4.2.1. Estructura de la norma jurídica.

En el siguiente gráfico se muestran los "tres elementos principales de la norma jurídica que deben existir para que una ley no sea incompleta, defectuosa e ineficaz" [1].

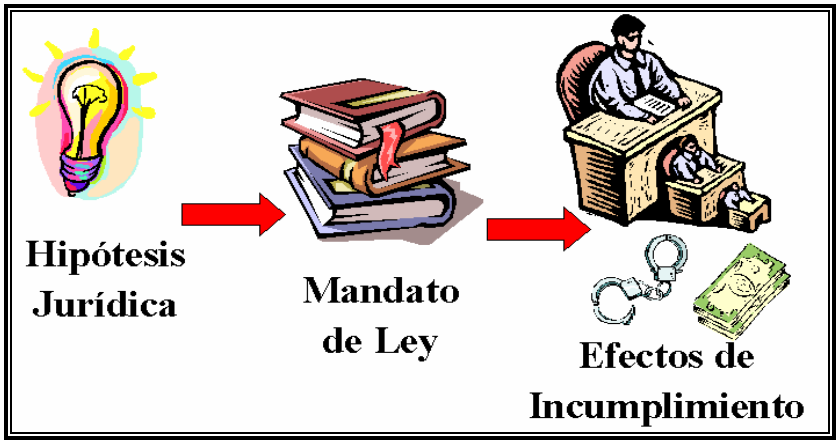

Figura 3. Estructura de la norma jurídica.

1. Hipótesis Jurídica.- Corresponde a la descripción de las diferentes conductas delictivas, es decir, un hecho que puede ocurrir en la sociedad.
2. Mandato de Ley.- Es lo que la ley dispone, pertenece al conjunto de artículos escritos por especialistas y que forman parte de la ley.
3. Efectos de Incumplimiento.- Es la sanción que se establece por el incumplimiento del mandato de ley. Puede ser prisión o multa o pérdida de derechos constitucionales.

4.2.2. Análisis de la Legislación Ecuatoriana.

Una vez revisada la "Legislación Ecuatoriana" en el capítulo 2 - sección 9, a continuación se expone un análisis de la situación actual respecto a la problemática que ocurre en Internet.

Por lo general las leyes o normas ecuatorianas definen algunas de las palabras que se expresan en los artículos de sus textos, sin embargo en el análisis realizado no se ha encontrado definiciones de carácter importante que ayudan a regular el uso de Internet, entre las cuales se puede mencionar: Internet, Hacker, Cracker, delito informático, falsificación informática, fraude informático, sabotaje informático, virus informático, gusano informático, bomba lógica y caballos de Troya.

Cuando se refiere al medio usado para la comisión de los delitos tradicionales como: sabotaje, fraude, estafa, falsificación, injuria, entre otros, se originaría "el Dilema de si Internet es o no un medio" en el momento que el delito se hace a través de Internet y más aún si no ha sido tipificado.

Por la falta de definición del término "Internet", la ley se aplicaría por analogía lo cual no está permitido en virtud de lo dispuesto en el Art. 4 del Código Penal Ecuatoriano que dice: "Prohíbese en materia penal la interpretación extensiva. El juez debe atenerse, estrictamente a la letra de la Ley. En los casos de duda se la interpretará en el sentido más favorable al reo". Aplicando criterios futuristas qué podría ocurrir en el caso de que existiese una proliferación de

[1] DR. VLADIMIRO ALVAREZ, "Elementos que debe tener una Ley", Diciembre 14 del 2002.

delitos informáticos, tal y como está la legislación actual la pregunta a formularse es : ¿si se aplicaría o no el delito a Internet?

El principal problema que radica en la legislación ecuatoriana ante las nuevas formas de comportamiento que se originan en Internet, ocurre en vista que la "legislación se basa en el principio del Derecho Romano: nulliun crimen nullium pena sine lege, es decir, no existe delito si previamente no se encuentra determinada la conducta típica antijurídica en la ley, por lo tanto, en el Ecuador no existe delito informático propiamente dicho"[2]. Si a esto se le suma el problema de la prueba, es decir, que contar con ellas es complicado porque son fáciles de borrar dado que las TIC´S lo permiten, el problema es entonces aún más grave.

Para lograr que las leyes sean más fácilmente interpretadas conviene en algunas ocasiones redactarlas más al detalle para que no exista lugar a dudas o malas interpretaciones. A continuación se destacarán los principales puntos que se deben tener presente cuando se elaboren proyectos de leyes que traten de controlar y regular las nuevas modalidades o formas de comportamiento que trae consigo Internet. Para mayor facilidad se mantendrá el mismo esquema de los temas tratados a lo largo del presente documento.

La siguiente tabla ilustra las ponderaciones que se utilizaron para determinar el grado de falencias de los diversos delitos que existen en los temas de: censura, propiedad, privacidad, seguridad y responsabilidad.

1	Nulo
2	Bajo
3	Medio
4	Alto
N/A	No aplica

Tabla 14. Ponderación de Falencias.

Censura.

La tabla muestra los delitos relacionados a la censura, en ella se establece el grado de falencias que tienen actualmente:

Delitos de Censura	**Ponderación**
Pornografía	N/A
Lenguaje violento	2
Información para la ayuda a actividades dañinas	2
Daño virtual	4
Ciberterrorismo	2

Tabla 15. Delitos relacionados a la Censura.

Pornografía.

Como se lo mencionó en la definición del problema, capítulo 1 - sección 2, la pornografía no será analizada porque el ámbito en el que se desarrolla es muy amplio, ya que

[2] OSWALDO Huilcapi Arturo, CETID, "El Delito Informático", http://www.dlh.lahora.com.ec/paginas/judicial/paginas/D.Informatico.23.htm , Noviembre 11 del 2002.

no solo se desarrolla por la falta de regulación en Internet, sinó que existen otros medios de comunicación que contribuyen a ella tales como: revistas, televisión, cine, entre otros.

Lenguaje Violento.

- En el Código Penal Ecuatoriano si existen sanciones para cualquier actitud que cause discordia entre los ciudadanos.
- El problema radica en que la ley no especifica la forma como puede originarse.
- Consideremos lo siguiente:
  - Caso 1: ¿Qué derecho se lesiona cuando se crea un sitio web en donde se publiquen temas raciales y se incite a la creación de movimientos que ataquen a los indígenas o negros?
  - Caso 2: ¿Qué derecho se lesiona cuando por medio de e-mail se forma una cadena de correos en donde se incita a las personas a armarse, tomar el país a la fuerza y violar toda la constitución?

En el caso 1 se atenta contra el derecho a la libertad, en cambio en el caso 2 se atenta hacia la seguridad nacional y la democracia.

Leguaje Violento es toda forma en la cual se atenta hacia la cultura, raza, religión, culto o alguna otra afinidad de los individuos, es decir, que a través del uso de palabras se entra en discordia.

Información para la ayuda a actividades dañinas.

- Las leyes ecuatorianas tipifican el daño como tal, existen sanciones ante los delitos mencionados
- El problema se origina cuando las personas aprovechándose del derecho a la libertad de expresión y de las facilidades que presentan las TIC´s, hacen un mal uso de Internet. Detectar la responsabilidad de quienes inducen a cometer los daños es complicado.

Información para la ayuda a actividades dañinas es la información donde se guía a la persona para la comisión de delitos tales como: creación de bombas, asesinatos, suicidios, robos, entre otros.

Daño Virtual.

- En la legislación ecuatoriana sólo se considera el daño tangible.
- Por lo tanto, existe la necesidad de que se consideren las diferentes formas en que se puede atentar contra la humanidad.
- Consideremos lo siguiente:
  - Caso 1: ¿Qué derecho se lesiona cuando en un sitio web se dan indicaciones para la creación de bombas o formas de asesinar?
  - Caso 2: ¿Qué derecho se lesiona cuando se presenta en un sitio web información de cómo efectuar un robo?.
  - Caso 3: ¿Qué derecho se lesiona cuando se presenta en un sitio web información difamatoria de una persona?.

En el caso 1 se atenta contra la vida, en el caso 2 es en contra de la seguridad y bienes materiales, en el caso 3 se atenta contra la honra de una persona, por lo tanto las consecuencias son diferentes, y debe haber sanción para cada una de los delitos.

Daño[3] "es el delito consistente de causar daños de manera deliberada en la propiedad ajena", entonces ***Daño Virtual*** es toda forma de causar daño en un medio intangible (Internet).

Ciberterrorismo.

- En el Código Penal Ecuatoriano se sanciona el terrorismo.
- El problema ocurre al no especificarse que medidas tomar cuando el terrorismo es cometido a través de Internet; razón por la que es necesario que se consideren las diferentes formas en se puede llevar a cabo el terrorismo en la red.
- Consideremos lo siguiente:
  - Caso 1: ¿Qué derecho se lesiona cuando se acceda a la base de datos de la seguridad nacional?
  - Caso 2: ¿Qué derecho se lesiona con la intersección de comunicados confidenciales del país?
  - Caso 3: ¿Qué derecho se lesiona con la falsificación de documentos?
  - Caso 4: ¿Qué derecho se lesiona con el sabotaje de los equipos de instituciones u organismos del Estado?
  - Caso 5: ¿Qué derecho se lesiona cuando se viola la seguridad de los sistemas del Estado?

Cada caso mencionado es diferente al otro, y por tanto, se deben de considerar los efectos de los mismos al momento de aplicar las sanciones.

Terrorismo[4] "es la sucesión de actos de violencia ejecutados para infundir terror", ciber es el prefijo utilizado en la comunidad Internet para denominar conceptos relacionados con las redes. Por lo tanto el ***Ciberterrorismo*** es toda acción de violencia terrorífica en la red.

Se puede observar que en los delitos relacionados a la "censura" (lenguaje violento, en la información para la ayuda a actividades dañinas, en el daño virtual y el ciberterrorismo) existe un ELEMENTO EN COMUN el cual es "el medio a través del cual se hacen las publicaciones de ciertos contenidos de Internet", la publicación de los sitios web se lo hace a través de empresas proveedoras de Internet (ISP), las cuales proporcionan el servicio de alojamiento necesario para levantar el sitio.

Se debe de considerar que los ISP no son responsables de los contenidos que se publiquen cuando:

a) No tengan conocimiento efectivo de que la actividad o la información almacenada es de carácter ilícito o de que lesionan bienes o derechos de terceras personas; y,
b) En caso de que existan contenidos que atenten al bienestar social, retiren los datos o hagan imposible el acceso a ellos.

---

[3] Diccionario de la Real Academia Española, Op. Cit. pp.13.
[4] Diccionario de la Real Academia Española, Op. Cit. pp.13.

Propiedad Intelectual.

La tabla siguiente muestra los delitos relacionados a la propiedad intelectual, en ella se establece el grado de falencias que tienen actualmente:

Delitos de Propiedad Intelectual	**Ponderación**
Piratería de software y otras propiedades	2
Cibersquatting(nombres de dominio)	3

Tabla 16. Delitos relacionados a la Propiedad Intelectual.

Piratería de software y otras propiedades

- La piratería de software si presenta regulación en las leyes ecuatorianas.
- El problema se origina en la medida del cumplimiento de las mismas, es decir, a la falta de honestidad de las personas; unos dicen que los softwares tienen costos elevados para la realidad del país, otros simplemente aprovechan la oportunidad y se las ingenian para obtenerlos.
- Ante esta situación es necesario que se describa bien el hecho de la piratería, pues al momento de establecer las pruebas del robo se debe tener presente que no necesariamente hay que sustraer físicamente el original, basta con sacar una copia sin autorización.
- Actualmente existe la tendencia del software libre, éstos son programas que están a disposición en Internet de forma gratuita.

Piratería de Software es toda acción donde se obtiene sin pago y licencia de uso un programa, el look and feel de un programa o el algoritmo.

Cibersquatting (nombres de dominio).

- Respecto a los registros de los nombres de dominio, no existe en la normativa jurídica ecuatoriana leyes o normas que regulen esta actividad, la encargada del registro de nombres de dominios es la empresa NIC.EC representante de la OMPI (Organización Mundial de la Propiedad Intelectual) cuando ocurren problemas interviene la Política Uniforme de Resolución de Disputas del ICAAN [5].

Privacidad.

La tabla muestra los delitos que atentan contra el derecho a la privacidad, en ella se establece el grado de falencias que tienen actualmente:

Delitos de Privacidad	**Ponderación**
Manipulación de Datos Personales	1
Hackers	2

[5] ICANN, Op. Cit. pp. 26

Publicidad Indeseada(spam)	1
Vigilancia Laboral	2

Tabla 17. Delitos relacionados a la Privacidad.

Manipulación de Datos Personales.

- La legislación ecuatoriana respecto a la protección al derecho de la privacidad, está bastante completa, con la reciente expedición de la ley de "COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS" y a su vez con las reformas que se hicieron al Código Penal Ecuatoriano donde se tipificó la problemática respecto a los e-mails y a la seguridad.

Hackers

- Con la reforma realizada al Código Penal Ecuatoriano y con la expedición de la ley de "COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS", los delitos informáticos relacionados con el sabotaje, fraude y falsificación, ya se encuentran tipificados.
- Las debilidades de la normativa jurídica se dan por el hecho de que no se hace mucha diferencia en el momento de aplicar las sanciones, es decir, un Hacker no es lo mismo que un Cracker. Para comprender mejor a la sociedad delictiva que actúa a través del uso de Internet, es conveniente establecer los casos que pueden presentarse.
- Consideremos lo siguiente:
  - Caso 1: ¿Qué derecho se lesiona cuando un sujeto motivado por el simple ánimo de competencia o por probar sus habilidades, viola la seguridad de un Estado o una empresa, de tal manera que sólo se limita a acceder y dan una mirada y sale sin hacer ninguna manipulación a la información?
  - Caso 2: ¿Qué derecho se lesiona cuando un sujeto viola la seguridad de un Estado o una empresa y se apropia de información y la vende a terceras personas?
  - Caso 3: ¿Qué derecho lesionan aquellos individuos que andan probando cada software de hacking y cracking que se encuentran en la red y sin ánimo de hacer daño perjudican a terceros?
  - Caso 4: ¿Qué derecho lesionan aquellos individuos que se encargan de navegar por la red, violando la seguridad para sustraer información interesante que se pueda vender?
  - Caso 5: ¿Qué derecho lesionan aquellos individuos que tienen conocimientos especializados en telefonía y los utilizan para escuchar conversaciones privadas?

Los casos mencionados tienen como elemento común la "violación a la privacidad", sin embargo se debe de analizar qué es lo que ocurre cuando el individuo está dentro del sistema de información, es decir, la finalidad que tienen al navegar por la red.

***Según* Claudio Hernández[6] éstos son las definiciones para:**

Hacker es el primer eslabón de una sociedad delictiva, experto en sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica, desean comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en computadoras remotas, con el fin de decir aquello de he estado aquí pero no modifican ni se llevan nada de la computadora atacada.

Cracker es el siguiente eslabón y por tanto el primero de una familia rebelde, tiene la capacidad de romper sistemas y software y se dedica única y exclusivamente a crackear sistemas.

Lamer rastrea en la basura cibernética de la red, se baja todos los programas y los prueba todos; pasa la vida fastidiando, enviando bombas lógicas o virus por la red, y lo peor de todo es que cree saber algo.

CopyHacker obtiene lo que le interesa y se lo vende a alguien sin escrúpulos que comercializará el sistema posteriormente, suelen leer todo lo que hay en la red y las revistas técnicas en busca de alguien que sabe algo. Después se pone en contacto con aquella persona y trata de sacarle la idea.

Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles e interfiere en las transmisiones.

Publicidad Indeseada(spam).

- Con la ley de "COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS" se puede controlar la publicidad indeseada, pues se establece que para recibirla se debe dar consentimiento, y a su vez se concede el derecho de ser removido de bases de datos, cadenas de información o listas de envío de publicaciones o publicidades periódicas.

- Lo que hace falta es normar que el mensaje enviado al individuo debe de tener como parte del título del mensaje la palabra "publicidad", de tal forma que sin tener que leer el mensaje los individuos pueden borrarlo, si así lo desean, y evitar pérdidas de tiempo.

Publicidad indeseada (spam) "es la publicidad que llega al correo electrónico sin que el usuario la haya solicitado, el correo no solicitado en Internet ocupa espacio en servidores que no son de los promotores, causa tráfico innecesario y le cuesta a los usuarios que usan tiempo de enlace para bajarlo a sus máquinas"[7].

---

[6] HERNANDEZ Claudio, libro: Hackers, Los piratas del Chip y de Internet, capítulo *" La Nueva Cibersociedad "*, 2001 , http://perso.wanadoo.es/snickers/, pp 31-48.

[7] *" Correo Electrónico, no solicitado "* http://laguna.fmedic.unam.mx/~adrian/spamlinks.html.

Vigilancia Laboral

- En la legislación ecuatoriana existe la protección a la privacidad y la intimidad.
- El problema ocurre en la medida de considerar que toda la información manipulada por el empleado durante las horas de trabajo pertenece a la empresa, con el acceso a Internet en muchas ocasiones, el personal dedica parte del tiempo de trabajo a hacer actividades personales; ante dicha circunstancia las empresas están aplicando mecanismos de vigilancia. Razón por la cual se debe regular, en vista de que se atenta contra los derechos civiles de los ecuatorianos estipulados en la Constitución Política de la República del Ecuador.
- Consideremos lo siguiente:
  - Caso 1: ¿Qué derecho se lesiona cuando se monitorea los e-mails y documentos electrónicos de un empleado?

En este caso se debe tener presente que durante las horas de trabajo se deben realizar actividades relacionados con la empresa, la revisión atenta contra el derecho a la privacidad del empleado.

Vigilancia laboral es la acción de controlar las actividades que realizan los empleados en su lugar de trabajo.

Seguridad.

La tabla muestra los delitos que atentan a la seguridad de las TIC´s, en ella se establece el grado de falencias que tienen actualmente:

Delitos de Seguridad	**Ponderación**
Virus	2
Delitos en el E-Commerce	2

Tabla 18. Delitos relacionados a la Seguridad de las TIC´s.

Virus

- En las modificaciones que se hicieron al Código Penal Ecuatoriano, a través de la ley de "COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS", se tipificaron las sanciones relacionadas al daño.
- La debilidad de la norma ocurre porque se expresa que "el daño sea realizado por cualquier método", y por analogía se puede incluir dentro de los métodos por los cuales se comete el daño al virus. Sería conveniente que se adjunte en el glosario de esta ley la definición de lo que debe entenderse por virus informático.

Virus informático es una serie de instrucciones de programación que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar al sistema por Internet o por cualquier soporte lógico tales como: diskettes, CDROM, etc.

Delitos en el E-Commerce.

- La ley de "COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS" es suficientemente completa porque abarca regulación para la firma digital, certificadores y además hace reformas al Código Penal Ecuatoriano respeto a las sanciones para los delitos de sabotaje, falsificación y fraudes informáticos.

- Para una mejor interpretación de la "Normativa Jurídica Ecuatoriana" sería conveniente que se definan los conceptos de los delitos posibles antes mencionados, de manera que se pueda hacer una diferenciación en las sanciones.

Según la Dra. María Cristina Vallejo[8] considera las siguientes definiciones:

Delito Informático son aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

Sabotaje Informático es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema.

Falsificación Informática es el engaño computarizado, es decir, que se pueden elaborar tarjetas de crédito, cheques, títulos valores, en general todo tipo de documentos públicos y privados, o se puede alterar todo el sistema contable de una Empresa, facilitando a las sociedades comerciales llevar la doble contabilidad, todo esto con miras a evadir impuestos.

Fraude Informático o Estafa informática, consiste en el provecho ilícito que se obtiene con daño patrimonial, mediante el empleo de artificios o engaños idóneos para conducir a otro en error, sirviéndose a su vez de una computadora o vulnerando sus seguridades.

[8] VALLEJO Maria Cristina, Dra., *"El sabotaje o daño"*, http://www.dlh.lahora.com.ec/paginas/judicial/paginas/D.Informatico.28.htm, Noviembre 11 del 2002