrará en operaciones en septiembre del año 2001.

Como consecuencia, Bolivia tendrá hasta fin de año dos redes de fibra óptica a disposición de las empresas y usuarios que las necesiten. De esta manera, el país se convertirá en el eje de las telecomunicaciones en Sudamérica.

Esa situación estratégica ha motivado que dos empresas, como ENTEL y AES, que tienen el apoyo de grandes transnacionales, ejecuten proyectos ambiciosos con altas inversiones para tender sus respectivas redes. Por ello se explica que Bolivia, con un mercado tan pequeño, pueda darse la oportunidad de tener dos redes de este tipo.

En el cuadro No. 1 se pueden observar las conexiones de fibra óptica en Bolivia(Anexos).

ENTEL cuenta con una red que va desde La Paz hacia Tambo Quemado (frontera con Chile), mientras que desde Tarija nace otra red

[12] AES Communications Bolivia - filial del grupo energético estadounidense "The AES Corporations

hacia Yacuiba (frontera con la Argentina). Finalmente, se tiene planificado conectar otra desde Santa Cruz hacia Puerto Suárez. A través de esta conexión se podrá obtener lo que se llama: "los grandes anillos ópticos".

En el cuadro No. 2 se puede apreciar las conexiones de Bolivia con los países vecinos (Anexos).

Si bien la mayor red de cableado corresponde al hemisferio norte, en el sur se están haciendo esfuerzos importantes para tejer una red de fibra óptica que achique las distancias y facilite las comunicaciones. En América Latina, las redes más importantes hasta la fecha son el Columbus 1-2 y el Rioja, que comunican el nuevo continente con Europa y Africa respectivamente; el América y el St. Thomas que conecta a Estados Unidos con el Caribe, Brasil y Venezuela; y el Unisur que une zonas del Brasil, con el Río de la Plata y conecta por tierra con el Pacífico vía Chile, además de otros tendidos terrestres que empalman los espacios marinos.

3.9 SECTOR PÚBLICO

La empresa pionera en ofrecer Internet fue BOLNET, que brindó sus servicios a partir del 16 de julio de 1995. Unos meses más tarde, en diciembre del mismo año, el sector gubernamental, a través de la Empresa Nacional de Telecomunicaciones (ENTEL), que cuenta tanto con recursos públicos como privados, se constituye en otra de las empresas importantes que brinda el servicio de Internet a partir de septiembre de 1996. Ambas empresas, posteriormente, firmaron un

(NYSE:AES) – opera en 32 paises con 130 proyectos, gran parte de los cuales son del área de energia.

acuerdo para dar servicios conjuntos. Al año siguiente, otra empresa importante que comenzó a ofrecer sus servicios fue DATACOM, que inició su servicio al público a partir de agosto de 1996. Dichas empresas fueron absorbidas por el Plan Central de Internet de ENTEL llamado Entelnet.

A partir de entonces, ENTEL ha elaborado un plan global y estratégico para Bolivia para aumentar e incrementar el uso de Internet y el comercio electrónico en el país.

Para tal efecto, ENTEL ha realizado esfuerzos para potenciar su red a través de inversiones en Hardware y Software con el soporte de IBM.

ENTEL en el mes de septiembre del año 2000 inauguró un Mall Virtual (www.SonNegocios.com) para ofrecer el servicio de comercio electrónico, dirigido al sector de la Pequeña, Mediana y Gran Empresa.

El objetivo de esta propuesta era desarrollar conjuntamente con el cliente una tienda virtual, que estaría ubicada en el Mall Virtual de ENTEL S.A. para ofrecer el servicio de comercio electrónico. El mencionado portal tiene cuatro tipos de tiendas: i) tienda inicial, recomendada para la mayoría de los comercios que deseen tener presencia en este portal; ii) tienda intermedia, para empresas que tengan un número considerable de productos en cartera; iii) tienda Pro, para empresas que tengan un número considerable de productos en cartera y iv) tienda remota, para empresas que tengan un sitio WEB ya en funcionamiento y que sólo requieran las funcionalidades del Servidor de Pagos (Payment Server).

Por otra parte, entre las labores que realiza el gobierno para participar activamente en el uso de esta tecnología de la informática, se puede destacar la implementación de sistemas e infraestructura informática en las entidades del sector público.

En este sentido, el Ministerio de Hacienda, en cumplimiento de las atribuciones que el artículo 20 de la Ley 1178[13] le confiere, ha encomendado al proyecto de Descentralización Financiera y Responsabilidad, ILACO II, el desarrollo de un sistema integrado de gestión y registro automático de las operaciones de los sistemas establecidos en la citada ley y asimismo, la utilización de la operatoria de la cuenta única del Tesoro, en el sistema de Tesorería, para su aplicación en todo el sector público.

El Proyecto de Descentralización Financiera ILACO II ha desarrollado el Sistema Integrado de Gestión y Modernización Administrativa (SIGMA), orientado a instrumentar los sistemas que regula la Ley 1178, articulando y operacionalizando los preceptos de centralización normativa, descentralización operativa e integración de sistemas.

El sistema SIGMA está compuesto por sistemas de presupuesto, contabilidad, tesorería, crédito público, compras y contrataciones, manejo y disposición de bienes y administración de personal, que se

[13] La Ley 1178 de Administración y Control Gubernamental, promulgada el 20 de julio de 1990, establece sistema de administración para programar, ejecutar y determinar los resultados y controlar la gestión del sector público, definiendo en su artículo 22 que el Ministerio de Hacienda es la autoridad fiscal y órgano rector de los sistemas de programación de operaciones, organización administrativa, presupuesto, administración de personal, administración de bienes y servicios, tesorería, crédito público y contabilidad integrada.

implantarán con carácter obligatorio en todas las entidades del sector público, según prevé el artículo 3 de la Ley 1178.

La implantación de este sistema se está realizando en dos fases: una primera a partir de enero de 2001 en todas las entidades de la administración central. Y una segunda, a partir de junio, del mismo año, en el resto de entidades del sector público.

Por otro lado, el gobierno está trabajando en la implementación de sistemas informáticos en otras instituciones como en la Aduana Nacional, a través de la instalación de un sistema integrado de control de comercio exterior, llamado "Sistema Aduanero Automatizado" (SIDUNEA). Este sistema utiliza redes informáticas entre esta entidad y sus diversos puestos fronterizos en todo el país, de tal manera, de lograr una intercomunicación, no sólo en cuanto a información, sino también en cuanto a la realización de trámites, envío y recibo de documentación.

Muchas instituciones públicas cuentan con su página web, por medio de la cual ofrecen información y/o los servicios que proveen. Tenemos el caso del Instituto Nacional de Estadísticas que, a través de su página web, brinda información estadística del país. Lo propio ocurre con casi todos los Ministerios del Poder Ejecutivo.

Otra entidad importante es el Servicio Nacional de Impuestos Internos que, en su proceso de modernización institucional, ha iniciado un servicio basado en un nuevo concepto de gestión integrado, orientado al servicio del contribuyente, que ofrece información de inmediata disponibilidad de sus usuarios y control efectivo de las

obligaciones de los contribuyentes.

Este proceso de modernización se soporta en dos aspectos fundamentales:

i) Incorporación de tecnología de punta, por medio de la utilización de metodologías modernas de desarrollo informático, del uso y aplicación de herramientas de software de última generación, y de la instalación de hardware de alta calidad y desempeño.

ii) Reingeniería de los procesos de las áreas de Recaudación, Fiscalización y Jurídica.

La orientación del proceso de modernización pretende ofrecer nuevos servicios, tanto a los funcionarios como a los contribuyentes, de manera de hacer más sencillos, ágiles y transparentes los trámites dentro de la administración pública, como a mejorar sustancialmente el control garantizando mayor exactitud y oportunidad en las operaciones.

Existen otras reparticiones públicas entre las que se puede mencionar al Servicio Nacional de Propiedad Intelectual (SENAPI), que está trabajando en un proyecto para velar por la propiedad intelectual de los bienes que se comercializan a través de comercio electrónico.

3.9.1 Salud

Los doctores del Hospital Japonés de Santa Cruz, figuran entre el número creciente de médicos de Bolivia que estiman que Internet podría

conducir al sector sanitario a dar pasos agigantados. Por esta razón han consagrado un volumen considerable de recursos a la construcción de la capacidad de Internet en su hospital.

Esta es una de las pocas instituciones que se ha integrado a la red en la realización de sus actividades. En este hospital se imparte capacitación a los estudiantes no solamente en lo que concierne a la práctica de medicina, sino en la capacitación en comunicaciones y ciencias informáticas.

Una vez graduados los nuevos doctores se trasladan a instituciones de salud ubicadas en diferentes regiones del país y pueden mantener contactos periódicos y frecuentes con profesionales del Hospital Japonés a través de Internet.

Por otro lado el hospital ha incorporado una parte de su programa educativo en Internet, con el objetivo de impartir capacitación a profesionales que habitan fuera de Santa Cruz.

3.9.2 Educación

sitios en Internet y dentro de las 40 universidades privadas existentes en Bolivia, al menos siete han abierto sitios en la red.

Varias universidades están avanzando en el establecimiento de ciertas condiciones para democratizar el acceso a Internet una de ellas es la Universidad Católica Boliviana (UCB) que, por ejemplo, ha adoptado la política de conceder cuentas de correo electrónico a todo su personal y la mayoría de sus estudiantes.

De acuerdo al estudio realizado por la UIT, los obstáculos con los cuáles tropiezan los sectores educativos para financiar los servicios de Internet son, comparativamente mayores, con respecto a otros países. Bolivia carece de políticas que establezcan las condiciones necesarias para que el acceso a este instrumento por parte de instituciones educativas sea, en lo económico, más bajo.

3.9.3 Comercio

En 1999 en América Latina se efectuaron transacciones a través de Internet por 200 millones de dólares, la participación de nuestro país en esta cifra es minúscula.

Existen, sin embargo, una serie de condiciones que en vez de ser vistas como obstáculos, pueden ser vistas como oportunidades. El hecho de que Bolivia sea un país mediterráneo, es una interesante oportunidad para que se desarrolle en el ámbito del comercio electrónico. El Internet en este caso se convertiría en uno de los instrumentos más idóneos para superar este tipo de barreras físicas.

Una de las propuestas más alentadoras de comercio electrónico en Bolivia es la ofrecida por *Bolivia Mall,* sitio que fue fundado en 1998 y que está destinado a bolivianos que viven en el extranjero.

3.9.4 Medios de Comunicación

El panorama más alentador en cuanto a medios de comunicación es el de la prensa: Al menos seis de los diarios nacionales cuentan con sitios en la *web* en los mismos incluyen ficheros Y, noticias actualizadas.

La radio en Bolivia es quizá uno de los medios más poderosos, esto por el bajo costo de los receptores y la alta penetración entre las poblaciones analfabetas. Sin embargo, sólo unas cuantas estaciones de radio cuentan con sitios en Internet, algunas de ellas proporcionan flujo radiofónico (audio).

La televisión cuenta hoy en día con más de 50 estaciones y más de la mitad se transmiten en las ciudades de La Paz, Santa Cruz y Cochabamba. No existen estrategias comerciales destinadas a promocionar servicios de televisión a través de Internet mediante módem en un futuro inmediato

3.9.5 INTERNET EN LO MUNICIPIOS

"Soluziona" desarrolla el portal en Internet de los municipios de Bolivia Santiago, Chile. Soluziona, a través de su área de servicios Internet, acaba de finalizar el desarrollo del portal que facilitará la comunicación virtual entre 314 municipios de Bolivia.

El proyecto es una iniciativa de la Agencia de Cooperación de Estados Unidos (USAID), y la Asociación de Administradores Municipales de Estados Unidos para la Asociación de Administradores municipales de Bolivia. Su objetivo es modernizar, agilizar e integrar la gestión entre los ayuntamientos del país andino, aprovechando los recursos que proporcionan las nuevas tecnologías de Internet.

El portal fue presentado este mes en el Museo de La Paz de Bolivia ante la presencia del presidente de la República, Jorge Quiroga, y diversas autoridades gubernamentales. "Esta iniciativa es una forma

de unir a los municipios, de hacer fuerza conjunta para avanzar hacia el desarrollo", señaló el máximo mandatario del país en el acto de inauguración.

La plataforma permitirá homogeneizar todos los procedimientos de actuación así como seleccionar y compartir los recursos y soluciones más eficaces para la gestión municipal diaria, gracias a la puesta en común e intercambio de información y experiencias de todos entre los municipios implicados.

3.10 Sector Privado

En cuanto al sector privado, cabe destacar que en Bolivia existen otros proveedores, además de ENTEL que brindan el servicio de Internet. Muchas de estas empresas brindan el servicio a través de servidores ubicados en otros países, principalmente en Estados Unidos.

En el uso de esta tecnología, el sistema bancario juega un papel trascendental. En este sentido, los Administradores de Tarjetas de Crédito (ATC) en Bolivia, han implementado el Sistema de Transacción Electrónica Segura (SET) y el Security Socket Lawer (SSL), que le permiten dar seguridad y garantías a los usuarios respecto de sus transacciones.

En Bolivia, los medios de pago electrónicos con los que se cuenta en el sistema bancario son: las tarjetas de crédito[14] y los cheques en línea a través de la Cámara de Compensación Electrónica[15].

En el sector privado, las Cámaras de Comercio e Industria también constituyen sectores importantes en el uso de esta tecnología de la informática porque poseen bases de datos globales de las empresas privadas nacionales. En dichas cámaras están trabajando en un proyecto para convertirse en entidades subsidiarias de certificación digital a nivel nacional. Este proyecto se encuentra en marcha y podría empezar a funcionar el 2001.

Existen otras iniciativas sobre comercio electrónico como el caso de Bolivia Mall, a través del cual se puede comprar productos nacionales desde cualquier lugar del mundo. Esta iniciativa privada nace en 1998[16] y tiene proyecciones de ampliar su mercado a través de estudios de mercado, publicidad. También se puede destacar la presencia de la empresa "Bolivia Store" con productos nacionales.

Ultimamente, se han creado nuevos portales como Bolivia.com; Boliviaunder.ground.com; Yapues.com etc., que ofrecen diversos

---

[14]En referencia a las Tarjetas de Crédito, en Bolivia es posible cobrar o pagar a través de las mismas por bienes o servicios prestados,. Sin embargo, aún no existe un comercio electrónico con las caracteristicas tecnicas y de seguridad que se manejan a nivel internacional.

[15]A partir de 1992, Asociación de Bancos (ASOBAN) incorpora un proceso de compensación de cheques en línea a través de la Cámara de Compensación Electrónica, en el cual, se aplica tecnología de punta en Software, Hardware y Comunicaciones para Cámara de Compensación Electrónica. El sistema de comunicación para la Cámara de Compensación Electrónica cuenta con el soporte técnico de la Empresa Nacional de Telecomunicaciones (ENTEL). Esta Empresa provee la red privada de fibra óptica, los circuitos de France Relay y los equipos de comunicación necesarios para la nueva red interbancaria de Bolivia asi como todos los otros servicios de comunicación complementarios, instalados en La Paz, Cochabamba y Santa Cruz. El sistema permite, además que la Asociacion de Bancos (ASOBAN) pueda garantizar un procesamiento continuo, seguro y eficiente para mantener en linea la información de la Cámara.

servicios. Entre ellos, se pueden mencionar recetas bolivianas de comidas típicas, información general sobre Bolivia, sectores de debates en diversos temas, páginas para encontrar trabajo, correos electrónicos, chat, deportes y turismo.

También se ha dado en las capitales de Departamento, principalmente, una proliferación de los cafés con acceso a Internet. Esto ha contribuido a que exista un mayor número de usuarios de Internet. Los costos en dichos cafés han permitido este acceso puesto que tienen precios módicos para el público.

CAPITULO IV

LA CRIMINOLOGÍA Y EL DELITO INFORMÁTICO

CAPITULO IV

LA CRIMINOLOGÍA Y EL DELITO INFORMÁTICO:

Dado que es profusa la literatura sobre los denominados delitos informáticos, es menester encarar desde el punto de vista criminológico, el estudio sobre la perpetración de conductas que, sucedidas o nó a través de la red, pueden llegar a constituir ilícitos penales, de existir una legislación que así los contemple. La exposición se centrará, no sólo en el "delito" sino en los aspectos criminológicos sociológicos y hasta psicológicos del tema.

El concepto de delito, sea informático o computacional, procura la elaboración de distintas definiciones y apreciaciones del fenómeno de la informática, y de internet como ámbito para el desarrollo y/o configuración de maniobras, sus repercusiones, modalidades etc.-[1], tratando todos estos puntos conjuntamente. Veremos, su aspecto criminológico.

Si bien los autores y estudiosos elaboran inteligentes pautas y cursos de acción posibles para el estudio de lo que se considera el delito informático. Por ello puede ser de utilidad responder a los interrogantes precedentes y sólo una ciencia puede hacerlo: la criminología como aquélla que ..."pregunta por las causas del crimen, su génesis y

[1] GARCIA MOLINA, PABLO
"Informática y Derecho Penal",
cit., p. 43-44

condiciones, inquiriendo por los factores del hecho delictivo para alumbrar con este estudio el germen que le da vida inicial" según textuales palabras del "maestro" Miguel Herrera Figueroa.[2]

4.1 CRIMINOLOGÍA

A los efectos del presente se ofrecen algunos conceptos de CRIMINOLOGÍA como el referido a su existencia en una *"enciclopedia de las ciencias penales"* entendida ésta *como "conjunto de saberes que de una u otra forma se ocupa del delito y de la pena"*[3] incluyéndola con carácter de ciencia *"principalmente causal explicativa"* citando al Dr. Jiménez de Asúa pág. 19 y sus de *"Elementos..."*.

Con relación a esta ciencia, se han elaborado también conceptos amplios como aquél que dice que es un conjunto indiscriminado de asuntos acerca del crimen y la engloba con la política criminal, antropología y otras ciencias como la Criminalística, también se restringieron criterios como el de la escuela austríaca que la circunscribe a *"a la teoría de las formas reales de comisión de delito y de la lucha contra el delito"*[4].

Restringiendo aún más el concepto también se ha dicho que es la ...."*ciencia sintética que estudia las causas de la criminalidad, tanto en su expresión individual como social"* llegando a considera que su objeto está

---

[2] HERRERA FIGUEROA, Miguel
" Psicología y Criminología"
pág. 97 y ss.
[3] DE RIVACOBA Y RIVACOBA, Manuel
"Elementos de Criminología"
Edeval 1982
[4] ob.cit. de Seelig

constituido por el delito mismo y no por sus causas o sea éste explicado por sus causas.

Ocurre que esta concepción de ciencia causal-explicativa, dificultaba el estudio del objeto de la criminología el cual venía dado por las leyes penales (criminalización primaria ...*"acto y efecto de sancionar una ley penal material"*), y obedecía a una concepción positivista (que venía de Cesare Lombroso), dado que la criminología se consideraba una ciencia con un objeto que se lo definía el poder político *"el delito"*.

Esa concepción *buscaba "causas frente a un derecho penal que presuponía una capacidad humana de elección"* y tenía una historia propia[5] y frente a ella, aparece la de la criminología como reacción social y surge definido su ámbito como la *"comprensión critica de la sociedad global y de la teoría social más general y no simplemente el estudio de algún grupo marginal, exótico o esotérico...."* y que sirve como campo propicio para exponer *"ideas sociológicas y filosóficas"* [6]así si va superando el aislamiento de la criminología de la política criminal y del derecho penal vinculándose definitivamente éste con otras ciencias penales.

Dado así un pantallazo sobre la criminología ensayaremos su importancia con relación al mundo de la informática.

4.2 CRIMINALIDAD E INFORMÁTICA.

---

5 RAÚL ZAFFARONI, Eugenio ob.cit.,
"Manual de derecho Penal" Parte General
pág.118-Edigraf 1987 y ver también "Derecho Penal" Parte General Ediar -2000.

6,P.WALTON - YOUNG , I. TAYLOR - J,
"La nueva criminología" (Contribución a una teoría social de la conducta desviada)
pág.12 -amorrortu 1990.

Con relación a este tópico a juzgar por los estereotipos que van apareciendo que colocan a los sujetos autores de los ilícitos cometidos a través de la informática y en especial de Internet como una especie de *"delincuentes"* y por las connotaciones que toman algunas maniobras que causan daños varios en ese medio, es evidente que se está ante una nueva forma de criminalidad.

El continuo avance de la tecnología en el mundo globalizado está provocando un fenómeno de poder que desborda a los poderes políticos locales y no resulta fácil hallar paliativo a conflictos como éste en el que las acciones criminales trascienden los límites locales.

No debe descartarse, que los intereses políticos que, desde siempre han estado en juego, los factores de poder que inciden en esta temática (porqué no como condicionantes?, coadyuvan frustrando o impidiendo una punibilidad que no todos los sectores de la sociedad se avienen a aceptar, (algo parecido a lo que sucede con el *"delito económico"*).

Estas consideraciones y las que seguiremos desarrollando en cada ítem nos llevan a pensar que efectivamente nace una nueva forma de criminalidad y a ver cómo la ciencia que la estudia –criminología- sufre la dinámica de los sucesivos cambios sociales en este caso los producidos por la tecnología.

Podemos ensayar los factores condicionantes que operan al respecto formulando una clasificación que considera:

4.3 CAUSAS DE CRIMINALIDAD

Si tomamos las acciones que se producen en Internet como todas aquellas que vulneran la privacidad de determinados datos, y las conductas perjudiciales que se efectivizan utilizando el medio informático en general, vemos que su causa puede obedecer a factores:

4.3.1 FAMILIARES:

El nivel social al que pertenecen los sujetos que pueblan el mundo de la informática, por lo general es de medio a alto por cuanto provienen de una extracción que les pudo proporcionar estas herramientas para alcanzar las metas que la cultura social les estaba proponiendo.

Así el acceso a la tecnología no es propio de las zonas marginales pues pese a los denodados esfuerzos gubernamentales de lograr llevar la computación (y el uso de Internet) hacia todos los rincones del país y del mundo, no es fácil aún encontrar a niños del Altiplano accediendo a ellos.

4.3.2 SOCIALES:

Se destaca la raigambre condicionante que va adquiriendo la ambición de Poder y riqueza como metas primordiales de la sociedad de consumo en particular en las clases nombradas.

La tendencia al agrupamiento o formación de "grupos económicos"[7] en continua expansión y la globalización de la economía son factores que dieron plafón al crecimiento de la informática y paralelamente la aparición de Internet con las ventajas que ello les ofrecía, en una palabra el incremento de la tecnología de las comunicaciones que permitieron transacciones en segundos conllevaron a un mayor poder económico y político extranacional[8].

Con relación a este tipo de criminalidad, no estamos armando a su respecto un derecho penal del autor, sino se trata de un esbozo desde el punto de vista criminológico sobre los que pueden agregarse otras reflexiones que ya han sido evaluadas por los estudiosos en la materia, y sería ocioso repetir.

Se puede aceptar una referencia al crimen ocupacional, o sea el cometido a través de ciertas ocupaciones o profesiones tema al que se viene haciendo alusión ya desde 1930 y que bien puede aplicársele.
Lo dicho sin soslayar la importancia que tienen las organizaciones que son quienes dictan los valores a los que adhiere la sociedad.

Es decir desde que surge el auge de la informática es notorio que todo aquél que desconoce el manejo de una computadora cae en la obsolescencia y ya desde muy pequeños se les inculca a los niños iniciarse en ese tema que a su vez por las características técnicas que presenta requiere de ciertas condiciones de aptitud para encararlas y

---

[7] TIEDEMANN, Klaus,
"Poder Económico y Delito"
Edit. Ariel, Barcelona, 1985, pag. 122.

[8] ALCONADA ARAMBURU, Carlos R. S.
"El caso Swift Deltec -La reparación judicial de una agresion económica foránea".
La Ley-1973.

que facilitan la agilidad mental de modo que va haciendo nacer en el sujeto el deseo de ser ese prototipo del ideal actual de la comunidad (obsérvese a jovencitos en el estímulo que ya sienten *"ganando a la computadora"* en cualquier juego).

El acrecentamiento de esos dictados unidos a la avidez que trae la sociedad consumista y la endebles de ciertas pautas de valoración pueden considerarse distintas fuerzas que conducen a producir desviaciones de conductas como las que se intenta analizar.

Podría aplicarse aquello que en estos casos los *"apetitos irrestrictos de la conciencia individual ya no están controlados, empieza a funcionar el egoísmo"*...y *"los sujetos están decididos a asumir su propio rol en esta división de trabajo no espontánea, donde la riqueza es una de las metas"*, siendo así que el agoísmo actúa como precursor directo de tal desviación [9].

Por ello podría considerarse una esquematización de las causas de estos procederes y también distinguirlos en inmediatas y mediatas.
Entre las primeras se elabora, a sus vez, una :

4.4 TIPOLOGÍA DE CONDUCTAS.

En un enfoque más sociológico del tema distinguiremos :

- maniobras y

[9] Durkehuu, Emile ob.cit
"La Nueva Criminologia"
. pág. 104.

- delitos (con la salvedad que, careciendo nuestro país de una legislación penal al respecto el término delito informático no resulta aplicable).

A su vez esas maniobras pueden producirse afectando el ámbito público como privado, y las conductas adoptan casi siempre una modalidad individual aunque pueden ser también grupales. Continuando con esta tipología definimos maniobra como acción que se lleva a cabo con habilidad para conseguir un determinado fin Táctica (en ejercicios militares) como una de las acepciones del vocablo.

Se llevan a cabo con el fin de perjudicar a otro y beneficiarse sea a sí mismo o usurpar derechos y/o eludir obligaciones. En una palabra son conductas destinadas al engaño.

En todos los casos dicha conducta posee un patrón[10]: la inescrupulosidad no importándole el efecto del proceder ni la manipulación que hace de sus ocasionales víctimas.(caso de la intromisión en un sistema o de su destrucción por un "virus") .

Se trata de conductas que, practicadas a través del uso personal de una computadora repercuten en el ámbito socio jurídico, algunas no sólo afectan al patrimonio privado (compras electrónicas utilizando datos de una tarjeta ajena por ejemplo) .y en otros casos hasta afecta patrimonios nacionales y/o bien causan daños de otra especie no susceptibles de valoración económica.

---

[10] BARATTA, Alessandro,
"Criminología Crítica y Crítica del Derecho Penal",
Siglo XXI , Editores, pp. 83 y ss

Otra división en lo que hasta ahora llamamos "maniobras" se refiere entonces al modo de comisión (sería una consecuencia de lo anterior) o sea pueden practicarse en pequeña escala y en gran escala.

En pequeña escala: fraudes individuales al comercio minorista, ofrecimiento de servicios induciendo con una falsa imagen, y en Gran escala: se trata de aquéllas maniobras que suceden a nivel estatal o en grandes corporaciones y/o industrias, capaces de afectar tanto el orden político interno como externo, o producir un ataque masivo a datos confidenciales empresariales redundando en un perjuicio económico o político. Es el caso de empleados infieles que logran penetrar en secretos del sistema provocando, desde el daño al mismo, hasta violaciones a esa información confidencial logrando ingresar a circuitos presuntamente invulnerables y/o causar ataques masivos sobre datos con posibilidad de producir daños económicos de importancia .

También podemos señalar y se aplicaría para ambos casos: acciones destinadas a obtener ventajas a través de la ocupación sea en el :

4.4.1 ÁMBITO PRIVADO:

Caso de altos jefes de empresas que venden información, previa sustracción del sistema para lucrar con ella, (espionaje informático)[11] y también mediante este mecanismo pueden instalar su propio negocio, hasta venta de influencias a través de la red . y en el .

---

11 SIEBER, Ulrich,
"The International Handbook on Computer Crime",
Ed. John Wiley & sons Ltd., 1986, Great Britain, 1986.

4.4.2 ÁMBITO PÚBLICO:

Cuando hacen una utilización desaprensiva de la persona jurídica creada al efecto de burlar intereses pecuniarios, como operaciones bajo el nombre de sociedades ficticias para producir rápidas transacciones, o perpetran maniobras en los sistemas de bancos u otras entidades financieras, públicas o privadas, (alteración a un sistema bancario para lograr ocultamiento de evidencias al efectuar transferencias de fondos a cuentas personales).

Es característica común de esta tipología de conductas el sentido de la oportunidad que evidencian sus autores en todos los casos y su claridad de juicio: hay especificidad técnica y alto grado de conocimientos así como capacitación por la práctica que otorga el uso permanente de una computadora. Es público y notorio que a veces se ha llegado a hablar de "adicción a la misma" por el grado de contracción que provoca en sus usuarios y en especial los más jóvenes ante el descubrimiento de sus posibilidades.

4.5 OBJETIVOS CRIMINALES.

4.5.1 OBJETIVOS INMEDIATOS:

La posibilidad de obtener beneficios, que pueden no ser económicos, en los que está presente el factor "poder" que involucra este manipuleo de personas y/o entes.

La asunción desinhibida de riesgos que ello implica, y las débiles o escasas consecuencias jurídicas, o bien dicho la falta de impunidad de

que gozan la mayoría casi siempre y que circunscriben el terreno a las simples maniobras o a "hechos" de consecuencias a veces civiles.

Si nos referimos a **delitos** que puedan cometerse encontramos que pueden ser ilícitos pluri ofensivos (fraudes a la industria y comercio por ej.) y violaciones en entes públicos, como se vio, (bancos, entidades financieras no bancarias) organismos recaudadores, donde al introducirse violan normativas específicas en una conducta merecedora de reproche penal.

También pueden efectuarse fraudes con tarjetas de crédito, evasiones impositivas, y vaciamientos a través de transferencias electrónicas de fondos, como desvíos a cuentas personales, apropiación de información con consecuencias económicas o no, violación de secretos de estado, en una gama de conductas que, como las vistas en apretada síntesis muestran como común denominador la especificidad, el dominio de conocimientos informáticos lo que autorizarían a configurar estos hechos, de tipificarse de alguna forma, como delitos especiales impropios.

No soslayamos la ejecución de delitos de carácter financiero cuando estas conductas tienen lugar en entes que intermedian entre la oferta y la demanda y estos sujetos pueden interferir entre ellos provocando desde bajas de acciones hasta caos financieros a niveles superiores o perpetrar falseamientos de datos contables,y/o lavado de dinero.

Estos tipos conllevan especialmente el manejo del factor "poder" que desean adquirir sus autores, sin desmerecer la ambición de riqueza que los mantiene en estas actividades.

4.5.2 OBJETIVOS MEDIATOS:

El dictado de normas legales específicas o leyes penales a fin de tipificar esa amplia gama de conductas que a falta de estigmatización sólo son censuradas con la crítica e indignación que provocan y la más de las veces quedan discriminadas.

4.6 DELITOS INFORMÁTICOS:

Dentro de la generalidad de este análisis que reclama una mayor profundización, se hace necesario respondernos a la pregunta ¿Que debemos entender por delitos informáticos? Y para ello debemos partir por la reflexión del profesor August Bequai, en su intervención: Computer related crimes ante el Concejo de Europa, quién señalo:

Si prosigue el desorden político mundial, las redes de cómputo globales y los sistemas de telecomunicaciones atraerán seguramente la ira de terroristas facinerosos.....Las guerras del mañana serán ganadas o pérdidas en nuestros centros de cómputo, más que en los campos de batalla. ¡La destrucción de los sistemas de central de una nación desarrollada podría conducir a la edad del oscurantismo!. En 1984, De Orwell, señalaba: "*los ciudadanos de Oceanía vivían bajo la mirada vigilante del Hermano Grande y su policía secreta, en el mundo moderno, todos nos encontramos bajo el ojo inquisidor de nuestros gigantes sistemas computacionales. En Occidente, la diferencia entre el* Hermano

Grande y nuestra realidad es la delicada fibra política llamada democracia; de colapsarse ésta, el edificio electrónico para una implantación dictatorial ya existe....La revolución de la electrónica y la computación ha dado a un pequeño grupo de tecnócratas un monopolio sobre flujo de información mundial. En la sociedad informatizada, el poder y la riqueza están convirtiéndose cada vez más en sinónimos de control sobre los bancos de datos. Somos ahora testigos del surgimiento de una elite informática"

Por otra parte si nosotros entendemos el concepto de Delito como toda acción destinada a violar alguna ley específica, debemos entender el concepto de Delito Informático como cualquier acción ilegal en que una computadora es una herramienta u objeto del delito; en otras palabras, cualquier delito en que los medios o propósitos en que se pretende alterar la función de la computadora. También puede ser: cualquier incidente asociado con tecnología de cómputo en que una víctima sufre o puede sufrir la pérdida y una intromisión intencional, propiciando o pudiendo propiciar una ganancia.

A nivel internacional, se considera que no existe una definición determinada de Delito Informático, sin embargo en la doctrina podemos encontrar algunos intentos para llegar a la mencionada definición:

"..No es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los Códigos Penales, lo cual en la mayoría de los casos no sucede.... en

consecuencia se conceptualiza el delito informático en forma típica y atípica, entendiendo por la primera a las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin. Y por las segundas a toda actitud ilícita en que se tiene a las computadoras como instrumento o como fin". **(Julio Tellez Valdés)**[12]

" ..Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo" **(Carlos Sarzana)**

"...Aquel que se da con la ayuda de la informática o de técnicas anexas..." **(Nidia Callegari)**

"...La realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española."
(Rafael Fernandez Calvo)

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

---

[12] TELLEZ VALDEZ, Julio.
"Derecho Informático"
Ed. Mac Graw Hill. 1996 - Mexico D.F..

4.6.1 SUJETO ACTIVO DE LOS DELITOS INFORMÁTICOS:

Las personas que incurren en estas acciones delictuosas poseen características comunes que los diferencian del común de los delincuentes, todos poseen habilidades para el manejo de los sistemas informáticos y por su situación ocupacional, por regla general, se encuentran en lugares donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Sus características los hacen similares a los denominados *"delincuentes de cuello blanco"*.

Puede hallarse en las formas de perpetración:

Individuales: Se trata de sujetos que actúan solitariamente, a veces en forma temporalmente aislada, pero sin asociarse siendo otra característica que a veces su formación es autodidacta y sólo les basta su habilidad y rapidez con los ordenadores, a diferencia del estafador común que por lo general puede acusar rasgos determinados como su encanto personal y despliegue de seducción, gustos refinados, que debe hacer a efectos de captar a sus posibles víctimas.

Acá se trata de seres que no pueden seducir a nadie visualmente y se mueven en el anonimato que otorga la invisibilidad, no pudiendo descartarse (ya en un enfoque psicológico del tema, válido si consideramos la necesidad de la inter disciplina a fin de aunar esfuerzos en pro del derecho penal), una naturaleza violenta dominada por la

frialdad de su actitud y repito claridad de criterio que los hace ser los mejores en lo suyo.

Conductas colectivas: o agrupadas se dan en los casos en que interactúan con *"socios"* que los secundan o dirigen en sus quehaceres con la facilidad en este ámbito, y para ellos, que pueden hallarse simultáneamente en lugares físicos diferentes para llevar a cabo la conducta, lo que sofistica el proceder.

4.6.2 SUJETO PASIVO DE LOS DELITOS INFORMÁTICOS:

Las víctimas de los delitos son aquellas personas o el ente sobre el cual recae la conducta, acción u omisión que realiza el sujeto activo y en este tipo de delitos pueden ser personas físicas, instituciones crediticias, gobiernos, etc, que usen sistemas automatizados de información, generalmente conectados a otros. Es de suma importancia conocer las características de los sujetos pasivos de este tipo de delitos, toda vez que para conseguir una prevención efectiva de la criminalidad informática se requiere en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

4.6.3 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS:

Julio Téllez Valdés clasifica a los delitos informáticos[13] en base a dos criterios, como instrumento o medio o como fin u objetivo.

1.- Como instrumento o medio: Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

2.- Como fin u objetivo: En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

4.6.3.1 FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS:

Constituye una forma de delito informático reconocido por Naciones Unidas y dentro de este concepto general se engloban la Manipulación de los datos de entrada, la Manipulación de Programas, Manipulación de los datos de salida, Fraude efectuado por manipulación informática.

a) FRAUDE CON TARJETAS DE CRÉDITO

Otra forma muy común de hacer mal uso de las líneas de Internet es utilizándola para robar número de tarjetas de crédito. Internet es

[13] 13 TELLEZ VALDEZ, Julio.
"Derecho Informático"
Ed. Mac Graw Hill. 1996 - Mexico D.F..

una gran red que aparte de funcionar para proporcionar información e intercambiar mensajes electrónicos, también funciona como un gran almacén comercial en donde se pueden conseguir toda clase de artículos, el único requisito es tener una tarjeta de crédito de la cual se pide el número para poder adquirir por la red.

El departamento de Servicio Secreto de los E.U. cree que medio billón de dólares se pierden anualmente por consumidores que tienen números de tarjetas de crédito robados de bases de datos en línea. Las medidas de seguridad son cada vez mayores y los métodos tradicionales de la ley parecen ser suficientes para procesar a los delincuentes que hacen mal uso de dicha información.

b) DECODIFICADORES DE PASSWORDS

Los decodificadores de passwords o códigos de acceso son programas que monitorean y graban el nombre y password de usuarios de redes tan pronto como se conectan. Una vez que se tiene acceso a la cuenta de otra persona, también se tiene acceso a cualquier documento que tenga en su cuenta pudiendo obtener información confidencial y hacer mal uso de ella.

La persona que tiene el password de acceso a una cuenta en especial se hace pasar por el verdadero dueño de la cuenta y puede llevar a cabo sus objetivos cualesquiera que sean sin ser detectado. Aunque la ley no es muy clara en lo que a personas que se hacen pasar por otras en la red, la forma en que la ley previene esto es legislación el acceso no autorizado a otros sistemas computacionales.

c) FALSIFICACIONES INFORMÁTICAS:

Como objeto, cuando se alteran datos de los documentos almacenados en forma computarizada y como instrumentos, ya que las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

4.6.3.2 DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS:

En este concepto genérico tenemos el Sabotaje Informático que es el acto de borrar, suprimir o modificar sin autorización, funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son Virus o Gusanos, siendo los primeros una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos y los segundos aquellos programas que se fabrican en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferencia del virus porque no puede regenerarse. También dentro de esta categoría tenemos la Bomba lógica o cronológica, el acceso no autorizado a servicios y sistemas informáticos.

a) Plagio:

Es "la copia o imitación que no confiesa el modelo o el autor seguido" (Diccionario Jurídico, Cabanellas). En este ámbito encontramos las infracciones del copyrigth como base de datos, siendo

su sistema de protección más habitual el contractual entre los usuarios de una base de datos determinada.

b) Piratería :

"...se dice de la destrucción o apoderamiento sin escrúpulos de los bienes ajenos, como los de ciertos administradores con demasiado espíritu de propiedad.." (Diccionario Jurídico, Cabanellas). Dentro de este concepto tenemos las intercepciones de e-mails y el espionaje industrial que se realiza a través del acceso no autorizado a sistemas informáiticos de grandes compañías, la usurpación de diseños industriales, formulas, sistemas de fabricación y Know How estratégico.

4.6.3.3 INVASIÓN A LA PRIVACÍA:

La privacidad en su acepción mas amplia nos lleva a colegir que se trata del derecho de controlar el acceso a la información disponible sobre nuestra vida personal. Este derecho, dada las técnicas de tele marketing y cruce de información entre los distintos agentes comerciales se hace cada vez más efímero. De esta forma con bases de datos que se alimentan diariamente, es posible obtener información esencial de una persona, desde sus hábitos alimenticios hasta sus preferencias sexuales o religiosas. Toda esta información va siendo dejada como verdaderas huellas por el individuo al llenar solicitudes préstamos, tarjetas de crédito, efectuar llamadas telefónicas, registro en clínicas o centros hospitalarios, informaciones de compañías de seguros, etc. De esta forma las bases de datos se han convertido en bienes comerciales altamente cotizados. Toda la información que se

obtuvo para fines específicos se coloca a la venta para que sea adquirida por el mejor postor sin ni siquiera pensar en el consentimiento de los involucrados.

a) INTIMIDAD INFORMÁTICA

En el derecho a poseer y publicar la información a manifestarla o no. El derecho mexicano regula la materia de la intimidad informática, aunque se ha creado grandes lagunas en este renglón, provocadas por los avances tecnológicos.

b) INTIMIDAD INFORMÁTICA EN EL ÁREA ADMINISTRATIVA, ÁMBITO PERSONAL, ÁREA EMPRESARIAL

Se deben legislar los derechos y deberes de los individuos que conocen o tiene alguna información. Nadie puede destruir la intimidad de las personas, por eso hay que preservar la esfera de la intimidad del individuo, pues es un derecho humano, una garantía humana que se puede traducir en constitucional.

La fuerza tecnológica irrumpe en 3 áreas: Administrativa o pública, Negocios, Privada o íntima.

En los 3 hay un sujeto activo que recaba, almacena y usa la información y un sujeto pasivo, que es el que debe respetar esa intimidad informática. A esto se le conoce como el principio de *"ERGA OMNES"*.

Lo que se logra es optimizar la administración pública y los negocios, pues se tienen bases de datos e información para la toma de decisiones y además se va a tener una herramienta útil que ayudará a resolver los problemas de la vida privada.

Por tal motivo deben existir normas que regulen el acceso a las bases de datos y a la información, para el buen funcionamiento de la intimidad informática.

4.6.3.4 CYBERPUNK:

Constituye una verdadera subcultura que se define como el "Trato con gente marginada mediante sistemas altamente tecnológicos....sistemas que dominan las vidas de un gran número de personas." En esta subcultura surgen denominaciones deleznables tales como: Hackers (genios de la computación que sus conocimientos les permiten hacer cosas que parecen mágicas), Hacker es un término que describe a aquellas personas que sin permiso entran a los sistemas computacionales de empresas o individuos. El equipo que se necesita para llevar a cabo esta serie de delitos es muy poco, por lo que se facilita aún más la actividad de los hackers, de hecho sólo se requiere de una computadora, equipo de comunicaciones como modems y su software y una lista de números telefónicos.

La forma en la que opera un hacker es muy sencilla como se muestra a continuación:

- Encontrar un sistemas computacional al cual infiltrarse
- Obtener un nombre o número de identificación

- Obtener o deducir una contraseña
- Una vez dentro del sistema se puede copiar una gran cantidad de información en forma de archivos incluyendo información confidencial.

a) CRACKERS

(personas que irrumpen en los sistemas computacionales de otras personas, sin su permiso, ya sea para obtener ganancias ilícitas o por mera venganza personal.

b) PHREAKS

(son una especialidad de los Crackers que manejan específicamente el sistema telefónico, desviando cargos por llamadas y otros usos ilícitos) y finalmente los llamados:

c) RAVERS

(quienes usan sintetizadores musicales y drogas de diseñador para crear una fiesta toda la noche.). La aparición de Internet y del WWW facilitan la comunicación de estas subculturas y la unión de muchas personas con intereses comunes.

4.6.3.5 TERRORISMO INFORMÁTICO:

Se puede conceptualizar como el abuso intencional de cualquier sistema informático a los efectos de apoyar o facilitar una campaña terrorista en curso, es el nexo entre la entrada a sistemas con

información criminal y la violencia física de los terroristas. Esta clase de delito informático admite su clasificación en:

a) TERRORISMO DE ESTADO:

Es el caso de aquellos gobernantes de un Estado en que para poder seguir ejerciendo un control político sobre sus gobernados recurren al uso de la computadora como un factor de opresión.

b) TERRORISMO ENTRE ESTADOS:

En este caso tenemos el caso del llamado Flujo de Datos Transfontera (PDT) por medio del cual se atenta contra la soberanía de otros Estados.

c) TERRORISMO ENTRE PARTICULARES:

Más conocido como virus informático, Un virus es un código que se adhiere a los programas y archivos y se reproduce a si mismo dentro de ellos. Algunos virus se activan con alguna fecha específica, evento u operación de la computadora para llevar a cabo su tarea. la forma en que el virus trabaja es muy variable y puede desde solamente mandar mensajes molestos o gráficas o si se trata de un virus destructivo puede ocasionar la pérdida de información o serios daños a los sistemas de cómputo tanto físicos como lógicos. Otro tipo de virus afecta las computadoras dándole información falsa al usuario acerca de fallas en el hardware de la computadora.

Los virus computacionales son una amenaza seria para las computadoras, conforme se crean programas para vacunar las computadoras también se crean nuevos tipos de virus. La única forma de mantenerse a salvo de ellos es adquiriendo el software más reciente para tratar este problema, hacer respaldos de la información asegurándose que este libre de virus y tener mucho cuidado con los disquetes que se manejan así como la información que se maneja vía Correo Electrónico..

d) TERRORISMO DE PARTICULARES HACIA EL ESTADO:

Puede incluir virus o ataques físicos a centros informáticos.

4.6.3.6 NARCOTRÁFICO:

Se ha detectado el uso de la red para la transmisión de formulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas de mercancía ilícita y recogidas de las mismas.

4.6.37 BLANQUEO DE DINERO:

La legitimación de ganancias ilícitas tiene una gran herramienta en la informática, toda vez que los sistemas electrónicos de pago ocasionan: dificultad de control, rapidez de transacciones, posibilidades de anonimato y dificultad de conocer el verdadero origen y destino de la transacción,
entre las formas más comunes de comisión de este delito tenemos:

Ingresar grandes sumas en efectivo en una cuenta, con el fin de efectuar inmediatamente una transferencia electrónica a otra cuenta.

e) SMURFING:

Numerosos depósitos de pequeñas cantidades, situadas por debajo de la obligación de declarar en varias cuentas, desde las que se efectúan transferencias de cuenta, generalmente en el extranjero.

- Uso de identidades falsas, testaferros y sociedades de papel, constituidas en otra jurisdicción y utilizando cuentas puente para dificultar la identificación del verdadero origen de la transferencia.

- Uso de entidades offshore y abogados que protegen a su cliente mediante la figura del secreto profesional.

- Introducción de personas de confianza en pequeñas entidades financieras o en delegaciones.

- Cuentas de colecta o recaudación: Un número atomizado de inmigrantes hacen pequeños ingresos que se envían al exterior en forma agrupada.

4.6.4 OTROS "DELITOS INFORMÁTICOS"

En este punto vuelvo a hacer hincapié mi coincidencia con el elevado criterio expuesto por los Dres. Guillermo Beltramone, Rodolfo

Herrera Bravo y Ezequiel Zabale, [14] siguiendo al profesor ***Julio Téllez Valdés*** en el artículo citado en la nota al referirse a las conductas según utilicen el computador como medio o como fin, y al concepto que utilizan de delito computacional diferente al delito informático considerando a éstos cometidos *"a través de equipos computacionales pero donde el elemento central no es el medio de comisión, sino que es el hecho de atentar contra un bien informático"*...o sea los delitos computacionales utilizan como medio la computación (software o hardware) para realizar conductas que constituirían delitos convencionales como los nombrados en último término pero no delitos informáticos que atacarían elementos puramente informáticos y aún no se hallan encuadrados penalmente.

Lo expuesto, vale como aclaración sobre los recaudos que hay que tener al hablar de "delito informático", por eso en esta exposición, tomamos el tema de la "criminalidad" o los aspectos criminológicos que trae la aplicación de la moderna tecnología informática, incluyendo el campo propicio que ofrece la red de Internet sobre la materia, mencionando todo tipo de conductas, aún las convencionales, pero que encontraron este nuevo medio para desarrollarse y que agrega otras características a las tradicionales .

El abanico se expande, continuamente en la efectivización de dichas conductas que, como dijera, van o no contra el patrimonio, utilizando la computadora como medio de comisión,(estafa a través de ella), o atacando el bien informático en sí (la seguridad de un sistema) nutriéndose de la más sofisticada tecnología.

---

[14] Drs. BELTRAMONE, HERRERA BRAVO Y ZABALE: Guillermo, .Rodolfo y Ezequiel "Nociones básicas sobre delitos informáticos" ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología realizado en Santiago de Chile del 19 al 22.08.1998- Comisión I Variaciones de la criminalidad, panorama actual.

4.6.4.1 ESPIONAJE INFORMÁTICO

(Previsto en la Ley chilena 19.223), casos en que la información se encuentra archivada en un espacio mínimo y puede pasar sin dificultad a otro soporte. Estas conductas pueden concluir en el hurto del software puesto que quien lo practica puede apoderarse del programa de la empresa en la que efectúa el espionaje y utilizarlo luego en su beneficio. Puede llevarse a cabo para obtener información de carácter político y no sólo con objetivos de beneficio económico.

4.6.4.2 SABOTAJE INFORMÁTICO

(actualmente también previsto en la ley chilena mencionada), siendo este otro caso que se ve favorecido por la concentración de información en mínimos espacios. Y puede producirse destruyendo programas (introducción de virus), siendo ésta otra conducta que puede llevarse a cabo por diferentes mecanismos técnicos que con la sofisticación de la tecnología para comprenderlos hay que inevitablemente concurrir al auxilio de los conocimientos que proveen los especialistas en informática, por lo que se destaca el valor de la colaboración interdisciplinaria.

Las conductas de sabotaje por lo general se llevan a cabo contra centros de cómputos industriales, como las que puede realizar una célula revolucionaria como protesta contra la industria armamentista [15]

---

[15] TIEDEMANN, Klaus
ob.cit. pág 128.

4.6.4.3 USO INDEBIDO DE INSTALACIONES DE CÓMPUTOS

Como el caso de empleados desleales que utilizan dichas instalaciones para su propio beneficio, o para perpetrar alguna de las conductas descriptas anteriormente.

El autor citado en la nota precedente (Klaus Tiedemann) habla en su obra de "hurto de tiempo" como posible tipo penal situación que requiere el apropiamiento indebido de los bienes en juego para su punibilidad que constituiría la actividad reprochable más allá del gasto de energía eléctrica o el enriquecimiento del autor.

4.6.4.4 ABUSOS MEDIANTE TARJETAS DE CRÉDITO:

Elementos que agudizan el ingenio de los que operan a través de ellas . Vemos que el moderno sistema de comercio electrónico permite introducir su número para compras on-line (por Internet) lo que ha permitido un uso ilegal del sistema propiciando el fraude. Por ejemplo cuando se recibe un resúmen de cuenta de gastos de tarjeta y en él vienen incluidos compras "on-line" que no fueron efectuadas por el usuario ocasionando al banco emisor de la tarjeta pérdidas bastante importantes.

Todo lo hasta aquí expuesto, constituye un simple muestreo de aquellos casos que pueden conformar la moderna criminalidad informática agregando que este campo, -y en especial el que ofrece Internet y el desarrollo del uso de redes- abrió un camino apto y rápido a todo tipo de conductas.

Además, proporcionó por su forma de operatividad, la herramienta ideal para su consecución con fines ilícitos (que son los que nos interesan para el presente).

Obsérvese que hasta operaciones relativas a tráfico de mujeres(prostitución), de niños, pornografía, lavado de dinero, por ejemplificar nuevamente, pueden efectuarse ahorrando tiempo y garantizando rapidez e impunidad.

A este crecimiento vertiginoso debe seguirle el mismo en igual forma de los medios de combatir estos mecanismos que, no en todos los países se hallan igualmente adelantados.

Esta situación, crea un problema que abarca también aspectos de política y sociología criminal, vale decir compromete a otras ciencias penales además de la criminología.

4.6.4.5 LAS CONDUCTAS LESIVAS Y DELICTIVAS SON, SEGÚN EL CONSEJO DE EUROPA Y EL XV CONGRESO INTERNACIONAL DE DERECHO, ENTRE OTRAS[16]:

1. Fraude en el campo de la informática.
2. Falsificación en materia informática.
3. Sabotaje informático y daños a datos computarizados o programas informáticos.

16 Así la Recomendación nº 89 del Consejo Europeo del 13 de Setiembre de 1989, excepto 8, 9 y 10 que son adiciones del XV Congreso Internacional de Derecho Penal.

4. Acceso no autorizado.
5. Intercepción sin autorización.
6. Reproducción no autorizada de un programa informático protegido.
7. Espionaje informático.
8. Uso no autorizado de una computadora.
9. Tráfico de claves informáticas obtenidas por medio ilícito.
10. Distribución de virus o programas delictivos.

En primer, lugar debe dejarse en claro que de todas estas conductas, algunas de ellas pueden ser abordadas a través de los tipos penales tradicionales (fraude en el campo de la informática, falsificación en materia informática, sabotaje informático y daños a datos computarizados o programas informáticos, reproducción no autorizada de un programa informático protegido y distribución de virus o programas delictivos).

En base a lo expuesto y acogiéndonos a la clasificación hecha por Adamski es que vamos a abordar el análisis de las conductas lesivas al bien jurídico propuesto. Adamski, ha creído más conveniente analizar los atentados contra la "información" a partir de las propiedades que les son inmanentes: confidencialidad, integridad y disponibilidad[17].

17 Esta clasificación tiene cercanas semejanzas con los postulados por Platt y Morrison, quienes a través del acrónimo P.A.P.A. (Privacy, Accuracy, Property, Access), buscaban identificar y estructurar los problemás éticos derivados del manejo de la información; detalladamente: Platt, Richard G. & Morrison, Bruce. Ethical and Social Implications of the Internet, en: ETHICOMP 95. An International Conference on the Ethical Issues of Ussing Information Technology, vol. I, pág. 23, Venue de Montford University Leicester, 1995; Erikkson, Inger. Computers or Humans: Who are in control?, en: Kizza, Joseph Migga (ed.). Social and Ethical Effects of the Computer Revolution, pag. 87-88.

La confiabilidad y la integridad de la información son propiedades referidas, básicamente, a impedir la revelación, alteración o delación de la información contenida en ficheros de ordenador. La confiabilidad de la información cobra sus matices más importantes, por ejemplo, en el ámbito de la información médica, estrategias mercantiles, investigaciones científicas, entre otros. En cambio, la integridad resulta vital en el control de tráfico aereo, la transferencia electrónica de fondos, etc.

Por otra parte, la disponibilidad de la información resulta ser el atributo más importante de los servicios comerciales que dependen de la información, actividades como el "spamming" o el "electronic-mail bombing" pueden generar que el disco duro del sistema de información afectado se bloquee y deje de operar.

En éste orden de ideas, los ilícitos informáticos pueden ser clasificados en: a) conductas lesivas a la confidencialidad de la información, b) conductas lesivas a la integridad de la información, y, c) conductas lesivas a la disponibilidad de la información, así será llevado en adelante el análisis.

4.6.4.6 CONDUCTAS LESIVAS A LA CONFIDENCIALIDAD DE LA INFORMACIÓN.

Entre estas conductas tenemos:

a) ESPIONAJE INFORMÁTICO (INDUSTRIAL O COMERCIAL).

Siguiendo a Gutiérrez Francés agregamos las acepciones industrial o comercial pues entendemos como ella que hacerlo así limita convenientemente la esfera de análisis, caso contrario estaríamos afirmando la inclusión de afectaciones a bienes jurídicos de contenido distante al materia de análisis (delitos contra el Estado y la defensa nacional, delitos contra la Intimidad, por ejemplo).

El Espionaje Informático (industrial o comercial) debe entenderse como "la obtención, con ánimo de lucro y sin autorización además"[18] "de valor para el tráfico económico de la industria o comercio"[19], surge allí una seria dificultad para el legislador ante la variedad de comportamientos que encajan en él.

Entre las modalidades más conocidas tenemos:

b) LA FUGA DE DATOS (DATA LEAKAGE)

modalidad informática de los prácticas de "espionaje industrial", aparece en tanto todas las empresa y entidades custodian sus

---

[18] GUTIERREZ FRANCES, Mariluz.
art cit., pág. 388,

[19] ROMEO CASABONA, C.M.,
Delitos Patrimoniales en conexión con sistemas informáticos y de Telecomunicaciones, Texto de Ponencias y Comunicaciones, Congreso sobre Derecho Informático, Facultad de Derecho de Zaragoza, pág. 512, 1989.

informaciones más valiosas en los archivos informáticos, posibilitándose su sustracción[20].

c) LAS PUERTAS FALSAS (TRAP DOORS),

Conducta consistente en la introducción a los sistemas informáticos a través de accesos o "puertas" de entrada no previstas en las instrucciones de aplicación de los programas, aunque, como bien ha subrayado Pérez Luño, estas conductas puedan ser verificadas sólo por quienes tengan un conocimiento cualificado de los sistemas informáticos víctimas[21].

d) LAS "LLAVES MAESTRAS" (SUPERZAPPING),

Es el uso no autorizado de programas con la finalidad de modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en los sistemas de información, su denominación se debe a un programa denominado "superzap", que a modo de "llave maestra" permite ingresar a cualquier archivo, así se encuentre reservado.

e) EL PINCHADO DE LÍNEAS (WIRETAPPING).

---

[20] PÉREZ LUÑO, Antonio-Enrique. ob. cit., 73.

[21] Ibid., pág. 74.

modalidad que consiste en la interferencia en líneas telefónicas o telemáticas, mediante las cuales se transmiten las informaciones procesadas[22].

f) LA APROPIACIÓN DE INFORMACIONES RESIDUALES (SCAVENGING)

Que consiste en la obtención de información abandona por los usuarios legítimos del sistema informático[23].

Nos parece necesario precisar que aunque el espionaje informático sea, en algunos casos, subsumible en la descripción típica del delito de Hurto, en tanto la equiparación a bien mueble realizada en nuestro Código penal prevé como objeto del ilícito cualquier elemento que tenga valor económico[24], creemos necesaria su determinación punitiva independiente, puesto que prevé un catálogo mucho más amplio de comportamientos.

Es por ello que la legislación chilena, pionera en nuestra región en la regulación punitiva de los delitos informáticos, regula el espionaje informático de manera independiente sancionando con presidio menor en su grado mínimo a medio a quien "con el ánimo de apoderarse, usar

---

22 Ibid., pág. 74.

23 Ibid., pág. 73.

24 Bolivia, Código Penal.Cochabamba-Bolivia

Ed. Serrano, pag. 117

"Art. 326.- " El que, se apodere ilegitimamente de una cosa mueble, ajena, incurrirá en reclusión de un mes a tres años.

La pena será de reclusión de tres meses a cinco años, en caos especialmente graves. Por regla un caso se considera especialmente grave cuando el delito fuere cometido:....."

o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él" y con pena de presidio menor en su grado medio al quien "maliciosamente revele o difunda los datos contenidos en un sistema de información" aumentándose la pena en un grado si el autor es el responsable del sistema de información[25].

g) INTRUSISMO INFORMÁTICO.

Comportamiento consistente en la introducción a sistemas de información o computadoras infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ella. Vemos que, aunque en ocasiones se afecten los datos computarizados o programas informáticos, ello no es determinante para la configuración del injusto, basta tan sólo el ingreso subrepticio a la información (con valor económico de empresa) para la concreción del comportamiento.

Aquí es necesario precisar que aunque en un inicio pareciera que el Sabotaje Informático y el Intrusismo fueran comportamientos idénticos, ello no resulta cierto, pues es el elemento subjetivo el que delimita la frontera de cada comportamiento; mientras en el primer supuesto, la intencionalidad del agente es obstaculizar el funcionamiento de un sistema informático, en el segundo caso la acción realizada busca únicamente el ingreso a tales sistemas sin dirigir sus actos a la producción de perjuicio, que ello se produzca es ajeno al comportamiento aunque es evidente que lo agrava.

[25] Arts. 2 y 4 de la Ley nº 19223, Ley relativa a delitos informáticos de Chile.

El discurso criminológico ha creído necesario también analizar el problema desde su óptica, pues el Hacking tiende a generar comportamientos de mayor dañosidad, el Hacker (intruso) no se complace con la conducta delictiva inicial, intenta analizar su capacidad técnica personal agotando las posibilidades de obtención de información, así el Hacker modificará progresivamente su accionar hasta concluir realizando actos de Sabotaje o Espionaje Informático.

4.6.4.7 CONDUCTAS LESIVAS A LA INTEGRIDAD DE LA INFORMACIÓN.

La integridad de la información puede resulta afectada, básicamente, a través del conocido como "sabotaje informático", cuyas modalidades más conocidas son las siguientes:

a) LAS BOMBAS LÓGICAS (LOGIC BOMBS).

introducciones lógicas Implantadas en un programa informático que se activará ante determinada circunstancia (fecha, orden, etc.), dañando o destruyendo los datos informáticos contenidos en el ordenador[26].

Las bombas por correo electrónico es la forma en que los terroristas han ingresado al ciber-espacio. La forma en que trabajan

---

[26] PÉREZ LUÑO, Antonio- Enrique.
ob. cit., pág. 73
GUIBOURG, Ricardo A. y otros.
ob. cit., pág. 278.

estas bombas es dándole a la computadora instrucciones para mandar mensajes por correo electrónico en forma repetitiva a una dirección de correo electrónico específica, el ciber-criminal puede saturar la cuenta de una persona y hasta llegar a apagar sistemas completos ya saturados de mensajes. Aunque no hay leyes específicas para este tipo de delitos, ciertamente es una actividad muy destructiva.

Por ejemplo, en otoño de 1994, dos escritores de columnas de computación fueron objeto de un ataque vía "bomba electrónica" (reportado por la revista Time, Diciembre 12, 1994). Aparentemente por venganza en contra de algunos artículos que las víctimas escribieron acerca de los crackers, alguien logró accesar las computadoras de los proveedores de servicio de Internet de los escritores, IBM y Sprint. su correo electrónico fue sobresaturado por miles de mensajes. Su conexión fue dada de baja y su teléfonos fueron reprogramados para que sus llamadas fueran enrutadas hacia otro número para que cuando les llamaran por teléfono se escucharan mensajes obscenos.[27]

b) LOS VIRUS INFORMÁTICOS

Es otra de las modalidades conocidas de sabotaje informático, los virus informáticos resultan ser programas secuenciales de efectos previsibles, con capacidad de reproducción en el ordenador y su expansión y contagio a otros sistemas informáticos[28]. Su incidencia es similar a la que ejercen los virus propiamente dichos en el organismo humano (de allí su denominación), por ello es que existen programas

[27] Dirección de Internet, http://199.111.112.137/others/seminar/notes/crime1.html

[28] PÉREZ LUÑO, Antonio- Enrique.
ob. cit., pág. 73.

"antivirus" que previenen y contrarestan sus efectos nocivos. Dentro de ésta catergoría es posible ubicar a las rutinas- cáncer.

El origen de los virus informáticos es desconocido, sin embargo, se sabe que es Bulgaria el país productor de la mayoría de ellos, seguido por Rusia y los Estados Unidos. Entre los virus informáticos más conocidos tenemos: Data Crime, Alabama, Disk Killer y, más recientemente, "I Love You" y Melissa.

4.6.4.8 CONDUCTAS LESIVAS A LA DISPONIBILIDAD DE LA INFORMACIÓN.

En éste punto, surgen serias dificultades, en tanto las citadas modalidades de sabotaje informático (bombas lógicas y virus informáticos) afectan también la disponibilidad de la información, pues, como es lógico, un sistema de información dañado a través de las referidas técnicas queda también fuera de la disponibilidad de su poseedor, sin embargo, la diferencia principal parece estar en los resultados obtenidos. Cuando las fórmulas de sabotaje informático sólo afectan momentáneamente al sistema informático, estamos ante conductas que afectan la disponibilidad de la información, si en cambio, el daño al sistema informático afecta la información contenida en ella, total o parcialmente, de forma permanente, estaremos ante conductas lesivas a la integridad de la información.

Además de las bombas lógicas y los virus informáticos, existen conductas que afectan también la disponibilidad de la información,

como las técnicas de "spamm" o el "electronic-mail bombing", los cuales no son sino mensajes de correo electrónico no solicitados o autorizados y que afectan el respectivo sistema informático al llenar el buzón de cientos e incluso miles de mensajes electrónicos[29].

Esa fue la técnica empleada en los ataques efectuados contra los sitios web de Buy.com, eBay.com, CNN, Amazón y ZDNet, principalmente, el ocho de Febrero de 2000. Estas páginas fueron bloqueadas a través del bombardeo de e-mails, esto es, alguna o algunas personas programaron sus ordenadores con el fin que enviaran millares de mensajes de correo electrónicos, ante la avalancha de información recibida, las computadoras que mantienen operativas éstas páginas web se paralizaron. Aunque no se verificaron daños sobre la información o los elementos informáticos relacionados con los web sites atacados, el perjuicio causado debe estimarse a partir del lucro cesante, sólo por citar el caso de Amazon.com, se calcula que durante las tres horas que se encontró inoperativa dejó de vender 560,000 dólares en libros y otros artículos que comercia[30].

---

[29] ENOS, Lori

De allí que en los Estados Unidos existan incluso leyes anti-spam; al respecto:. "Spam Strikes Again", en: E-Commerce Times, 17 de Marzo de 2000,

http://www.ecommercetimes.com/printer/.

[30] TREJO DELARBE, Raúl.

Estaf@s.com. Ataques que entorpecieron los servicios en la Red, en: Bitniks Magazine, 15-03-00: http://www.bitniks,es;

ROZENBERG, Dino.

Los Sitios Web bajo Ataque, en: Information Week México,

: http://www.infoweek.com.mx.

a) PORNOGRAFÍA INFANTIL

Este es uno de los crímenes que es seriamente castigado tanto dentro como fuera de Internet. Aunque se han rastreado a diversos criminales que llevan a cabo esta actividad, este como tanto otros delitos computacionales pueden ser bien disfrazados y existen maneras de adquirir imágenes de niños con diferentes tipos de ropa y llevando a cabo una gran variedad de actos sexuales. Legalmente hablando, las personas que proveen acceso a sitios donde se puedan encontrar este tipo de imágenes enfrenten el mismo tipo de cargos que aquéllas que manejan imágenes fotográficas o de video.

b) DELITOS CONTRA EL HONOR

Son aquellas perpetradas a través del Internet, generalmente dirigidas contra personas del ámbito publico, farándula o gobierno, son materializadas a fin de dañar su popularidad, estima y hasta veces la credibilidad, dañando su honra y honorabilidad mucho mas aun si esta información es difundida en la red llegando a millones de usuarios dando la vuelta al mundo.

CAPITULO V

DELITOS CONTRA EL HONOR DE LAS PERSONAS A TRAVÉS DEL INTERNET

CAPITULO V

DELITOS CONTRA EL HONOR DE LAS PERSONAS A TRAVÉS DEL INTERNET

5.1 EL HONOR

El Honor como bien jurídicamente protegido constituye el derecho que cada ser humano tiene al reconocimiento y al respeto ante el mismo y ante las demás personas. En nuestra sociedad, de acuerdo al grado de cultura de cada persona, en mayor o menor intensidad tomando en cuenta las diferentes clases sociales que existen, el honor como objeto de protección penal ha sido concebido desde diferentes perspectivas, sin embargo para tener una concepción estrictamente jurídica la dignidad de la persona, como sujeto de derecho constituye la esencia misma del honor, el cual es y se considera un derecho natural, pues este tiene su origen en el ser humano y en su propia naturaleza y no como algo otorgado por la sociedad o por consecuencia de su Inter-relación con otras personas, sin ser excluyente del carácter social, así podemos observar que el honor esta en la conciencia de todo ser humano tenga este mayor o menor cultura, pues independientemente de esto una persona reaccionara cuando su honor es ultrajado con ofensas, pues es parte de su patrimonio natural y tiene un Derecho subjetivo a que se respete su propia dignidad.

Existen tres concepciones diferentes a decir :

- El sentimiento de la propia dignidad
- La buena opinión o estima que otros tienen de nosotros
- La capacidad o potencia que tiene una buena reputación de lograr ciertas ventajas materiales.

Toda legislación desde las mas antiguas hasta las mas modernas han protegido los Delitos contra el honor de las personas, pues si muy bien no tiene una existencia material o física no deja de tener importancia en el acervo moral de una persona.

" Es un sentimiento que solo tienen una parte de los seres humanos " y que *" es un concepto muy difícil de precisar en cuanto a los elementos que lo constituyen"*[1] del anterior concepto se desprende que los delitos contra el honor atacan a un ámbito espiritual y moral de la persona.

La honra de una persona es esencial en su vida social y es parte indisoluble de su relación como ser humano empero de manera general *" El honor es el concepto que una persona tiene de si misma y aquel que los terceros se han formado acerca de ella, en lo relativo a su conducta y sus relaciones éticas y sociales"*[2].

Francisco Carrara, distingue entre : a) El honor propiamente dicho ,formado por el concepto por la valoración que tiene cada persona de si mismo, por tanto es propio, subjetivo y de elaboración intima, en conciencia de los meritos que uno cree poseer, denominado por otros autores dignidad, honor subjetivo, honor interno, etc. Por tanto

---

1 Ramos Juan P. "Delitos Contra el Honor". Buenos Aires, Argentina. Abeledo Perrot. 1958

2 Garrido Montt, Mario. Los Delitos Contra el Honor Santiago de Chile. Carlos E. Gibbs A. Editor. Pag. 11

inherente a la personalidad; b) La Reputación que es ya algo mas objetivo y va mas allá del individuo emanando de la personalidad por tanto son las opiniones de la sociedad de los valores morales, sociales e intelectuales atribuidas a un individuo por la colectividad. Y c) Existen ventajas materiales que tienen su origen en una buena reputación, por tanto al mellar el honor de una persona no solo se lesiona su honra y dignidad, sino que también se dañan derechos y ventajas obtenidos por la buena reputación de una persona, siendo algunas veces irreparable se afirma también que *" El honor puede ser herido, pero no arrebatado"* por tanto el prestigio y la fama son elementos de valor indiscutible.

5.2 DERECHO AL HONOR

Como podrá observarse los ataques y lesiones inferidos al honor de una persona merecen y son dignos de tutela jurídica pues son considerados de alto valor social y estima personal. Si bien el honor tiene naturaleza especial es decir que un enajenado mental no tiene honor subjetivo, conciente pues el honor como elaboración psíquica, tiene como requisito indispensable en el sujeto, la conciencia de si mismo.

Podemos concluir entonces que existe una clara diferencia entre *"Honor" y "Derecho al Honor"*, pues esta ultima es una institución jurídica que nos otorga la facultad de reclamar un trato digno y racional en cuanto una persona tiene la facultad de exigir y también la obligación de guardar consideración, respeto y decoro para con sus congéneres y estos hacia el, acorde con las exigencias de una convivencia en sociedad.

El honor y la intimidad de la persona pueden ser lesionados con una acción conjuntamente o por separado, no obstante son distintos bienes de la persona, pues el derecho a la intimidad se caracteriza por el derecho del individuo a preservar su vida privada de cualquier injerencia ajena; mientras que el derecho al honor se entiende por el derecho al respeto que merece toda persona en su dignidad humana.

5.3 DERECHO AL HONOR EN INTERNET

Desde este orden de ideas, partimos por reconocer que ambos pueden verse afectados a través del empleo de *"medios Informáticos"* en concreto el Internet, sin duda el debate se ha desarrollado debido a numerosos reclamos interpuestos por usuarios contra proveedores de servicios de Internet, típicamente operadores de foros de discusión, por mensajes Contra el honor de las personas, publicados en esos foros.

Ahora bien el alcance del control que se ejerce varia significativamente según los medios tecnológicos utilizados, en concreto la simple aplicación de programas de filtro que detectan el empleo de expresiones que pueden ser indicio de la existencia de contenidos ilícitos, no es un medio determinante del efectivo control de la presencia de contenidos contra el honor de las personas. Por lo tanto , la mera contraposición entre la ausencia de todo control de una parte , y el efectivo control de los contenidos en los términos tradicionales de la supervisión editorial de los medios de información tradicionales , de otra , es una simplificación que margina la realidad del alcance de las tecnologías de filtrado mas difundidas .

En esta línea, la tradicional distinción entre los grupos de noticias moderados u aquellos en los que no esta presente un moderador, a los efectos de atribuir responsabilidad al proveedor en la medida, en que un foro moderado, no impide apreciar que la función del moderador es controlar mensajes que son difundidos, su selección en un contexto caracterizado por la multiplicidad de mensajes, la participación de diversos servidores en la difusión de los foros la heterogeneidad de los participantes en la red y la velocidad al que se sucede la publicación de mensajes se ciñe en muchas ocasiones a comprobar que el mensaje corresponde con la materia a la que se refiere ese foro , sin analizar su contenido y en particular esta puede generar responsabilidad.

Ante la incertidumbre generada, diversos ordenamientos jurídicos han reaccionado fijando legislativamente el alcance de la responsabilidad de los provcedores de servicios de Internet en supuestos de intromisión en el derecho al honor o a la propia imagen.

5.4 DELITOS CONTRA EL HONOR DE LAS PERSONAS A TRAVÉS DEL INTERNET

Ahora bien, la posible afectación del honor mediante el empleo de sistemas Informáticos configura un delito Informático, en la medida en que el medio Informático representa una mas de las características de la conducta llevada a cabo, que por si misma no varia en su naturaleza de actividad en contra del honor. En efecto conductas que afectan el honor mediante publicaciones en paginas WEB, el envió de correo masivo, envió de telememos, y otros medios se constituyen en delito Informático, contra el honor de las personas vía Internet.

El envió de un correo electrónico o E-mail, cuyo contenido es difamatorio constituye un medio idónco para la realización de un delito contra el honor, la excepción en juicio, promovida en virtud a establecerse si como consecuencia de utilizar un correo electrónico cuando se dirige a numerosas empresas corporativas con acceso al personal de cada una de ellas, constituye el medio de comunicación masiva.

La discrepancia suscitaría al interior de un juzgado penal oscilando entre la consideración del envió de un correo electrónico a varias personas como la realización de la conducta típica de revelar o divulgar de una persona un hecho, una calidad o una conducta que pueda perjudicar su honor o reputación de manera que pueda difundirse la noticia.

Esto es si el uso de Internet constituye un medio de difusión idóneo para la comisión de delitos contra el honor vía Internet, ante varias personas reunidas o separadas y por otro lado, de considerarse un medio idóneo para la realización del tipo penal, es posible su comprensión dentro de los alcances de la formula *" otro medio análogo de publicidad"* entonces se podrá considerar el Internet como medio idóneo para la realización y comisión de delitos contra el honor, en virtud de que es asimilable al delito cometido por Internet cuando el correo electrónico, telememo, publicación, periódico en Internet, publicación en pagina WEB, es dirigido a varias personas, estas a su vez pueden comentar con otras personas, por lo que constituye un medio de comunicación masiva. Existe, no obstante, el voto singular considerando el envió de un correo electrónico como idóneo para la realización del delito de difamación a través de un medio de

comunicación social, en atención a que viene a ser un medio de intercomunicación personal a través de un sistema Informático o Red de comunicación electrónica de datos.

Sobre esta polémica debemos efectuar algunas notas que sirvan a la aclaración de lo discutido. En cuanto a determinar si el envió de un correo electrónico con información a diversas personas configura el tipo básico de delitos contra el honor en términos tipicidad, el delito de difamación se caracteriza por la atribución a una persona de un hecho, calidad o conducta que pueda perjudicar su honor o reputación, ante varias personas reunidas o separadas, de manera que pueda difundirse la noticia ; para ello el envió de un correo electrónico se muestra como un medio idónco para su realización, no siendo necesario que se lleve a cabo mediante el envió de un correo masivo, sino, un solo e-mail a distintas personas ya que la propia experiencia puede darse este delito respecto de personas que se encuentran separadas a través del envió de varios e-mails. A ello se ha de agregar que concurrirán todos los elementos necesarios para que pueda difundirse la noticia ya que el envió de un correo puede generar, a su vez, su reenvió a una infinidad de usuarios de la red. Entendemos por otra parte , que si bien el envió de varios correos electrónicos a distintas personas puede considerarse como medio idóneo para la realización de la conducta típica de delitos contra el honor, en función de una exposición al publico y del uso de medios de difusión masiva, como sucede a través de la radio o la televisión de ahí que coincidimos en el análisis en el sentido de que el Internet resulta un medio de intercomunicación personal a través de la red, sin que represente un medio de comunicación social.

Nace ahora una nueva problemática cuando el delito se comete " mediante medios de comunicación divulgados o expuestos al publico". La razón de esta mayor gravedad nace, como decía CARRARA de *"la permanencia"* ; nace de la misma impersonalidad del ataque. Es curioso que un determinado sujeto nos ataque, si lo hace decimos que el lo hizo pero si fue a través de un medio de comunicación decimos que fue el medio olvidándonos de la persona.

Acerca de la exposición al publico, digamos solamente que se verifica o se realiza la comisión del delito en el momento que esta a disposición de quien lo quiera ver. No es necesario que se ponga en venta; ni basta el dejarlo en la red de Internet para que haya divulgación sino que debe estar a disposición del público pues si el anuncio divulgación u otro contra el honor no a llegado a cocimiento popular o público el delito no se habrá consumado ya que ni el ISP, tiene conocimiento del contenido.

Por ultimo es necesario advertir como ha sido explicado líneas arriba que si debería ser considerado como medio de publicidad la edición y publicación de una pagina web vía Internet, con información contra el honor, ya que no solo resulta un medio idóneo para la realización de la conducta típica del delito, sino que además no se trata de una comunicación interpersonal sino que esta dirigida a la comunidad de la red y pueden acceder a ella todos los usuarios del sistema sin limitación alguna, resultando un medio de comunicación masivo. En definitiva, observamos que la jurisprudencia nacional todavía no ha recogido la verdadera dimensión del uso de los sistemas Informáticos ni su operatividad en la realización de determinadas conductas típicas, ello ha de responder a un progresivo desarrollo de los

conocimientos Informáticos dentro de los magistrados y a la elaboración de una casuística que permita una jurisprudencia circulante.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines delictivos.

No son los grandes sistemas de información los que afectan la vida privada y el honor sino la manipulación por parte de individuos poco conscientes e irresponsables.

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento del honor de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

CONCLUSIONES.

A través del desarrollo de la presente Tesis, sobre los delitos Contra el Honor de la Personas a Través del Internet, emergentes, este nuevo milenio que comienza y por ser de carácter exploratorio y en base a todos los antecedentes y bibliografía recopilada, el alumno tesista logra llegar a las siguientes conclusiones sobre el tema tratado:

- Que si bien existe una nueva forma de comunicación social y humana, esto ha dado lugar al surgimiento de nuevos hechos o delitos, que valiéndose de la red, de sus computadores como medio o como fin, logran transgredir y superar ampliamente las distintas figuras típicas penales. generalizando el entendimiento de que "Delitos Informáticos", son todas aquellas conductas ilícitas susceptibles de ser sancionados por el derecho penal, que hacen uso indebido de cualquier medio informático.

- La legislación penal comparada, ha demostrado la importancia estos últimos años en la aplicación e incorporación en sus legislaciones penales, los delitos informáticos, como necesidad en especifico Alemania, Austria, Francia, Estados Unidos de Norteamérica, España, Argentina, Francia y Perú, por la creciente ola de delitos informáticos así mismo la comunidad internacional, se ha abocado al control, destacándose la labor desarrollada por la Organización de las Naciones Unidas.

- Se concluye además de que en Bolivia existe un vació jurídico en cuanto se trata de los delitos Contra el Honor cometidos o ejecutados a través del Internet, pues no existe una norma que adecue la conducta del sujeto activo, quien utiliza la computadora como medio o fin a decir de Téllez Valdes y la ONU, y mucho menos a través del Internet tipificando este hecho como delito y materializando la hipótesis de la norma.

- Se ha demostrado que el acervo moral de la persona es dañado por mensajes emitidos en forma masiva, mellando el honor de la persona máxime si se trata de un profesional o una persona de reconocido prestigio pues en este caso no únicamente se daña su honor, dignidad y decoro, sino también sufre un daño patrimonial por cuanto sus valores morales entran en duda y esto trae consigo el desprecio y desconfianza de pacientes, clientes e incluso amigos.

Se ha demostrado en base la recopilación de información y bibliografía, legislación comparada, y encuestas que:

"El avance tecnológico informático a nivel mundial a generado la probabilidad de que los delitos contra el honor de las personas realizadas a través del Internet quedan impunes situación que repercute con mayor intensidad en Bolivia por su atraso técnico jurídico".

RECOMENDACIONES

Siendo un tema de gran interés y de preocupación, y el carácter transnacional de los delitos cometidos contra el honor de las personas a través del Internet, recomendamos que:

Es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología informática, en su conjunto (chips, inteligencia artificial, nanotecnología, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

Dado que la calidad de vida y el desarrollo humano dependen en gran medida de las nuevas tecnologías, especialmente de la información y las telecomunicaciones, como ha afirmado la ONU, es necesario brindar las seguridades que garanticen su uso por parte de los Bolivianos, sin riesgo de ser víctimas de delitos.

· SEGURIDAD JURÍDICA

La legislación penal Boliviana no puede seguir siendo la principal fuente de inseguridad jurídica mucho menos en legislación informática. ello afecta la existencia misma del Estado de Derecho.

La descodificación penal debe cesar. Se impone una necesidad urgente que es la reforma del Código Penal para modificar el capitulo de los delitos contra el honor de las personas cuyo medio o fin ejecutivo sea la computadora y a través del Internet, dentro de una concepción sistemática e integradora, conjuntamente con los nuevos delitos de naturaleza informática, que también deben ser incluidos.

· POLÍTICA CRIMINAL:

Como quiera que Bolivia posee un sistema de legislación penal, caracterizados por su expresión en un Código Penal clásico, por tanto se hace prioritario optar por la reforma del Código Penal, sin más.

Solo allí estará expresada la política criminal del Estado boliviano en materia penal-informática, en el marco del Estado de Derecho. delegando al Ministerio de Justicia, la creación de una comisión codificadora, para el estudio y actualización del Código Penal adelantando tareas que sean necesarias, como ser:

a) Procederse de inmediato a elaborar el proyecto de reforma parcial del Código penal en los artículos que sean procedentes para incorporar las variantes informáticas de los delitos vigentes, mediante la técnica legislativa de reforma.

b) Se debería emprender el estudio de la reforma integral del Código Penal a los fines de incluir los nuevos delitos de reciente data y contar con un proyecto de reforma total en unos dos años.

c) Primero como reforma parcial y luego en la total del Código Penal salvaguardando, al menos, los siguientes bienes jurídicos:

I) Los derechos humanos tales como la libertad, seguridad jurídica, confidencialidad, secreto, honor, intimidad e inviolabilidad de todas las comunicaciones y de las telecomunicaciones, información, y datos que se intercambian en la red;

II) La información y datos personales como bienes jurídicos intangibles e inviolables;

III) La publicidad de la información y datos que sean de interés para la sociedad y que no vulneren derechos subjetivos;

Debe existir así mismo el libre acceso y uso de la Internet, como parte de la política prioritaria del Estado boliviano para el desarrollo cultural, social y político de la sociedad en su conjunto precautelando derechos inherentes a la persona y su personalidad.

BIBLIOGRAFÍA

DE RIVACOBA Y RIVACOBA, Manuel
"Elementos de Criminología"
Edeval 1982

ZAFFARONI, Raul Eugenio ob.cit.:
"Manual de derecho Penal" Parte General
p.118-Edigraf 1987 y ver también "Derecho Penal" P. General
Ed. –2000.

P.WALTON - YOUNG , I. TAYLOR - J,
"La nueva criminología" (Contribución a una teoría social de la conducta desviada)
p. 12 –Amorrortu 1990.

TIEDEMANN, Klaus,
"Poder Económico y Delito"
Ed. Ariel, Barcelona, 1985, pág. 122.

ALCONADA ARAMBURU, Carlos R. S.
"El caso Swift Deltec –La reparación judicial de una agresión económica foránea" .
La Ley-1973.

DURKEHIM, Emile
"La Nueva Criminología"
. pág. 104.

BARATTA, Alessandro,
"Criminología Crítica y Crítica del Derecho Penal",
Siglo XXI , Editores, pp. 83 y ss

SIEBER, Ulrich,
"The International Handbook on Computer Crime"°,
Ed. John Wiley & sons Ltd., 1986, Great Britain, 1986.

TELLEZ VALDEZ, Julio.
"Derecho Informático"
Ed. Mac Graw Hill. 1996 - Mexico D.F..

BELTRAMONE, HERRERA BRAVO Y ZABALE: Guillermo, .Rodolfo y Ezequiel
"Nociones básicas sobre delitos informáticos"
ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología realizado en Santiago de Chile del 19 al 22.08.1998-Comisión I Variaciones de la criminalidad, panorama actual.

GUTÍERREZ FRANCES, Mariluz.
art cit., pág. 388,

ROMEO CASABONA, C.M.;
Delitos Patrimoniales en conexión con sistemas informáticos y de Telecomunicaciones, Texto de Ponencias y Comunicaciones, Congreso sobre Derecho Informático, Facultad de Derecho de Zaragoza, pág. 512, 1989.

FALCON Enrique M.
" Que Es La Informática Jurídica "
1ra. Edición, Ed. Abeledo Perrot, Buenos Aires, Argentina, 1992.

ALTMARK, Daniel R. y BIELSA, Rafael A.
" Informática y Derecho" volúmenes I, II, III, IV y V
Ed. La Roca, Buenos Aires, Argentina, 1987

GATES, Bill
" Camino al Futuro "

GUSTAVINO, Elias P.
"Responsabilidad Civil Y Otros Problemas Jurídicos En Computación"
Ed. De Palma, Buenos Aires, Argentina, 1998.

UWE KALBHEN, Fritz Kiuckeberg y REESE, Jurgen
" Repercusiones Sociales De La Tecnología Informática "
Ed. Fundesco/Tecnos, Madrid, España, 1983

GARCIA MOLINA, Pablo
"Informática y Derecho Penal",

FALCONI, Perez Miguel
" Protección Jurídica "
Guayaquil, Ecuador, 1991

HERRERA FIGUEROA, Miguel
" Psicología y Criminología"

HANCE, Oliver
" Leyes y Negocios en Internet"
Ed. Mc Graw Hill, The Best of Programas Educativos S.A. Mexico D.F.1996

VERA, Bacarreza Veronica
" Legislación y Fundamentos Básicos Del Derecho Aplicables a La Informática " .

PAGINAS WEB

JIJENA Leiva Renato "Informe legal: sobre la improcedencia de censurar legalmente los contenidos de Internet. Análisis del Boletín N°. 2395-19 en *http://publicaciones.derecho.org/redi* (Redi Octubre de 1999).

Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones. Bruselas 16/10/96 – "Contenidos ilícitos y nocivos en Internet" en <*http://www.aui.es/biblio/documentos/eu_contenidos.htm*>

LYNCH Horacio M. "La incierta naturaleza de internet" en Ecomder 2000-Primer Congreso Internacional por Internet sobre Aspectos Jurídicos del Comercio Electrónico-Facultad de Derecho-UBA. Bs. As. Argentina", *http<://ecomder.com.ar*>

VILLATE Javier "Un ciberespacio público" en Cuadernos Ciberespacio y sociedad N°0 en *www.cys.derecho.org*

"Cibernautas por la Tolerancia" "Declaraciones de Independencia del Ciberespacio" John Perry Barlow. Davos, Suiza, 8/2/1996, <www.ctv.es/users/mrb/tolerancia>.

SANCHEZ Almeida Carlos "Libertad para todo" <http://www.bufetalmeida.com/robot.htm>;

SANCHEZ Almeida Carlos "Caso archivado" <http://www.bufetalmeida.com/archivo.htm>.

BRENNA Ramón Gerónimo "Internet: Espacio Virtual sin Ubicación ni Ley" en http://.ecomder.com.ar conferencia proclamada en el "Primer Congreso Internacional por Internet sobre Aspectos jurídicos del Comercio Electrónico. Facultad de Derecho. Uba Bs. As. Argentina"

JOHNSON David R. "Garantías individuales y liberjurisdicción" en "Cuadernos Ciberespacio y sociedad N°. 3-Marzo de 1999" en www.cys.derecho.org;

VILLATE Javier "Un ciberespacio público" en Ciberespacio y Sociedad N°0 en www.cuys.derecho.org

RODRIGUEZ Felipe "Sobre los sistemas de clasificación y etiqueta de contenidos" en Cuadernos Ciberespacio y Sociedad N° 0, en <www.cys.derecho.org>

LESSIG Lawrence "Las leyes del ciberespacio" en Cuadernos Ciberespacio y sociedad Nº. 3, mayo 1999 <*cys.derecho.org/03/leyes.html*>.

JIMÉNEZ Villada Tomás, "¿Están seguros los derechos?" <*http://www.buenafuente.com/20000811/leeditorial.html*>

Diario del Navegante del 6/8/99 "En Internet se ha acabado con la impunidad" <*http://www.elmundo.es/navegante/diario/99/agosto/06/impunidad.html*>

GALÍNDEZ Maricel "Acceso ilegítimo a sistemas informáticos. La informática y el derecho a la intimidad. Necesidad de una reforma" <*http://www.ulpiano.com/bo18_delito_maricel.htm*>;

SOBRINO Waldo Augusto Roberto "La necesidad de un 'Orden Público Tecnológico con especial referencia a Internet; E-Commerce y el Proyecto Genoma Humano" *www.eldial:com.ar*; 18/8/2000.

"Contenidos ilícitos y contenidos nocivos" en <*WWW.onnet.es/c09.htm*>

MARTINO Antonio Anselmo, "E-Comerce y Derecho hoy. La experiencia de la Comunidad europea" Ecomder 2000-Primer Congreso Internacional por Internet sobre Aspectos jurídicos del Comercio electrónico-Facultad de Derecho-UBA, en *http://ecomder.com.ar*

"Censura en Internet" <*http://cnn.com*> en <*www.onnet.es/c0_9.htm*> actualizada a junio de 1996.

Informe profesional sobre las iniciativas emprendidas en los Estados miembros de la UE contra los contenidos ilícitos y nocivos en Internet Versión 7 (4 de junio de 1997) *http://www.ipso.cec.be/legal/en/internet/wp2es-chap.html;*

OLIVIER Hance "Leyes y negocios en Internet" McGrw Hill, 1996; Laneza Gonzalez, Paloma "Internet y Comunicaciones digitales" [1] "Contenidos ilícitos y contenidos nocivos" *www.onnet.es/C09.htm*

COLAUTTI Carlos E. "La libertad de expresión y el espacio cibernético" La Ley 1999-E-1329. Ver Llaneza Gonzalez, Paloma "Internet y Comunicaiones digitales", p. 203; el fallo en <*http://www.freexpression.org/*>; <*comunidad.derecho.org/carlospal*>.