ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Escuela de Diseño y Comunicación Visual

LA LIBERTAD DE EXPRESIÓN EN LA SOCIEDAD DE LA INFORMACIÓN COMO DERECHO FUNDAMENTAL PARA LA DIVULGACIÓN DE LA CIENCIA Y TECNOLOGÍA: ENTORNO MUNDIAL Y SITUACIÓN EN EL ECUADOR

Previa la obtención del Título de:

Magíster en Comunicación Pública de Ciencia y Tecnología

Presentado por:

Lcda. Lady Katherine Rodríguez Dumes

Guayaquil- Ecuador

2013

DEDICATORIA

A Dios por regalarme tantas bendiciones y oportunidades.

Lcda. Lady Rodríguez Dumes

AGRADECIMIENTO

La finalización de esta tesis fue posible con la dirección del Ph.D. Fernando Morante, las sugerencias de la M. Sc. María de los Ángeles Custoja y las opiniones de todos los expertos que participaron dentro del proceso de mi investigación.

Lcda. Lady Rodríguez Dumes

TRIBUNAL DE GRADO

Máster Fausto Jácome

DIRECTOR DE LA ESCUELA

Ph.D. Fernando Morante

DIRECTOR DE TESIS

M. Sc. María de los Ángeles Custoja

VOCAL

DECLARACIÓN EXPRESA

La responsabilidad del contenido de este Proyecto de Grado, corresponde exclusivamente a la autora; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

_____

Lcda. Lady Katherine Rodríguez Dumes

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Introducción

No hay libertad sin libertad de información. No hay libertad de Información sin libertad de Internet" (Global Internet Freedom Consortium, 2008).

Internet, hoy en día, proporciona un sistema insuperable para la comunicación pública de la ciencia y la tecnología de una forma interconectada e interoperable, a nivel mundial.

El acceso a la información, la creación y el compartimiento del conocimiento, que caracterizan a la Sociedad de la Información en que vivimos, contribuyen significativamente al desarrollo económico, social y cultural de los pueblos.

Los gobiernos del mundo reconocieron en la Cumbre Mundial de la Sociedad de la Información (2003) que las Tecnologías de la Información y la Comunicación (TIC) permiten a la población tener acceso a la información y al conocimiento en cualquier lugar del mundo y de manera prácticamente instantánea. La comunidad científica está aprovechando las ventajas de las comunicaciones instantáneas utilizando las herramientas modernas que ofrece la web 2.0, como las redes sociales, blogs, wikis, grupos de discusión, webcasts, conferencias virtuales y sistemas de mensajería instantánea, entre otras. La difusión de los resultados de la ciencia y la tecnología efectuada tradicionalmente a través de libros y revistas especializadas impresas en papel se ha trasladado a la web, al publicarse simultáneamente en versiones electrónicas. Las bases de datos bibliográficas con formato electrónico consultadas a través de Internet facilitan notablemente la actividad de la investigación científica y de la academia Igualmente los repositorios o archivos digitales científicos tienen como objetivo

fundamental difundir por Internet de una manera más visible, los resultados de la investigación científica.

CICYT (2009, p. 23) sostiene que "El auge de la sociedad de la información, el fenómeno de la globalización y los procesos derivados de la investigación científica y del desarrollo tecnológico están transformando las maneras de organizar el aprendizaje o de generar y transmitir el conocimiento. Dentro de este contexto, la Espol debe liderar el proceso de cambio en el Ecuador y reforzar su actividad investigadora para configurar un modelo que tenga como eje el conocimiento".

Las TICs se constituyen en la herramienta fundamental para la construcción de esta Sociedad de la Información, por lo tanto es vital que esté garantizada la libertad de Internet como un derecho fundamental de todas las personas.

Las libertades comunicativas e informativas que ofrece el uso colectivo de las tecnologías de la información y comunicación en la tendencia actual de la Sociedad de la Información, amerita sean analizadas en cuanto a sus alcances como garante de la libertad de expresión, del derecho a la información, del derecho a la privacidad, de la seguridad informática, de la protección a menores, de la protección legal y regulatoria de los derechos digitales en su entorno mundial y en el Ecuador.

Internet se ha convertido en un medio de comunicación vital para que las personas puedan ejercer su derecho a la libertad de expresión o el derecho de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, como se garantiza en los artículos 19 de la Declaración Universal de Derechos Humanos y del Convenio o Pacto Internacional de Derechos Civiles y Políticos. Se consideran como Derechos digitales de una manera genérica a aquellos que están vinculados directamente

con la libertad de expresión en línea, pero también indirectamente, a través de esta libertad, al acceso a Internet, a la privacidad y la protección de datos personales.

En la presente tesis se investigará si en el entorno mundial y en el Ecuador se dispone del marco legal que garantice la libertad de expresión en línea, si se reconoce la libertad de expresión en línea como un derecho universal de todas las personas y si existe libertad de Internet en todos los países del mundo.

En el Capítulo 1 se hará una revisión de la literatura que se ha escrito sobre la libertad de expresión en línea y las limitaciones que se encuentren en ella. En el Capítulo 2 se hará referencia a la metodología utilizada para realizar la investigación y se plantearán las hipótesis de investigación. En el Capítulo 3 se desarrollará el marco teórico conceptual de este estudio, efectuando un análisis minucioso de los enunciados de la Cumbre Mundial de la Sociedad de la Información, de la normativa internacional que constituye el marco legal que garantiza la libertad de Internet como un derecho fundamental de todas las personas; el rol central que están jugando las redes sociales como portadoras de nuevas formas de interacción social, de diálogo, intercambio y colaboración; las diferentes técnicas utilizadas para el filtraje en Internet y, un análisis sobre la percepción mundial sobre la libertad de expresión en línea como un derecho fundamental de todas las personas y sobre los aspectos que más preocupan a los usuarios. En el Capítulo 4 se establecerán las protecciones legales y regulatorias de los derechos digitales, determinando primeramente en base a investigaciones realizadas por organizaciones no gubernamentales, los países donde se practica la censura en internet; los derechos de propiedad intelectual versus la libertad de acceso al conocimiento; el derecho a la privacidad y a la protección de los datos personales; la protección de los niños en línea y la normativa internacional sobre el discurso odioso. En el Capítulo 5 se estudiarán las políticas mundiales sobre la seguridad informática; se tratará sobre la Agenda sobre la ciberseguridad mundial, y la estrategia nacional de ciberseguridad reflejada en la

creación del Centro de Respuesta a Incidentes Informáticos en el Ecuador. En el Capítulo 6 se presentarán 3 casos de estudio sobre amenazas a la libertad de expresión en línea: Wikileaks, China y la primavera árabe, los mismos casos que mediante un análisis comparativo nos pueden permitir establecer si en el Ecuador existe libertad de expresión en línea. Finalmente, en el Capítulo 7 se hará un análisis detallado de la Constitución de la República del Ecuador para establecer si está consagrado en la Carta Magna el derecho a la libre expresión en Internet, al acceso a Internet, a la información, a la privacidad y a la protección de los datos personales; de igual forma se efectuará un análisis de la Ley Orgánica de la Comunicación a fin de establecer si contiene disposiciones que puedan representar amenazas para la libertad de expresión en línea en el Ecuador; y, finalmente se detallará la aplicación del método Delphi utilizado en esta investigación y los resultados obtenidos.

Capítulo 1

Revisión de la literatura sobre la libertad de expresión en la era digital.

1.1. Literatura existente sobre la libertad de expresión en línea.

El informe de la Comisión Internacional para el Estudio de los Problemas de la Comunicación establecida por la Unesco en 1980, titulado ´Un solo mundo, voces múltiples: Comunicación e información en nuestros tiempos´, conocido como el Reporte MacBride, por ser su autor Sean MacBride, presidente de la Comisión y Premio Nobel de la Paz, propone un nuevo orden mundial de la información y la comunicación, más justo y eficiente.

En este informe se manifiesta que entre las obstrucciones más evidentes y repugnantes a la libertad de expresión, se encuentra la violencia física sufrida por los periodistas de todas las corrientes del pensamiento, que incluye el hostigamiento, el secuestro, la detención, la tortura, los ataques con bomba y los asesinatos.

Se agrega que es posible que las restricciones legales más graves se apliquen en nombre de la "seguridad nacional" y que, aunque todos los Estados tienen derecho a mantener en secreto la información que afecte la seguridad nacional, hay abuso cuando se extienden leyes para incluir la información política, técnica o industrial y, peor aún, la expresión de opiniones.

La censura, agrega el informe, en una forma u otra es muy común – puede usarse para controlar la pornografía, o la incitación a la violencia, por ejemplo, o puede operar en épocas de emergencia nacional –, pero también se usa para proteger a los gobiernos contra la crítica y es así que por todo el mundo se han implementado sistemas arbitrarios y abusivos de censura. El informe recomienda diseñar instrumentos de política de nivel nacional, a fin de evaluar las implicaciones sociales, positivas y negativas, de la introducción de poderosas tecnologías de la comunicación de nuevo cuño.

En el informe provisional presentado por la Comisión en 1978, se afirma que pese a la expansión de todas las estructuras de comunicación social tradicionales, hay un nuevo sector del mundo de la comunicación que rebasa a todos los demás por su rapidez de crecimiento, que está transformando rápidamente las sociedades actuales y que será indudablemente uno de los fundamentos del porvenir; se trata de un inmenso campo de operaciones, relativo a los datos y la información y que se designa habitualmente con la palabra *informática*.

Es oportuno mencionar, por tratarse del tópico de la maestría en Comunicación Pública en Ciencia y Tecnología, realizada en la ESPOL, que en este informe se afirma que la función principal de la comunicación en materia de ciencia y tecnología es "la gestión del saber humano -de la memoria colectiva-, de toda la información que necesita la sociedad para progresar en el mundo moderno. Esta función consiste en crear dispositivos de transferencia de la información, lo cual plantea tres problemas de carácter esencialmente técnico: ¿cómo tener acceso a la información?, ¿cómo administrar y tratar la información? y ¿cómo utilizarla eficazmente?".

Se reconoce en este informe que hoy en día, se siente de un modo cada vez más general la exigencia de un nuevo orden mundial de la información, cuya implementación está

íntimamente relacionada con las aspiraciones encaminadas al establecimiento de un nuevo orden económico internacional.

Dutton, et al. (2011, p. 5) elaboran un marco conceptual de la **ecología** de la libertad de expresión tomando en consideración que el Internet y su convergencia con las comunicaciones móviles han permitido incrementar inmensamente el acceso a los recursos de información y comunicación y que, paralelamente, ha aumentado la preocupación de los defensores de los derechos digitales sobre medidas que pueden atentar contra la libertad de expresión en Internet. Este marco se centra en los siguientes seis aspectos:

1.- Iniciativas técnicas relacionadas a la conexión y desconexión, tales como filtraje de contenidos.
2.- Derechos digitales, incluyendo aquellos vinculados directamente con la libertad de expresión y censura, pero también indirectamente, con la libertad de expresión, privacidad y la protección de datos.
3.- Regulación y políticas industriales, conteniendo derechos de autor y propiedad intelectual, estrategias industriales y TIC´s.
4.- Usuarios, en lo que respecta a mediciones centradas en fraude, protección de niños, honestidad, difamación y control del discurso del odio.
5.- Prácticas y políticas de red, incluyendo estándares sobre la identidad y la regulación de proveedores de servicio de Internet; y,
6.- Seguridad informática, extendiéndose desde el control de spam y virus hasta la protección de la seguridad nacional.

Dutton, et al. (2011, p. 8) declaran que la continua reinvención y difusión mundial de Internet lo han convertido en el principal medio de expresión del siglo XXI, cada vez más creciente, desafiando el rol de los más tradicionales medios de difusión masivos

incluyendo la radio, la televisión y los periódicos. Sin embargo, los autores expresan su preocupación sobre la existencia de amenazas legales y regulatorias contra la libertad de expresión en Internet, como el filtraje de los contenidos en Internet.

Dutton, et al. (2011, p. 11) manifiestan que Internet como una red de redes de cubertura mundial permite a los pueblos informarse y educarse por sí mismos, expresar sus puntos de vista y participar en la sociedad civil y en los procesos democráticos en una extensión nunca vista antes. Nuevas formas de información y participación como periódicos en línea, blogs y sitios de redes sociales, están desafiando a los medios tradicionales proponiendo nuevas formas de comunicación, al permitir a los usuarios: compartir, generar y aún, cocrear o coproducir información.

Faris y Villeneuve (2011, p. 10) sostienen que la percepción de amenaza a la seguridad nacional es una razón común que se utiliza para bloquear el contenido. El filtrado de Internet que se dirige a los sitios web de los insurgentes, extremistas, terroristas y otras amenazas, generalmente gana amplio apoyo público.

Faris y Villeneuve (2011, p. 24) consideran que la conexión entre regímenes represivos y filtraje político sigue una lógica clara, sin embargo, la conexión entre regímenes que suprimen la libre expresión y realizan actividad de filtraje social, es menos obvia.

Zittrain and Palfrey (2011, p. 29) opinan que parece difícil de creer que una enciclopedia online y gratuita que todos pueden editar en cualquier momento podría importar mucho a alguien. De ahí que, Wikipedia se ha convertido en muy popular y enormemente influyente a pesar de su formato inusual. Artículos de Wikipedia relatan las protestas en la Plaza Tiananmen de 1989, el Dalai Lama, el Movimiento Internacional del Tíbet Independiente y el movimiento de Taiwan Independiente; tanto en las versiones en inglés y chino de Wikipedia, cada una escrita independientemente, estos artículos han

sido escritos desde un punto de vista que Wikipedia llama neutral. Sin embargo, los puntos de vista de Wikipedia en algunos tópicos no son vistos por las autoridades chinas como neutrales. Wikipedia ha incrementado su influencia y en efecto ha atraído la atención de la censura china por lo menos tres veces entre 2004 y 2006.

Zittrain and Palfrey (2011, ps. 32 – 33) sostienen que cuando los Estados deciden filtrar el acceso a Internet, el enfoque generalmente implica el establecimiento de una falange de leyes y medidas técnicas para bloquear el acceso o la publicación de información en línea a los ciudadanos. Las leyes son generalmente extensiones de regímenes regulatorios de medios o de telecomunicaciones. Ocasionalmente, estas leyes toman la forma de regulaciones y estatutos específicos de Internet. Estas leyes raras veces establecen explícitamente el régimen técnico de filtraje, pero más comúnmente establecen un marco para restringir ciertas clases de contenido en línea y prohibir ciertas actividades en línea.

Los autores agregan que un Estado tiene varias opciones iniciales para establecer un régimen técnico de filtrado: sistema del nombre de dominio (DNS), filtraje de las direcciones de Protocolo Internet (IP) y filtraje URL. Muchos Estados con regímenes de filtrado avanzado implementan el filtraje URL en vista de que este método puede ser el más seguro.

Zittrain and Palfrey (2011, p. 42) afirma que hay un continuo crecimiento en la creación de información en línea por parte de los ciudadanos, incluyendo ciudadanos periodistas, en la mayor parte del mundo, pero el filtraje está produciendo un impacto en la forma cómo las personas llevan a cabo esta actividad.

Jeremy Brown, ministro para las Américas del Ministerio Británico de Relaciones Exteriores, con motivo de celebrarse el 3 de mayo del 2012 el Día Mundial de la Libertad de Prensa, expresó que:

> *"La libertad de prensa tiene el poder de transformar las sociedades y de cambiar el curso de la historia. Durante el año pasado, a lo largo del Medio Oriente y África del Norte, los ciudadanos comunes descubrieron sus voces mediante el uso de las redes sociales y los blogs. Pero la libertad de expresión sigue siendo reprimida en muchos países y algunos de ellos han visto una disminución significativa de la libertad de prensa. En todo el mundo periodistas, bloggers, entre otros, han percibido obstáculos durante el desarrollo de su trabajo, siendo acosados, vigilados, detenidos o sometidos a la violencia…Los medios digitales y sociales han cambiado el mundo, pero ese proceso de cambio plantea nuevos desafíos. El actual marco de la ley internacional de derechos humanos - incluido el derecho a la libertad de expresión - es igualmente aplicable si estamos conectados o no a Internet. Pero mientras los gobiernos encuentran nuevas maneras de bloquear la crítica legítima y los manifestantes encuentran nuevas maneras de escapar de su control, la batalla tecnológica diaria muestra cómo las reglas van cambiando constantemente… La libertad en Internet existe y es imparable - los intentos de bloquear sitios web y de sofocar el libre debate serán inútiles. La pregunta para los gobiernos de todo el mundo no es cómo reprimir la libertad de expresión - en línea o fuera de línea -, sino más bien cómo participar e interactuar con su población".*
>
> *(ukinecuador.fco.gov.uk/es/news/?view=News&id=761348482,* visto el 14 de febrero del 2013)

Mendel, et al. (2012, p. 9) expresan que hay una tensión entre el derecho a la expresión y el derecho a la privacidad. Estos autores (p. 14) agregaron que cada computador,

teléfono móvil, u otro aparato conectado a Internet tiene una única dirección IP, la cual provee una identificación única para cada aparato, lo que significa a su vez que ellos pueden ser rastreados. La capacidad de localizar cualquier aparato crea significativos nuevos desafíos de privacidad.

1.2 Limitaciones de la literatura.

En lo que respecta a la literatura revisada se puede concluir que, existe una importante colección de publicaciones realizadas por organizaciones no gubernamentales y fundaciones privadas que han estudiado y estudian la situación de la libertad en Internet, con toda la temática en ella involucrada que será analizada en los siguientes capítulos de la presente tesis; sin embargo, no existe un estudio en conjunto de la interrelación entre los diferentes factores que afectan a la libertad de expresión en línea, no se ha investigado la situación de la libertad de expresión en línea en varios de los países del mundo, entre ellos el Ecuador, y si bien existe un pleno conocimiento del marco legal y regulatorio que garantiza la libre expresión en línea, no se dispone de un estudio que determine si en Ecuador existe dicho marco legal que proteja los derechos digitales de los ecuatorianos. Estas limitaciones serán cubiertas con la presente tesis.

Capítulo 2

Metodología

2.1 Objetivos de la Investigación

Objetivo General

La investigación propuesta tiene por objeto evaluar si existe una verdadera libertad de expresión en Internet y un pleno goce del derecho de acceso a Internet en los países del mundo, en general, y en el Ecuador, en particular. Se revisarán casos de estudios y se utilizará el método Delphi para probar si están garantizados éstos derechos digitales y si existe seguridad informática que brinde a los usuarios de Internet la confianza necesaria para la utilización de las tecnologías de la información y la comunicación.

Objetivos específicos

- Determinar si la libertad de expresión se aplica a Internet.
- Investigar si la libertad de expresión en línea será un derecho de todas las personas.
- Detectar si existe libertad de expresión en línea.
- Determinar si existe seguridad y confianza para los usuarios de Internet.
- Revisar el marco legal ecuatoriano para establecer si está garantizada la libertad de expresión en línea en el país.

Hipótesis

Las hipótesis nulas (H_0) y las hipótesis alternativas (H_1) que se plantean en este estudio son:

$H_{0:}$ La libertad de expresión en línea no será un derecho de todas las personas.

H_1: La libertad de expresión en línea será un derecho de todas las personas.

H_0: En los próximos años no habrá libertad de expresión en línea en todos los países del mundo.

H_1: En los próximos años habrá libertad de expresión en línea en todos los países del mundo.

H_0: El Centro de Respuesta Global (CRG) no brindará la protección y confianza necesarias contra las ciberamenazas que afectan a los usuarios de Internet.

H_1: El Centro de Respuesta Global (CRG) brindará la protección y confianza necesarias contra las ciberamenazas que afectan a los usuarios de Internet.

H_0: La Constitución de la República del Ecuador no proveerá el marco legal que garantice la libertad de expresión en línea.

H_1: La Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea.

H_0: El Reglamento de Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y Valor Agregado del Ecuador no atentará contra la privacidad de los usuarios de Internet.

H_1: El Reglamento de Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y Valor Agregado del Ecuador atentará contra la privacidad de los usuarios de Internet.

H_0: La Ley Orgánica de Comunicación del Ecuador no constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet.

H_1: La Ley Orgánica de Comunicación del Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet.

H_0: No existirán amenazas de ciberataques a los usuarios de Internet en el país.

H_1: Existirán amenazas de ciberataques a los usuarios de Internet en el país.

Para la prueba de razón de verosimilitud de la hipótesis nula con estadística inferencial o predictiva, se utilizará un intervalo de confianza (1 – α) 100% del 95%, es decir que el nivel de significancia será α = 0.05. Para el efecto se efectuará "**la prueba t de una muestra"** (one-sample test) utilizando el software SPSS Statistics 17.0 (Statistical Package for the Social Science). El valor t de la muestra se determina mediante la fórmula:

$$t = \frac{\bar{x} - \mu}{\frac{S}{\sqrt{n}}}$$

Donde:

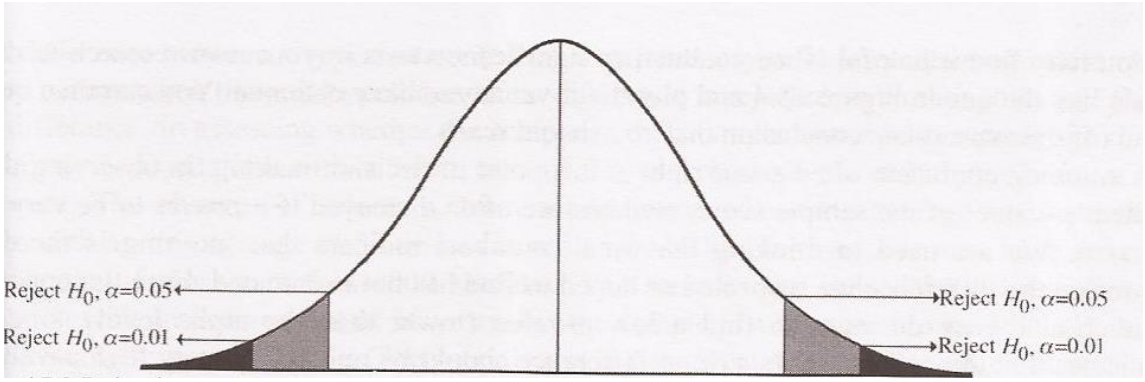
$\bar{x}$ = valor promedio de la muestra

μ = valor de la prueba

S = desviación estándar de la muestra

n = numero de observaciones

El valor crítico de t se lo obtiene de la tabla estadística (ver Anexo 2) de valores críticos de t en función del grado de libertad (n-1) y del nivel de significancia (α). En la Figura 2.1 se ilustra las regiones críticas de distribución t para rechazar la hipótesis nula (H_0), así como también el intervalo de confianza.



Fuente: Argyrous G (2010, p. 223, Fig 15.2)

Figura 2.1: Regiones críticas de distribución t para rechazar la hipótesis nula (H_0) en α=0.05 y α=0.01, para una o dos colas

Siguiendo el criterio de Freund, Miller y Miller (2000, p. 417), se utiliza la "prueba t de una muestra" para rechazar o aceptar la hipótesis nula (H_0) en virtud de que en el presente estudio el número de observaciones es menor que 30 y no se conoce la desviación estándar de la población.

2.2 Método de investigación

Neuman (2006, p. 2) sostiene que metodología y métodos, son dos términos considerados a menudo como sinónimos. Metodología es más amplia que métodos y abarca a los métodos. Neuman agrega que la metodología es el entendimiento del contexto social organizacional, las asunciones filosóficas, los principios éticos, y los asuntos políticos de la actividad de los investigadores sociales que usan métodos. El autor agrega que métodos son un grupo de técnicas específicas para seleccionar casos, medir y observar aspectos de la vida social, obtener y redefinir información, analizar la

información y reportar en resultados. Metodología y métodos están muy vinculados y son interdependientes, pero distintos. La metodología se preocupa de la estrategia de la investigación como un todo.

Sanders & Pinhey (1983, p. 12) afirman que la metodología es el plan exacto y el procedimiento para llevar a cabo una investigación, mientras que los métodos son técnicas más específicas para ser usadas en el diseño de la investigación.

La investigación es una prueba de la teoría pero existe una reciprocidad cíclica entre teoría e investigación, puesto que la teoría señala los datos relevantes y los datos confirman o refutan la teoría.

Para llevar a efecto la investigación propuesta, se utilizará la proposición deductiva para explicar la relación entre teoría e investigación social, siguiendo la siguiente secuencia: teoría, hipótesis, colección de datos, resultados, hipótesis confirmadas o rechazadas y revisión de la teoría.

La presente investigación es descriptiva puesto que se proveerán respuestas a preguntas tales como: quién, qué, dónde, cuándo y cómo, que estén relacionadas al problema de investigación. Las respuestas serán encontradas en el análisis de datos secundarios, casos de estudio y en las opiniones de expertos.

Se investigarán las dificultades al acceso a la información, incluyendo las restricciones impuestas por políticas gubernamentales; las limitaciones a los contenidos a través de censuras gubernamentales y aquellas impuestas por la industria de Internet; restricciones a los derechos de los usuarios, tales como desconexiones legales o ilegales.

Se prestará atención especial a investigar el trabajo realizado por organizaciones no gubernamentales sobre mediciones de niveles de filtraje de Internet en diferentes países.

El método de investigación será mixto, pues se utilizará tanto el método cuantitativo no obstrusivo de análisis secundario de información estadística existente para evaluar el entorno mundial y el método cualitativo/cuantitativo Delphi. El método Delphi es una técnica cualitativa, es decir subjetiva, en la que los juicios de expertos se presentan en forma de evaluaciones cuantitativas; es decir que en el método Delphi se pasa del método cualitativo al cuantitativo porque se da objetividad a los criterios de los expertos al convertir la escala ordinal de las respuestas en escala de intervalo utilizando la escala de Linkert.

El método Delphi (deriva su nombre del antiguo oráculo de Delphos), se enmarca dentro de los métodos de prospectiva o predicción. Este método fue desarrollado por el proyecto RAND Corporation para la Fuerza Aérea de los Estados Unidos de Norteamérica, en los 1950s.

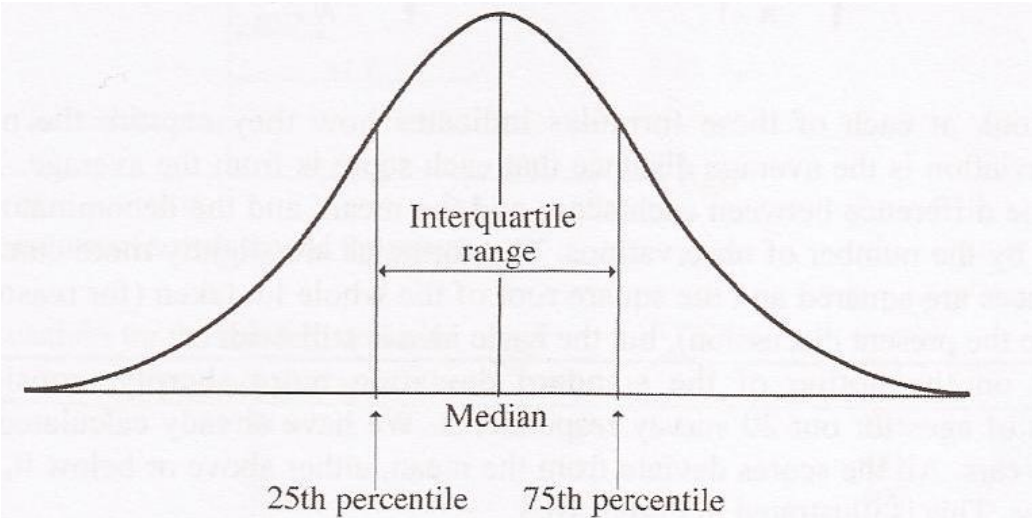
Martin (1996) sostiene que la prospectiva es "la tentativa sistemática de observar a largo plazo el futuro de la ciencia, la tecnología, la economía y la sociedad, con el propósito de identificar las áreas de investigación estratégica y las tecnologías genéricas emergentes que probablemente generen los mayores beneficios económicos y sociales". Los métodos de investigación orientados a la prospectiva, se pueden agrupar en tres tipos fundamentalmente: métodos de expertos (basado en las opiniones de conocedores del problema que se quiere analizar), métodos extrapolativos y métodos de correlación.

El método Delphi es un método de expertos definido como "un proceso sistemático e iterativo encaminado a la obtención de las opiniones, y si es posible el consenso, de un grupo de expertos" (Landeta, 1999).

Astirraga (2004, p. 63) opina que “la capacidad de predicción de la Delphi se basa en la utilización sistemática de un juicio intuitivo emitido por un grupo de expertos”.

El método Delphi procede por medio de la interrogación a expertos con la ayuda de cuestionarios sucesivos, a fin de poner de manifiesto convergencias de opiniones y deducir eventuales consensos. La encuesta se lleva a cabo de una manera anónima (actualmente es habitual realizarla haciendo uso del correo electrónico o mediante cuestionarios web establecidos al efecto) para evitar los efectos de "líderes". El objetivo de los cuestionarios sucesivos, es "disminuir el espacio intercuartil precisando la mediana" (Astirraga, 2004, p. 64).

El espacio o rango intercuartil es la diferencia entre los límites superiores del tercer cuartil (Q3) o percentil del 75% y del primer cuartil (Q1) o percentil del 25% de una distribución. La mediana corresponde al percentil del 50%. La Figura 2.2 ilustra el espacio o rango intercuartil.



Fuente: Argyrous G (2010, p. 137, Fig 10.1)

Figura 2.2: Rango intercuartil

Anderson et al. (1999, p. 206) describen el método Delphi manifestando que:

> *"Una de las técnicas de pronóstico cualitativo más usada es el método Delphi. Esta técnica elaborada inicialmente por un grupo de investigación en Rand Corporation, intenta elaborar pronósticos por medio del "consenso de grupo". En su aplicación común, a los miembros de un panel de expertos, que están separados físicamente y no se conocen entre sí, se les pide que respondan una serie de cuestionarios. Las respuestas del primer cuestionario se tabulan y emplean para preparar un segundo cuestionario que contiene información y opiniones del grupo entero. Luego se pide a cada uno de los que responden que reconsideren y revisen sus respuestas a la luz de la información de grupo proporcionada. Este proceso continúa hasta que el coordinador siente que se ha alcanzado algún grado de consenso. La meta del método Delphi no es producir una sola respuesta como salida, en su lugar, producir un despliegue de opiniones relativamente reducido dentro del cual coincida la mayoría de los expertos".*

En la técnica Delphi, el análisis de las respuestas de los expertos se lo realiza en forma estadística. En el presente estudio se utiliza para el efecto, el software SPSS.

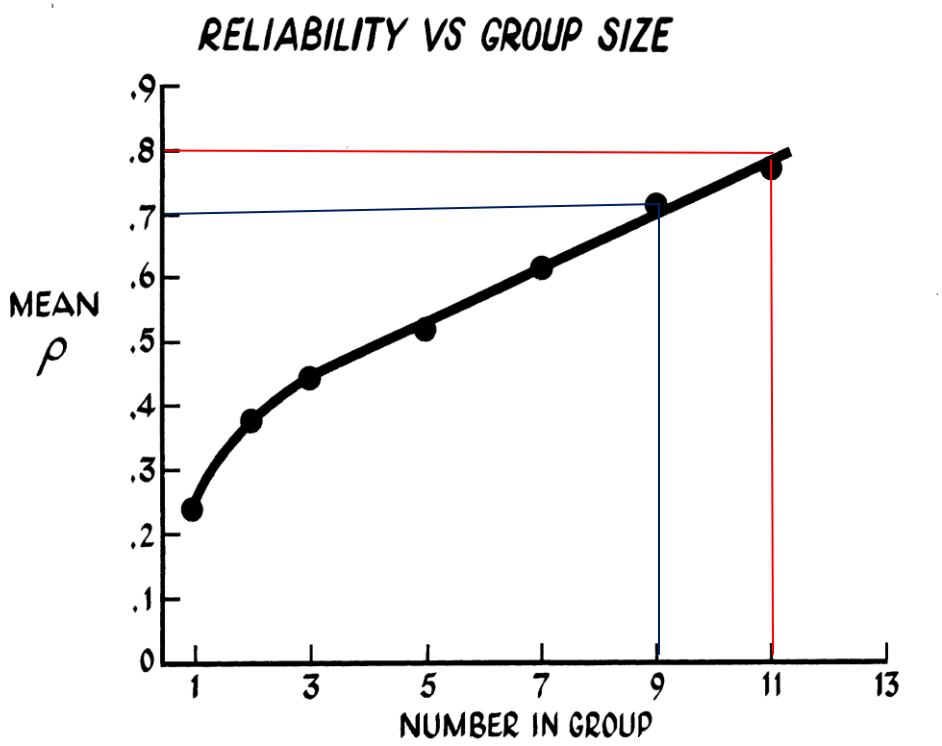
La confiabilidad es un tema central en una investigación y ayuda a establecer la credibilidad de los resultados. La confiabilidad significa consistencia.

Coakes et al. (2010, p.129) consideran que existen diferentes coeficientes de confiabilidad; uno de los más comúnmente usados es el Cronbach´s Alpha (ρ).

Pallant (2011, p. 6) opina que el coeficiente Cronbach's Alpha provee una indicación de la correlación promedio entre todos los ítems que hacen la escala. Su valor oscila entre 0 y 1, en que los valores más altos indican mayor confiabilidad.

Nunnally (1978, p. 230) recomienda un mínimo de 0.7 para el valor del coeficiente Cronbach's Alpha.

Dalkey (1969, p. 7) propone un gráfico (Figura 2.3) que muestra la confiabilidad promedio de una respuesta de grupo en dependencia del tamaño del grupo para el método Delphi.



Fuente: Dalkey N / Rand Corporation (1969, p. 13, Fig. 5) (las líneas en puntadas son mías)

Figura 2.3: Confiabilidad versus tamaño del grupo de expertos

Del análisis de la Figura 2.3 se puede establecer que con un grupo integrado por 9 expertos se alcanzará el valor mínimo del Coeficiente Cronbach's Alpha ($\rho = 0.7$) y con 11 miembros conformando el grupo se alcanzará un valor aceptable de 0.8.

Para la evaluación del cuestionario se utilizará la escala de Linkert con la siguiente valoración:

Fuertemente de acuerdo = 5

De acuerdo = 4

Neutral = 3

En desacuerdo = 2

Fuertemente en desacuerdo = 1

Capítulo 3

Marco teórico conceptual.

3.1. Sociedad de la Información.

El 8 de diciembre del 2000, la Asamblea General de la Organización de las Naciones Unidas (ONU) adoptó la resolución 55/2 titulada *La Declaración del Milenio*, mediante la cual se decidió reducir, hasta el año 2015, el porcentaje de habitantes en el mundo que sobreviven con menos de un dólar diario y el de las personas que padecen hambre. En la actualidad hay más de 1,400 millones de personas que viven en estas condiciones.

También se acordó que hasta el 2015, los niños y niñas de todo el mundo puedan terminar un ciclo completo de enseñanza primaria. Además haber reducido, para ese mismo año, la mortalidad materna en tres cuartas partes y la mortalidad de los niños menores de 5 años en dos terceras partes respecto de las tasas del 2000. Para entonces, haber detenido y comenzado a reducir la propagación del VIH/SIDA, el flagelo del paludismo y otras enfermedades graves que afligen a la humanidad.

Los 8 objetivos de la Declaración del Milenio son:

- Erradicar la pobreza extrema y el hambre
- Lograr la enseñanza primaria universal
- Promover la igualdad entre los géneros y la autonomía de la mujer
- Reducir la mortalidad infantil
- Mejorar la salud materna
- Combatir el VIH/SIDA, el paludismo y otras enfermedades
- Garantizar la sostenibilidad del medio ambiente

- Fomentar una alianza mundial para el desarrollo

En el año 2001, durante la Asamblea General de la ONU los gobernantes del mundo reconociendo la urgente necesidad de aprovechar las posibilidades del potencial del conocimiento y la tecnología para promover los objetivos de la Declaración del Milenio de las Naciones Unidas y encontrar medios eficaces e innovadores de poner éstas posibilidades al servicio de un desarrollo para todos.

Se acordó realizar la Cumbre de la Sociedad de la Información al más alto nivel posible en dos etapas: la primera en Ginebra, del 10 al 12 de diciembre de 2003, y la segunda en Túnez, en 2005. La ONU invitó a la Unión Internacional de Telecomunicaciones (UIT) a asumir la función administrativa principal de la secretaría ejecutiva de la Cumbre y su proceso preparatorio.

En la primera fase de la Cumbre Mundial de la Sociedad de la Información, se aprobó la Declaración de Principios titulada *Construir la Sociedad de la Información: un desafío global para el nuevo milenio,* en la que los gobiernos del mundo se pusieron de acuerdo en su visión común de una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo.

La CMSI definió en la Declaración de Principios a la Sociedad de la Información como aquella en la que "*todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos"*.

En la Declaración se reafirmó como fundamento esencial de la Sociedad de la Información, y según se estipula en el Artículo 19 de la Declaración Universal de Derechos Humanos, que:

> *"todo individuo tiene derecho a la libertad de opinión y de expresión, que este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir información y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. La comunicación es un proceso social fundamental, una necesidad humana básica y el fundamento de toda organización social. Constituye el eje central de la Sociedad de la Información. Todas las personas, en todas partes, deben tener la oportunidad de participar, y nadie debería quedar excluido de los beneficios que ofrece la Sociedad de la Información".* (Declaración de Principios de la CMSI)

Se reconoce en la Declaración de Principios que la educación, el conocimiento, la información y la comunicación son esenciales para el progreso, la iniciativa y el bienestar de los seres humanos y que las tecnologías de la información y las comunicaciones (TIC) tienen inmensas repercusiones en prácticamente todos los aspectos de nuestras vidas. El rápido progreso de estas tecnologías brinda oportunidades sin precedentes para alcanzar niveles más elevados de desarrollo. La capacidad de las TIC para reducir muchos obstáculos tradicionales, especialmente el tiempo y la distancia, posibilitan, por primera vez en la historia, el uso del potencial de estas tecnologías en beneficio de millones de personas en todo el mundo. Se señala también en esta declaración que la capacidad universal de acceder y contribuir a la información, las ideas y el conocimiento es un elemento indispensable en una Sociedad de la Información integradora y que es posible promover el intercambio y el fortalecimiento de los conocimientos mundiales en favor del desarrollo si se eliminan los obstáculos que impiden un acceso equitativo a la información para actividades económicas, sociales,

políticas, sanitarias, culturales, educativas y científicas, y si, de igual forma, se facilita el acceso a la información que está en el dominio público. Se agrega que, un dominio público abundante es un factor esencial del crecimiento de la Sociedad de la Información, ya que genera ventajas múltiples tales como un público instruido, nuevos empleos, innovación, oportunidades comerciales y el avance de las ciencias. Se manifiesta que los gobiernos deben esforzarse en promover el acceso universal, con las mismas oportunidades para todos, al conocimiento científico y la creación y divulgación de información científica y técnica, con inclusión de las iniciativas de acceso abierto para las publicaciones científicas.

En esta primera fase de la CMSI también se aprobó el Plan de Acción donde se establecieron nueve líneas de acción concretas (denominadas con letras C) para construir una Sociedad de la Información en un nivel nacional, regional e internacional. El Plan de Acción C3 titulado 'Acceso a la Información y al Conocimiento' sostiene que se debe alentar las iniciativas que faciliten el acceso por Internet, incluido el acceso gratuito y a precios asequibles, a las publicaciones periódicas y libros de acceso abierto, y a los archivos abiertos que contienen información científica. En el Plan de Acción C7 titulado 'Aplicaciones de las TIC: ventajas en todos los aspectos de la vida' se establece que es necesario promover una conexión a Internet asequible, fiable y de alta velocidad en todas las universidades e instituciones de investigación para apoyar su función crucial de producción de información y de conocimientos, educación y capacitación, y apoyar la creación de asociaciones, la cooperación y el intercambio entre estas instituciones; promover iniciativas de publicación electrónica, precios adaptados al mercado local y acceso abierto, a fin que la información científica sea asequible y accesible en todos los países, en condiciones equitativas, y, promover el uso de tecnología entre pares para compartir el conocimiento científico, los manuscritos y reediciones de documentos de autores científicos que han renunciado a la debida remuneración.

En la segunda fase de la CMSI realizada en Túnez, del 16 al 18 de noviembre del 2005, se aprobó la Agenda de Túnez para la Sociedad de la Información con el fin de pasar de los principios a la acción, en la cual se reconoció que la magnitud del problema vinculado al cierre de la brecha digital, necesitará durante muchos años inversiones adecuadas y duraderas en la infraestructura y los servicios de las TICs, así como en el fomento de capacidades y la transferencia de tecnología. Efectivamente, la implementación de la Sociedad de la Información ofrece oportunidades sin precedentes para todos; pero además genera enormes disparidades entre poblaciones y países. La desigual distribución global de las TICs ha creado una división digital conocida como la *brecha digital* que separa individuos y naciones mediante la accesibilidad selectiva a equipos de TICs y servicios.

Villao (2012, p. 12) manifiesta, respecto a la división digital, que hoy en día una nueva forma de brecha digital está surgiendo en términos de diferencia en calidad y velocidad de acceso a las TICs, conocida como la brecha de la banda ancha.

La Agenda de Túnez para la Sociedad de la Información le dedica especial atención a la Gobernanza de Internet, reafirmando los principios enunciados en la primera fase de la CMSI, en el sentido de que:

> *"Internet se ha convertido en un recurso mundial disponible para el público y su gobernanza debería constituir un elemento esencial de la agenda de la Sociedad de la Información. La gestión internacional de Internet debería ser multilateral, transparente y democrática, y hacerse con la plena participación de los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales. Esta gestión debería garantizar una distribución equitativa de los recursos, facilitar el acceso de todos y garantizar un funcionamiento estable y seguro de Internet, tomando en consideración el multilingüismo".*

En la misma Agenda los gobernantes del mundo solicitaron al secretario general de las Naciones Unidas, Ban Ki-moon, la creación del foro para la Gobernanza de Internet - IGF, al que se referirá más adelante, con mandato para debatir temas de políticas públicas relativos a la sostenibilidad, la solidez, la seguridad, la estabilidad y el desarrollo de Internet. Hasta la presente fecha se han realizado siete foros para la Gobernanza de Internet; en Atenas, Grecia (2006), Río de Janeiro, Brasil (2007), Hyderabad, India (2008), Sharm El Sheikh, Egipto (2009), Vilnius, Lituania (2010), Nairobi, Kenia (2011) y Baku, Azerbaijan (2012).

Se puede concluir que los gobiernos de los países del mundo se encuentran comprometidos a implementar la Sociedad de la Información, la misma que tiene como fundamento esencial, según se estipula en el Artículo 19 de la Declaración Universal de Derechos Humanos, el respeto al derecho a la libertad de opinión y de expresión que tienen todos los individuos. Se reconoce que para la construcción de una Sociedad de la Información incluyente es fundamental mejorar el acceso a las tecnologías de la información y la comunicación. Internet permite disfrutar a todas las personas de los beneficios de esta nueva sociedad.

3.2. Libertad de expresión: fundamentación en los derechos humanos. Libertad de información. Libertad de conexión.

La libertad de expresión está consagrada en la Declaración Universal de los Derechos Humanos adoptada y proclamada por la Resolución de la Asamblea General de las Naciones Unidas 217 A (iii) del 10 de diciembre de 1948 en cuyo Artículo 19 proclama que:

> *"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar*

y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

De igual forma, el Convenio Internacional sobre los Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de las Naciones Unidas en su Resolución 2200A (XXI) del 16 de diciembre de 1966 y que entró en vigor el 23 de marzo de 1976, en el Artículo 19 señala que:

"1. Nadie podrá ser molestado a causa de sus opiniones.

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;

b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas".

Una de las funciones de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) es precisamente fomentar:

"el conocimiento y la comprensión mutuos de las naciones prestando su concurso a los órganos de información para las masas; a este fin, recomendará los acuerdos internacionales que estime convenientes para facilitar la libre circulación de las ideas por medio de la palabra y de la imagen".

La Convención Americana sobre Derechos Humanos suscrita en la Conferencia especializada Interamericana sobre Derechos Humanos realizada en San José, Costa Rica, del 7 al 22 de noviembre de 1969, también proclama en su Artículo 13 el derecho a la libertad de pensamiento y de expresión, al expresar que:

> *"1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.*
>
> *2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:*
>
> *a) el respeto a los derechos o a la reputación de los demás, o*
>
> *b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.*
>
> *3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones".*

La estructura internacional de los derechos humanos provista por los instrumentos jurídicos antes citados se aplica a la comunicación sobre Internet, de igual forma que se aplica a otras formas de comunicación.

El Art. 33 de la Constitución de la Unión Internacional de Telecomunicaciones (UIT), reformado en la Conferencia de Plenipotenciarios de Minneapolis en 1998, titulado

Derecho del público a utilizar el Servicio Internacional de Telecomunicaciones, dispone que los Estados Miembros reconocen al público el derecho a comunicarse por medio del servicio internacional de correspondencia pública.

Los participantes en la Conferencia patrocinada por la UNESCO en el Día Mundial de la Libertad de Prensa, reunidos en Dakar (Senegal), del 1 al 3 de mayo de 2005, adoptaron la Declaración de Dakar titulada "Medios de comunicación y buen gobierno" en la que se insta a los Estados Miembros a:

> *"Velar porque en sus actividades los organismos estatales respeten los principios de transparencia, rendición de cuentas y acceso público a la información;*
> *Respetar la función de los medios de información como factor esencial del buen gobierno, fundamental para reforzar la transparencia y la rendición de cuentas en los procesos de toma de decisiones, y a transmitir los principios de buen gobierno a los ciudadanos;*
> *Tomar medidas para acabar con los asesinatos, los ataques, el acoso, la detención y la encarcelación de periodistas, los que investigan sobre casos de corrupción, a hacer todo lo posible para llevar a los responsables ante la justicia;*
> *Garantizar el derecho de los periodistas a proteger sus fuentes confidenciales de información".*

De igual forma, mediante esta Declaración se instó a la UNESCO a sensibilizar a los gobiernos, los legisladores y las instituciones públicas sobre la importancia de la libertad de expresión, en particular la libertad de tener acceso a la información, así como de producirla y compartirla.

Es oportuno mencionar que el 14 de febrero del 2006 la Sra. Condoleezza Rice, en ese entonces Secretaria de Estado de los Estados Unidos de Norteamérica, estableció el Grupo de Trabajo de la Libertad Mundial en Internet (Global Internet Freedom Task Force) como un grupo interno del Departamento de Estado para dirigir los desafíos que presenta la libertad de expresión y el libre flujo de información en Internet alrededor del mundo. Los objetivos de este Grupo son: maximizar la libertad de expresión y el libre flujo de información e ideas, minimizar los casos de regímenes represivos en la censura y en silenciar el debate legítimo y promover el acceso a la información e ideas sobre Internet.

Los participantes en la Conferencia patrocinada por la UNESCO en el Día Mundial de la Libertad de Prensa, reunidos en Maputo, Mozambique, adoptaron el 3 de mayo del 2008, la Declaración de Maputo titulada "Libertad de Expresión, Acceso a la Información y Empoderamiento de las Personas", en la que se insta a los Estados Miembros a fortalecer un entorno en el cual las nuevas tecnologías de la información sean utilizadas para disminuir la brecha digital y del conocimiento en los países en desarrollo y para proveer una pluralidad de opciones de medios y acceso a las noticias; de igual forma evitar medidas que dificulten la libertad de expresión, y particularmente la censura de los sitios Web.

La necesidad de respetar la libertad de expresión en línea también está expresada en la Declaración de Brisbane titulada "Libertad de Expresión: El Derecho a Saber" adoptada igualmente durante la conmemoración anual de la UNESCO del Día Mundial de la Libertad de Prensa, el 3 de mayo del 2010 en Brisbane, Australia. En esta Declaración se pide a los Estados Miembros de la UNESCO que aprovechen las capacidades de las tecnologías de la información y la comunicación para poner en práctica el derecho a la información y fomentar un mayor pluralismo en la circulación de la información; reduzcan la brecha digital y del conocimiento, elevando los bajos niveles de

alfabetización y de conectividad a Internet, y proporcionando la información disponible en lenguas locales y en formas fácilmente comprensibles para distintos públicos; de igual manera se pide a la UNESCO que promueva la libre circulación de la información y las ideas en Internet, y condene la censura y otras violaciones de la libertad de expresión en esa Red.

El Relator Especial de Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, Frank La Rue; la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) de la Organización de Estados Americanos (OEA), Catalina Botero Marino; la Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) para la Libertad de los Medios de Comunicación, Dunja Mijatović; y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), Faith Pansy Tlakula; emitieron el 1 de junio del 2011 una Declaración Conjunta en la que establecen lineamientos para proteger la libertad de expresión en Internet. En esta Declaración se adopta como uno de los principios generales, que la libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad.

Con respecto a la responsabilidad de intermediarios, se manifiesta en la Declaración Conjunta que ninguna persona que ofrezca únicamente servicios técnicos de Internet como acceso, búsquedas o conservación de información en la memoria caché deberá ser responsable por contenidos generados por terceros y que se difundan a través de estos servicios, siempre que no intervenga específicamente en dichos contenidos ni se niegue

a cumplir una orden judicial que exija su eliminación cuando esté en condiciones de hacerlo ("principio de mera transmisión"). Se agrega que no se debería exigir a los intermediarios que controlen el contenido generado por usuarios y no deberían estar sujetos a normas extrajudiciales sobre cancelación de contenidos que no ofrezcan suficiente protección para la libertad de expresión.

En lo relacionado al bloqueo obligatorio de sitios web enteros, direcciones IP, puertos, protocolos de red o ciertos tipos de usos (como las redes sociales), la Declaración lo considera una medida extrema—análoga a la prohibición de un periódico o una emisora de radio o televisión— que solo podría estar justificada conforme a estándares internacionales, por ejemplo, cuando sea necesaria para proteger a menores del abuso sexual. Los sistemas de filtrado de contenidos impuestos por gobiernos o proveedores de servicios comerciales que no sean controlados por el usuario final constituyen una forma de censura previa y no representan una restricción justificada a la libertad de expresión. Se debe exigir que los productos destinados a facilitar el filtrado por los usuarios finales estén acompañados por información clara dirigida a dichos usuarios acerca del modo en que funcionan y las posibles desventajas si el filtrado resulta excesivo.

En lo que se refiere al acceso a Internet, se expresa en la Declaración que los Estados tienen la obligación de promover el acceso universal a Internet para garantizar el disfrute efectivo del derecho a la libertad de expresión. El acceso a Internet también es necesario para asegurar el respeto de otros derechos, como el derecho a la educación, la atención de la salud y el trabajo, el derecho de reunión y asociación, y el derecho a elecciones libres. La interrupción del acceso a Internet, o a parte de este, aplicada a poblaciones enteras o a determinados segmentos del público (cancelación de Internet) no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional. Lo mismo se aplica a las medidas de reducción de la velocidad de navegación de Internet o de partes de éste. La negación del derecho de acceso a Internet, a modo de

sanción, constituye una medida extrema que solo podría estar justificada cuando no existan otras medidas menos restrictivas y siempre que haya sido ordenada por la justicia, teniendo en cuenta su impacto para el ejercicio de los derechos humanos.

El Secretario General de la ONU, Ban Ki-moon, en su Informe A/66/290 presentado a la Asamblea General el 10 de agosto del 2011 sobre la "Promoción y protección del derecho a la libertad de opinión y de expresión", reconoció que Internet se ha convertido en un medio de comunicación vital para que las personas puedan ejercer su derecho a la libertad de expresión o el derecho de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, como se garantiza en los artículos 19 de la Declaración Universal de Derechos Humanos y del Convenio o Pacto Internacional de Derechos Civiles y Políticos. Agregó que Internet, a diferencia de cualquier otro medio de comunicación anterior, permite a las personas comunicarse instantáneamente y a bajo costo, y sus repercusiones en el intercambio y el acceso a la información y a las ideas, y en el propio periodismo, son impresionantes.

En la celebración del Día Mundial de la Libertad de Prensa, en el año 2012, realizada en Cartago, Túnez, cuna de la primavera árabe, se adoptó la Declaración de Cartago mediante la cual los participantes pidieron a todos los Estados Miembros de la UNESCO, reafirmen y cumplan con sus obligaciones de cumplimiento con los estándares internacionales en materia de libertad de expresión, incluyendo el Artículo 19 de la Declaración Universal de los Derechos Humanos, y reconozcan la importancia de este derecho para la participación ciudadana en todas las manifestaciones mediáticas, en el desarrollo de las sociedades y particularmente en la transformación hacia sistemas democráticos; desarrollen e implementen políticas que promuevan la pluralidad de los medios de comunicación y que impidan concentraciones en manos de un solo propietario, al mismo tiempo que apoyen el acceso equitativo a los medios y la lucha contra las brechas digitales; provean sistemas independientes de investigación judicial

en los casos de violaciones y asesinatos de periodistas e informen al Director General de la UNESCO sobre la seguridad de los periodistas y la cuestión de la impunidad.

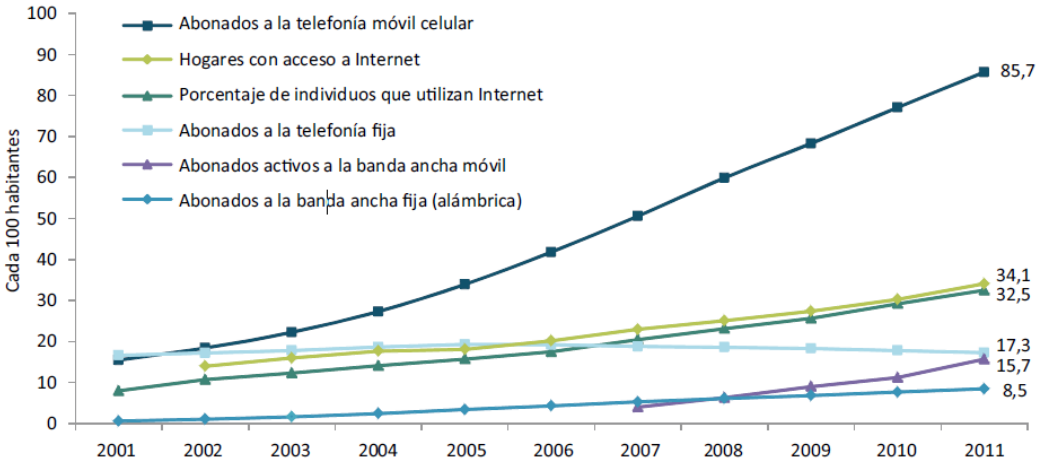
Cabe mencionar que durante la realización de la Conferencia Mundial de Telecomunicaciones Internacionales (CTMI) de la UIT, realizada en Dubai, Emiratos Árabes Unidos, del 3 al 14 de diciembre del 2012, en una propuesta presentada por la delegación de Túnez, se solicitó a la conferencia que incluyera un nuevo texto para el Artículo 1 del Reglamento de las Telecomunicaciones Internacionales a fin de proteger específicamente la libertad de expresión, señalando que "las personas deben tener los mismos derechos en línea que en el mundo físico". Asimismo, se exhortaba a los Estados Miembros a proteger el derecho al "acceso a toda divulgación de información por medio de las telecomunicaciones/TICs en el ejercicio de este derecho, así como el derecho a la libertad de reunión y de asociación pacíficas en línea". Túnez subrayó que consideraba CMTI-12 debería enviar un mensaje claro sobre la necesidad de proteger el derecho a la libertad de expresión. La conferencia resolvió que no era necesario añadir texto adicional a un tratado tan técnico, habida cuenta de que el derecho a la libertad de expresión ya está expresamente protegido en distintos tratados que, desde un punto de vista jurídico, tienen jerarquía sobre el Reglamento de Telecomunicaciones Internacionales, en particular en el Artículo 19 de la Declaración Universal de Derechos Humanos, el Artículo 19 del Convenio Internacional de Derechos Civiles y Políticos y en el Artículo 33 de la propia Constitución de la UIT.

Se concluye categóricamente que la comunidad internacional reconoce que también se aplica a Internet, la libertad de expresión garantizada por la normativa internacional de los derechos humanos. En muchos Estados, el derecho a la libertad de expresión está fortalecido por la libertad de información, lo cual dota a los ciudadanos de un derecho legal a requerir y accesar a la información a cargo de los gobiernos. Las libertades de expresión e información deben ser vistas como un derecho fundamental, en un gran

contexto de valores competitivos e intereses. De acuerdo con la UNESCO, la libertad de información puede definirse como el derecho a tener acceso a la información que está en manos de entidades públicas.

3.3. Las redes sociales.

De acuerdo con el informe de la UIT (2012) "Medición de la Sociedad de la Información", a finales del año 2011 el número de abonados a nivel mundial del servicio móvil celular fue de alrededor de 6 mil millones, es decir alcanzó una penetración del 85.7%; el número de abonados a la banda ancha fija aumentó a casi 600 millones, que corresponde a una tasa de penetración mundial del 8.5%; el número de abonados a la banda ancha móvil aumentó a casi 1.100 millones, que corresponde a una tasa de penetración mundial del 15.7%, es decir prácticamente duplica a los abonados a la banda ancha fija; y, el número de personas con acceso a Internet superó los 2.300 millones equivalente al 32.5% de la población mundial. La Figura 3.1 muestra la evolución de las TICs en el período 2001-2011 donde se pueden apreciar los porcentajes antes citados.



Fuente: UIT Medición de la Sociedad de la Información 2012

Figura 3.1: Desarrollo mundial de las TICs, período 2001-2011

El “milagro” de la telefonía móvil ha hecho posible que un tercio de los habitantes del mundo están conectados a Internet.

El informe de la UIT “Medición de la Sociedad de la Información” (2011) manifiesta que algunos acontecimientos ocurridos recientemente, como los relacionados con la primavera árabe y la publicación de información política confidencial en Internet, han demostrado el poder de la comunicación y la conexión, y han hecho aumentar enormemente el interés político en la sociedad de la información. Efectivamente, los sucesos ocurridos en el medio oriente en el 2011 han demostrado que Internet se ha convertido en un medio crucial por el cual los ciudadanos pueden movilizar y defender reformas políticas, sociales y económicas.

La UNESCO ha participado activamente desde el año 2006 en los Foros para la Gobernanza de Internet. Es así que dentro del marco del quinto Foro para la Gobernanza de Internet (FGI) celebrado en Vilna, Lituania (2010), organizó el Taller de la UNESCO sobre la vida privada y las redes sociales, donde los participantes afirmaron que “la popularidad creciente de las redes sociales en Internet trae consigo nuevos desafíos en términos de protección de la vida privada y libertad de expresión”. Los panelistas de dicho Taller señalaron que, las redes sociales han originado nuevas relaciones, en cuanto al intercambio de datos personales entre usuarios.

Es oportuno en este punto definir qué son los medios sociales y las redes sociales. Kaplan and Haenlein (2010, ps. 60 - 61) sostienen que la creciente disponibilidad de acceso a Internet de alta velocidad sumada a su popularidad, dio lugar a la creación de sitios de redes sociales como MySpace (en 2003) y Facebook (en 2004). Esto, a su vez, acuñó el término “medios sociales", y ha contribuido a la importancia que tiene hoy.

Estos autores afirman que una definición formal de “Medios Sociales” requiere primero trazar una línea a dos conceptos relacionados que son frecuentemente nombrados en conjunto con dicha denominación: la Web 2.0 y el Contenido Generado por el Usuario. Agregan que la Web 2.0 es un término que fue usado por primera vez en el año 2004 y que describe una nueva forma en la cual los desarrolladores de softwares y los usuarios finales comenzaron a utilizar la World Wide Web; esto es, como una plataforma por medio de la cual el contenido y las aplicaciones ya no creados y publicados por los individuos, sino que se modifica continuamente por todos los usuarios de una manera participativa y colaborativa.

Kaplan and Haenlein consideran a la Web 2.0 como la plataforma para la evolución de los Medios Sociales. Afirman que mientras la Web 2.0 representa el fundamento ideológico y tecnológico, el Contenido Generado por el Usuario (CGU) puede ser visto como la suma de todas las formas en la cual las personas hacen uso de los Medios Sociales. Basados en las aclaraciones efectuadas entre la Web 2.0 y el CGU, sostienen los autores que ahora es más sencillo dar una definición de lo que son las Redes Sociales. Medio Social es un grupo de aplicaciones basadas en Internet que se desarrollan sobre los fundamentos ideológicos y tecnológicos de la Web 2.0, y que permiten la creación y el intercambio de Contenidos Generados por el Usuario. Dentro de esta definición general, hay varios tipos de Medios Sociales que necesitan ser diferenciados mayormente. Sin embargo, a pesar de que la mayoría de las personas probablemente están de acuerdo que Wikipedia, YouTube, Facebook y Second Life son todos ellos parte de este gran grupo, no existe una forma sistemática en la cual las aplicaciones de los diferentes Medios Sociales puedan ser categorizadas.

Kaplan and Haenlein (2010, p. 63) definen a los sitios de “redes sociales” como aplicaciones que permiten a los usuarios conectarse mediante la creación de perfiles de información personal, invitar a amigos y colegas a tener acceso a esos perfiles, y enviar

correos electrónicos y mensajes instantáneos entre cada uno de ellos. Estos perfiles personales pueden incluir cualquier tipo de información, incluyendo fotos, videos, archivos de audio y blogs. Algunas de estas aplicaciones son: MySpace, Facebook, YouTube, Second Life, Twitter, LinkedIn y Flickr.

Hoy las redes sociales, como Facebook y Twitter, son portadoras de nuevas formas de interacción social, de diálogo, intercambio y colaboración. Los sitios de interconexión social (llamados, en un sentido más amplio, medios sociales) facilitan a los usuarios la comunicación de ideas, así como actualizaciones y comentarios o la participación en diversas actividades, compartiendo con sus interlocutores sus intereses comunes. De simples pláticas amistosas a la propagación de noticias de actualidad, de una cita al seguimiento de los resultados electorales o la coordinación de las respuestas en caso de catástrofes, del humor sano a las investigaciones serias, las redes sociales se usan hoy para los fines más diversos, en el marco de diferentes comunidades de usuarios. (UIT News, No.6, 2010).

Shashi Tharoor, ex Subsecretario de las Naciones Unidas para Comunicaciones e Información Pública, ex candidato a Secretario General de la ONU y ex Ministro de Estado en la India, durante la charla que dio en la UNESCO sobre Comunicación y Redes Sociales el 7 de junio de 2011 afirmó que "es indudable que las redes sociales dieron un mayor impulso a la primavera árabe". Agregó que está convencido de que las redes sociales tendrán un papel cada vez más importante en las relaciones internacionales en los próximos años, y sentenció: "Las redes sociales han llegado para quedarse, hay que vivir con ellas, así que es mejor sacarles el máximo provecho".

Durante el Sexto Foro de la Gobernanza de Internet realizado en Nairobi, Kenia, en el año 2011, la UNESCO organizó el Taller titulado "Flujo Libre de Información y las Redes Sociales: un Rol para la Democracia y la Participación Social". Este Taller

discutió el rol importante de las redes sociales en promover la democracia y la participación social y exploró la manera de fortalecer este rol al fomentar el libre flujo de información por Internet. Se reconoció que en los recientes movimientos sociales, las redes sociales han llegado a ser las herramientas de comunicación masivas y vehículos para movilización. Se manifestó que la apropiación social de Internet está llegando a ser una parte importante de los procesos de democratización. Sitios web tales como Facebook y Twitter están siendo usados ampliamente por activistas y ciudadanos para transmitir información que no siempre es accesible a través de los medios de comunicación tradicionales, y también para evitar la censura.

Facebook y Twitter han anunciado que tienen en la actualidad más de 1.000 millones y 100 millones, respectivamente, de usuarios activos alrededor del mundo.

3.4. Tecnologías de la desconexión.

El Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, presentado al Consejo de Derechos Humanos de la Asamblea General de la ONU el 16 de mayo del 2011, expresa que la reciente oleada de manifestaciones en países de la región de Oriente Medio y África Septentrional ha demostrado la función esencial que puede cumplir Internet en la movilización de la población para pedir justicia, igualdad, rendición de cuentas y un mayor respeto de los derechos humanos. En este sentido, agrega La Rue, para los Estados debería ser prioritario facilitar el acceso de toda la población a Internet con las mínimas restricciones posibles del contenido en línea.

La Rue opina que como se establece en el párrafo 3 del artículo 19 del Convenio Internacional de Derechos Civiles y Políticos al que nos referimos en el numeral 3.2 de la presente tesis, existen excepcionalmente determinados tipos de expresión que pueden restringirse legítimamente de conformidad con el derecho internacional de los derechos

humanos, fundamentalmente para salvaguardar los derechos de otras personas. Toda limitación del derecho a la libertad de expresión debe superar la siguiente prueba acumulativa tripartita:

> a) Debe estar prevista por ley de manera clara y accesible para todos (principios de previsibilidad y transparencia);
> b) Debe obedecer a uno de los fines establecidos en el párrafo 3 del artículo 19 del Convenio, que son: i) asegurar el respeto a los derechos o a la reputación de los demás, o ii) proteger la seguridad nacional, el orden público o la salud o la moral públicas (principio de legitimidad); y
> c) Debe probarse ser necesaria y ser el medio menos restrictivo requerido para lograr el objetivo previsto (principios de necesidad y proporcionalidad).

En este sentido, agrega el informe del Relator La Rue, entre los tipos legítimos de información que pueden restringirse cabe mencionar la pornografía infantil (para proteger los derechos del niño), la incitación verbal al odio (para proteger los derechos de las comunidades afectadas), la difamación (para proteger los derechos y la reputación de los demás contra ataques injustificados), la incitación directa y pública a cometer actos de genocidio (para proteger los derechos de los demás) y el fomento del odio nacional, racial o religioso que constituya incitación a la discriminación, hostilidad o violencia (para proteger los derechos de los demás, como el derecho a la vida). Sin embargo, puntualiza el Relator, en muchos casos los Estados restringen, controlan, manipulan y censuran contenidos difundidos por Internet, sin fundamento jurídico o amparándose en leyes amplias y ambiguas, sin justificar el objeto de esas acciones o de una manera claramente innecesaria o desproporcionada para el logro del objetivo previsto. Esas acciones son claramente incompatibles con las obligaciones contraídas por los Estados en virtud del derecho internacional de los derechos humanos y a menudo

crean un "efecto inhibidor" más amplio del derecho a la libertad de opinión y de expresión.

Se manifiesta en el informe al que estamos haciendo referencia, que el uso estatal de tecnologías de bloqueo o filtrado incumple con frecuencia su obligación de garantizar el derecho a la libertad de expresión y que las restricciones del derecho de las personas a expresarse por Internet pueden adoptar diversas formas, desde medidas técnicas para impedir el acceso a determinados contenidos, como bloqueos y filtros, hasta garantías inadecuadas del derecho a la intimidad y la protección de los datos personales, lo cual coarta la difusión de opiniones e información. El Relator Especial considera que el uso arbitrario del derecho penal para sancionar las expresiones legítimas constituye una de las formas más graves de restricción del derecho, pues no solo genera un "efecto inhibidor" sino que también da acceso a otras violaciones de los derechos humanos, como detenciones arbitrarias y torturas y otros tratos o penas crueles, inhumanos o degradantes.

Se entiende por bloqueo toda medida adoptada para impedir que determinados contenidos lleguen a un usuario final, como por ejemplo impedir a los usuarios el acceso a determinados sitios web, direcciones del Protocolo Internet (IP) o extensiones de nombres de dominio, eliminar sitios web del servidor de web en los que están alojados o usar tecnologías de filtrado para que no aparezcan páginas que contengan determinadas palabras clave u otro contenido concreto. Por ejemplo, varios países siguen bloqueando el acceso a YouTube. China, que dispone de uno de los sistemas más amplios y avanzados de control de la información en Internet, ha adoptado numerosos sistemas de filtrado que bloquean el acceso a sitios web donde aparecen vocablos clave como "democracia" y "derechos humanos". Es motivo de honda preocupación para el Relator Especial el hecho de que se empleen mecanismos cada vez más avanzados para regular y

censurar la información, mediante controles en niveles múltiples que a menudo se ocultan al público.

Preocupa también al Relator Especial la tendencia en auge de los bloqueos programados ("en momentos precisos"), que impiden a los usuarios acceder a información o difundirla en coyunturas políticas importantes, como elecciones, épocas de descontento social o aniversarios de acontecimientos de relevancia política o histórica. Es así que se bloquean los sitios web de los partidos de la oposición, los medios de comunicación independientes y las redes sociales como Twitter y Facebook, como se observó en el contexto de las recientes protestas en la región de Oriente Medio y África Septentrional. En Egipto, los usuarios de Internet quedaron completamente desconectados, se expresa en el informe del Relator.

Denuncia el Relator La Rue en su informe, que los tipos de actuaciones con las que los Estados pretenden limitar la difusión de contenidos en línea no solo consisten en medidas encaminadas a impedir que la información llegue a su usuario final, sino también en medidas dirigidas concretamente a quienes buscan, reciben y difunden por Internet información políticamente delicada. El silenciamiento físico de las críticas o disensiones mediante detenciones y reclusiones arbitrarias, desapariciones forzadas, acosos e intimidaciones es un fenómeno antiguo que también se aplica a los usuarios de Internet. El Relator Especial manifiesta su preocupación por la tipificación como delito de la expresión legítima en línea, que contraviene las obligaciones internacionales de los Estados en materia de derechos humanos mediante la aplicación de la legislación penal vigente a la expresión en línea o mediante la creación de nueva legislación que tiene por objeto tipificar como delito la expresión por Internet. Un ejemplo claro de tipificación como delito de la expresión legítima de opiniones es el encarcelamiento de autores de blogs en todo el mundo. Según Reporteros sin Fronteras (Reporters without Borders), en 2010 estaban encarcelados 109 autores de blogs por cargos relacionados con el

contenido de su expresión en línea. Solo en China había 72 personas encarceladas, tras de lo cual seguía Viet Nam (17 personas) e Irán (13).

Se comenta además en el informe citado que una de las características singulares de Internet es que la manera en que se transmite la información depende en gran medida de los intermediarios, sociedades privadas que ofrecen servicios y plataformas para facilitar la comunicación en línea o transacciones entre terceros, lo cual incluye el acceso, el alojamiento, la transmisión y la indexación de contenidos. Así pues, son intermediarios desde los proveedores de servicios de Internet (ISPs) a los motores de búsqueda, y desde los servicios de blogs a las plataformas de comunidades en línea. Desde la aparición de los servicios Web 2.0 se puede publicar información sin el control centralizado de revisión editorial característico de los formatos de publicación tradicionales. Muchos Estados han aprobado leyes que hacen responsables a los intermediarios si no filtran, eliminan o bloquean contenidos generados por usuarios que se consideran ilegales. En otros casos, la responsabilidad de los intermediarios se establece mediante leyes de protección de la intimidad y los datos.

Se puede distinguir en el informe analizado, las diferentes tecnologías de desconexión que utilizan los Estados para restringir la libertad de expresión en Internet. Esta temática también es preocupación de varios organismos internacionales y de organismos no gubernamentales.

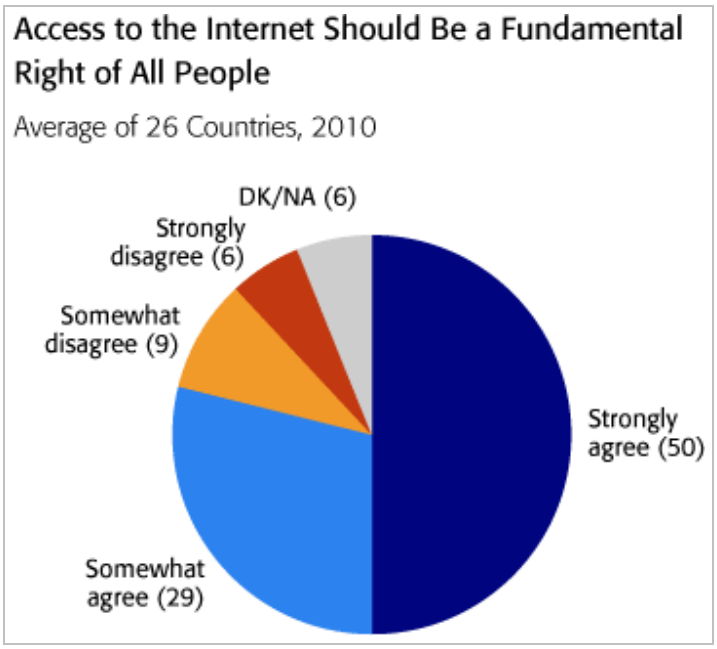
3.5. Opinión pública respecto a la libertad en internet.

Entidades no gubernamentales han realizado estudios para medir la opinión pública sobre creencias y actitudes concernientes a la libertad en Internet.

Uno de estos estudios es el realizado por BBC World Service en el año 2010, donde fueron encuestados 26 países, que permite establecer que casi 4 de 5 personas alrededor del mundo creen que el acceso a Internet es un derecho fundamental.

La muestra de la encuesta que fue encargada a GlobeScan fue de 27.973 personas adultas, incluyendo 14.306 usuarios de Internet, habiendo encontrado que el 87% de los que usaban Internet sentían que el acceso a Internet debería ser "derecho fundamental de todas las personas". El 71% de quienes no eran usuarios de Internet también sentían que ellos deberían tener el derecho de acceder a la web.

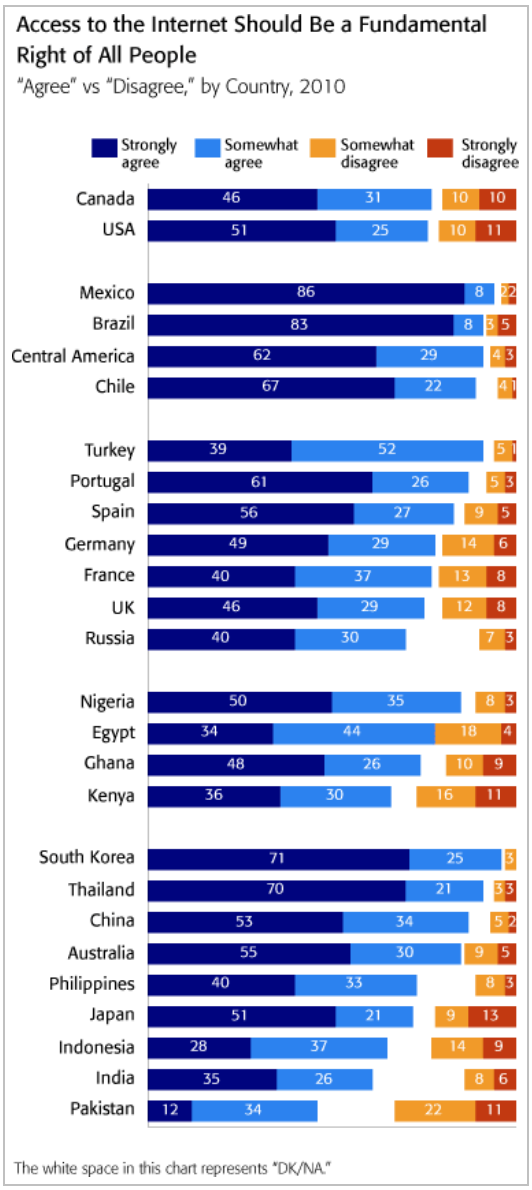
En la Figura 3.2 se muestra el porcentaje global de todos los 26 países encuestados, dando como resultado que el 79% estaban de acuerdo en que Internet debe ser un derecho fundamental de todas las personas ("fuertemente de acuerdo: 50%, "algo de acuerdo: 29%); 9% estaban "algo en desacuerdo" y 6% "fuertemente en desacuerdo". "DK/NA" ("Don't Know/No Answer") alcanzó el 6%. Los países con muy alta proporción respecto que estuvieron "fuertemente de acuerdo" y "algo de acuerdo" con el anterior enunciado fueron Corea del Sur (96%), México (94%) y China (87%).



Fuente: BBC World Service/GlobeScan (2010)

Figura 3.2: Porcentaje promedio en 26 países encuestados respecto a la declaración de que si Internet debe ser un derecho fundamental de todas las personas

En la Figura 3.3 se muestra el gráfico por países del porcentaje de usuarios de Internet que están "fuertemente de acuerdo", "algo de acuerdo", "algo en desacuerdo" y "totalmente en desacuerdo" con la declaración de que el "Acceso a Internet debe ser un derecho fundamental de todas las personas".

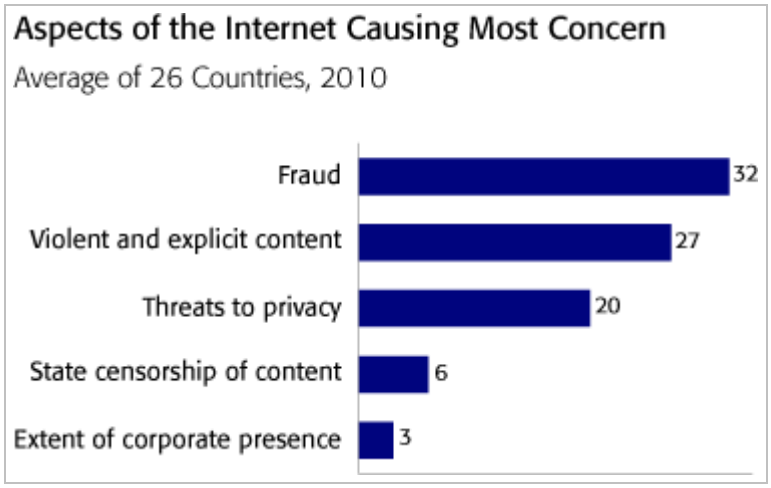


Fuente: BBC World Service/GlobeScan (2010)

Figura 3.3: Porcentaje por países respecto a la declaración Internet debe ser un derecho fundamental de todos los países

La encuesta también encontró que el fraude fue el aspecto de Internet que más preocupaba a las personas, con un 32%. El fraude emergió como la mayor preocupación pública superando a la violencia y los contenidos explícitos (27%), a la amenaza a la

privacidad (20%) y a la censura estatal de contenidos (6%). La Figura 3.4 muestra los aspectos de Internet que causan mayor preocupación a las personas.



Fuente: BBC World Service/GlobeScan (2010)

Figura 3.4: Aspectos de Internet que causan mayor preocupación a las personas

Podemos concluir que existe un consenso en la opinión pública mundial de que la libertad en Internet debe ser un derecho fundamental de las personas y que la mayor preocupación de los usuarios es el riesgo de fraude que pueden sufrir en la red.

Capítulo 4

Protecciones legales y regulatorias de los derechos digitales.

4.1. Censura: filtraje de internet.

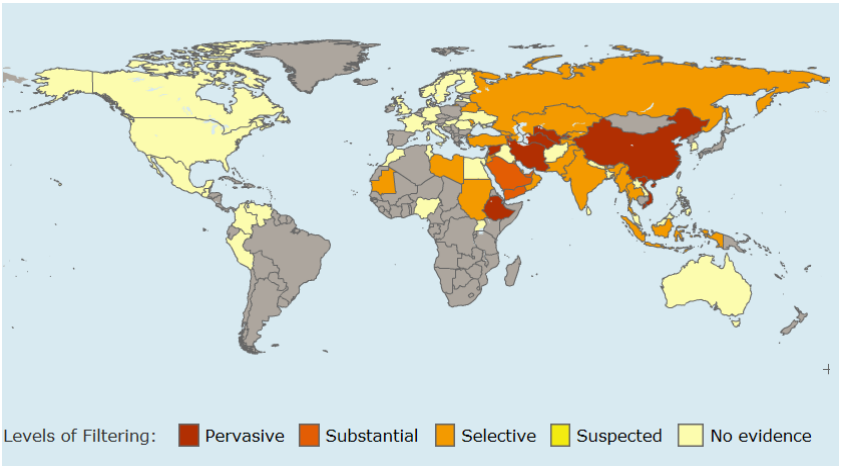
Existen organizaciones no gubernamentales, fundaciones, grupos de investigación y alianzas, que se dedican ha efectuar mediciones del filtraje de Internet que practican algunos Estados.

OpenNet Initiative (ONI) es una asociación de colaboración de tres instituciones: el Citizen Lab de la Escuela Munk de Asuntos Globales de la Universidad de Toronto, el Centro Berkman para Internet y Sociedad de la Universidad de Harvard, y el Grupo SecDev (Ottawa). El objetivo de ONI es investigar, exponer y analizar el filtrado de Internet y las prácticas de vigilancia de una manera creíble y no partidista. Para el efecto desarrolla y despliega un conjunto de herramientas de enumeración de técnicas y metodologías básicas para el estudio de filtrado de Internet y vigilancia.

ONI utiliza una metodología técnica simple para verificar la censura en Internet. Con el fin de identificar y documentar el filtraje en Internet, ONI chequea dos listas de sitios web en cada uno de los países analizados: una lista universal (constante para cada país) y una lista local (diferente para cada país). La lista mundial está formada por sitios web relevantes a nivel internacional con contenido en Inglés que pueden considerarse provocativos o censurables. Las listas locales están diseñadas de forma individual para

cada país para documentar el filtrado y bloqueo de comportamiento único. En los países donde se ha reportado censura en Internet, las listas locales también incluyen aquellos sitios que supuestamente habrían sido bloqueados.

Los resultados son presentados por ONI en mapas clasificados por categorías como una ayuda para interpretarlos, en lugar de una medida absoluta de cómo los países filtran (los datos utilizados por ONI están actualizados hasta noviembre del 2012). En la Figura 4.1 se muestra el mapa de resultados en la categoría de "contenidos políticos", que son aquellos que expresan puntos de vista en oposición a los del gobierno actual o están relacionados con los derechos humanos, la libertad de expresión, los derechos de las minorías y los movimientos religiosos; los niveles de filtraje mostrados en colores son: persuasivos, sustanciales, selectivos, sospechosos y no evidencia. El color gris significa que "no hay datos", lo cual no necesariamente indica ausencia de prácticas de filtraje.



Fuente:OpenNet Initiative

Figura 4.1: Niveles de filtraje de contenidos políticos

Los niveles de filtraje se clasifican en: penetrante (pervasive), substancial (substantial), selectivo (selective), sospechoso (suspected), y no evidencia (no evidence).

El filtrado penetrante se caracteriza tanto por su profundidad - un régimen que bloquea una gran parte de los contenidos dirigidos a una categoría determinada - y su anchura - un régimen de bloqueo que incluye el filtrado en varias categorías en un tema dado.

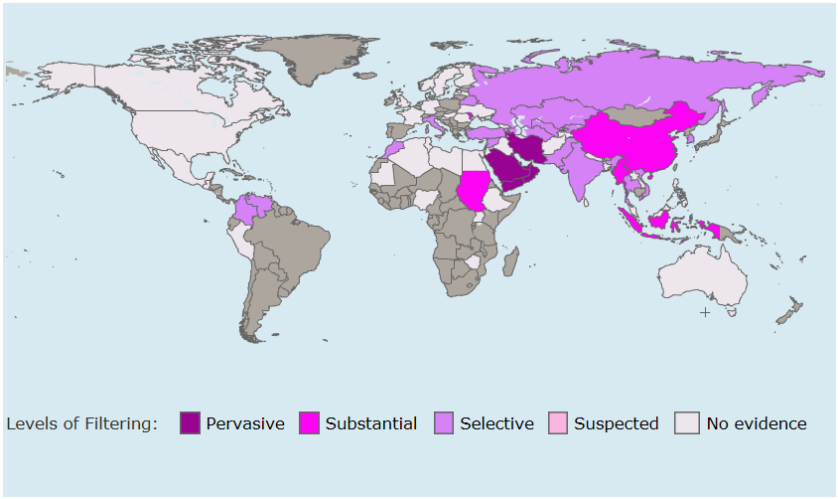
El filtraje substancial es aquel que tiene ya sea profundidad o amplitud: un número de categorías se sujeta a un nivel medio de filtración o un bajo nivel de filtrado se lleva a cabo en muchas categorías.

El filtraje selectivo es aquel que es muy específico que bloquea un número reducido de sitios específicos a través de unas pocas categorías o filtrado que se dirige a una sola categoría o tema.

En el filtraje sospechoso se presentan anormalidades de conectividad que sugieren la presencia de filtraje, aunque el trabajo de diagnóstico no pudo confirmar de manera concluyente que los sitios web de difícil acceso son el resultado de una deliberada manipulación.

La no evidencia de filtraje significa que las pruebas de ONI no encontraron evidencias de que sitios web hayan sido bloqueados.

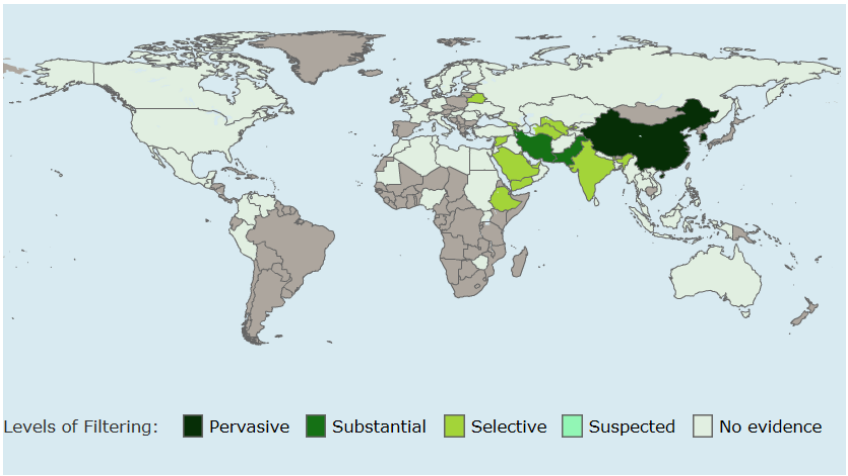
En la Figura 4.2 se muestran los resultados por “contenidos sociales” que son aquellos relacionados con la sexualidad, el juego, y las drogas ilegales y el alcohol, así como también otros temas que pueden ser socialmente sensibles o percibidos como ofensivos.



Fuente: OpenNet Initiative

Figura 4.2: Niveles de filtraje de contenidos sociales

En la Figura 4.3 se muestran los resultados por "contenidos de conflictos y seguridad" que son aquellos relacionados con conflictos armados, disputas de fronteras, movimientos separatistas y grupos militantes.



Fuente: OpenNet Initiative

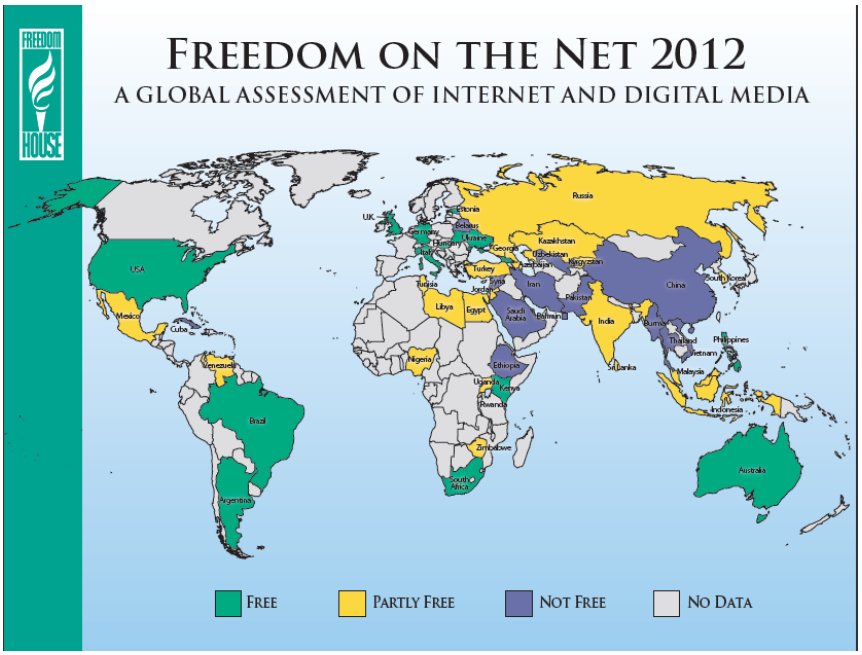
Figura 4.3: Niveles de filtraje de contenidos de conflictos y seguridad

Cabe mencionar que en todos los mapas de ONI mostrados, Ecuador aparece con color gris lo cual significa que no hay datos para nuestro país.

Freedom House, es una organización independiente de vigilancia fundada en New York en el año 1941, dedicada a la expansión de la libertad en el mundo. Esta organización realizó entre enero del 2012 y mayo 2012 un estudio exhaustivo de la libertad de Internet en el mundo que cubrió los acontecimientos que ocurrieron en 47 países. Más de 50 investigadores, casi todos establecidos en los países que analizaron, contribuyeron al proyecto mediante la investigación de las leyes y las prácticas concernientes a Internet, poniendo a prueba la accesibilidad a sitios web seleccionados y entrevistando a una amplia gama de fuentes. Los resultados obtenidos indican que la libertad de Internet en muchos países ha seguido creciendo, a pesar de que los métodos de control están llegando a ser más sofisticados y menos visibles.

Concluye en su estudio Freedom House, que ataques brutales contra los bloggers, la vigilancia por motivos políticos, la manipulación proactiva de contenidos web y leyes restrictivas que regulan la expresión en línea, son algunas de las diversas amenazas a la libertad de Internet que han surgido en los últimos dos años, sin embargo también se han producido varias victorias notables como consecuencia de un mayor activismo de la sociedad civil, las empresas de tecnología y los tribunales independientes.

La Figura 4.4 muestra la medición efectuada por Freedom House en el año 2012 sobre la libertad de Internet en el mundo, estableciendo como niveles de libertad: libre, parcialmente libre, no libre y sin datos. En esta investigación, Ecuador también aparece sin datos.



Fuente: Freedom House

Figura 4.4: Libertad de Internet en el mundo en el 2012

Reporters Without Borders (Reporteros sin Fronteras) fue fundada en Montpellier (Francia) en 1985 por 4 periodistas: Robert Ménard, Rémy Loury, Jacques Molénat and Émilien Jubineau. Esta asociación está registrada como una organización sin fines de lucro desde 1995, y pronto adquirió una dimensión internacional. La actuación de Reporteros sin Fronteras se extiende a los cinco continentes, gracias a sus secciones nacionales (Alemania, Austria, Bélgica, Canadá, España, Francia, Italia, Suecia y Suiza), sus oficinas en Londres, Nueva York y Washington, y su red de más de ciento cincuenta corresponsales.

De acuerdo con Reporteros sin Fronteras, en el 2011 en el mundo existieron 5 netciudadanos asesinados (3 de ellos en México), 199 blogueros y netciudadanos arrestados, 62 blogueros y netciudadanos agredidos, y 68 países afectados por alguna

forma de censura de la Red. Según el "barómetro" de esta organización existen en el año 2013, 178 internautas encarcelados.

En su informe correspondiente al año 2012, Reporteros sin Fronteras opina que las redes sociales complican la tarea de los regímenes autoritarios, que intentan asfixiar toda información molesta. Agrega que la mayoría de los regímenes que censuran la Red, desde el inicio de las revoluciones tunecina y egipcia han reforzado el filtraje para intentar impedir toda propagación de esos movimientos en su país. Otros, incorporaron el uso de filtros como una herramienta de gobierno, útil para ampliar su dominio en el poder. Esta organización establece en su reporte, la nueva lista del año 2012 de los "enemigos de Internet", mencionando que dos países, Bahréin y Bielorrusia, pasan de la categoría de"países bajo vigilancia" a la de "Enemigos de Internet" uniéndose a Arabia Saudita, Birmania, China, Corea del Norte, Cuba, Irán, Uzbekistán, Siria, Turkmenistán y Vietnam, que combinan a menudo problemas de acceso a Internet, un filtraje severo y persecución de ciberdisidentes. Todos esos países se distinguen no sólo por su capacidad de censurar la información y las noticias en línea, sino también por su persecución virtualmente sistemática de los usuarios de Internet. El informe concluye también que Venezuela y Libia dejaron de pertenecer a la lista de países "bajo vigilancia", mientras que India y Kazajistán entraron en ella. Los países bajo vigilancia son aquellos donde se han producido inquietantes acontecimientos que amenazan el acceso a la información en línea y la libertad de expresión. En la Figura 4.5 aparecen los países clasificados como "enemigos de Internet" y "bajo vigilancia".

Fuente: Reporters without Borders, Internet Enemies Report 2012

Figura 4.5: Países Enemigos de Internet y Bajo Vigilancia en el 2012

Cabe mencionar que también existen grupos que se dedican a combatir el filtraje como por ejemplo *Global Internet Freedom Consortium* constituido en el año 2006, una alianza de algunas organizaciones líderes en desarrollar e implementar tecnologías anti-censura para los usuarios de Internet en regímenes opresivos. Los socios de este Consorcio han contribuido significativamente al avance de la libertad de información en China, Irán, Burma, y en muchas otras sociedades cerradas. El Consorcio y sus organizaciones miembros son en gran parte apoyados y operados por voluntarios. La mayoría de voluntarios son practicantes de la disciplina espiritual denominada Falun Gong, exiliados de China, y muchos de ellos eran también estudiantes que estuvieron en Tiannamen Square en 1989. Los socios del Consorcio, como por ejemplo *Dynamic Internet Technology Inc., UltraReach Internet Corp. U.S.A y Garden Networks*, tienen

un portafolio de herramientas anti-censura, como FreeGate , UltraSurf y GTunnel, que se constituyen en la columna vertebral de su operación anti-censura.

De las investigaciones realizadas por las organizaciones no gubernamentales citadas anteriormente se puede concluir que no existe una libertad de expresión en línea en algunos países del mundo o existen limitaciones a esa libertad y que los usuarios de Internet, adicionalmente a sufrir filtrajes en la red, han sido víctimas de represiones. En estos estudios, Ecuador aparece "sin datos" por cuya razón después del estudio que se efectuará en el Capítulo 7 de la presente tesis, se establecerá una conclusión sobre la situación de nuestro país.

4.2. Derechos de propiedad intelectual.

El Informe 2011 del Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, al que se ha referido anteriormente, pone de relieve su preocupación en que en algunos países se están aprobando legislaciones con el fin de desconectar a los usuarios para impedir su acceso a Internet si violan derechos de propiedad intelectual, entre las que se incluye una legislación basada en el concepto denominado "respuesta graduada", que consiste en imponer a quienes infrinjan los derechos de propiedad una serie de penas que pueden culminar en la suspensión del servicio de Internet, como ocurre con la denominada "ley de los tres avisos" aprobada en Francia y en la "Ley de la Economía Digital" en el Reino Unido.

Dutton, et al. (2011, p. 55) opinan que la arquitectura de Internet ha hecho más difícil la aplicación de los derechos de propiedad intelectual y que esta situación ha apoyado la creación de redes abiertas (open) y entre pares (peer-to-peer) conocidas como P2P para compartir archivos. Estas redes P2P permiten el intercambio directo de información

entre los servidores interconectados, las mismas que se implementan como redes superpuestas en Internet y pueden ser utilizadas para intercambiar archivos, cuyos contenidos están sujetos a las leyes de propiedad intelectual.

Con relación a la "Ley de los Tres Avisos" o de "Respuesta Graduada" aprobada en Francia, los autores expresan que está dirigida a hacer cumplir los derechos de propiedad intelectual, dando a las Cortes la facultad de desconectar a usuarios de Internet si son encontrados culpables de una ilegal compartición de archivos P2P de material que tiene derechos de autor. Respecto a la "Ley de la Economía Digital y Protección de la Propiedad Intelectual" adoptada en el año 2009 en Reino Unido, contiene una serie de medidas diseñadas para proteger las industrias creativas existentes, particularmente de música y filmación. Se proponen medidas que podrían presionar a los Provedores de Servicios de Internet (ISPs) a monitorear a los usuarios con el fin de identificar a aquellos que están participando en una ilegal compartición de archivos y crear mecanismos para desconectar a aquellos usuarios del Internet.

Se ha generado entonces un debate acerca de los derechos de la propiedad intelectual en la era digital.

Dentro de esta temática es oportuno comentar los intentos del Congreso de los Estados Unidos de aprobar leyes que tienen como finalidad proteger los derechos de propiedad intelectual. El primero fue el proyecto de Ley PIPA denominado así por sus siglas en Inglés (Protect IP Act - Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act) cuya traducción al Español sería "Acta de prevención de la Propiedad Intelectual - Acta de Prevención a las Verdaderas Amenazas a la Creatividad Económica y al Robo de Propiedad Intelectual" presentado a la Cámara del Senado el 12 de mayo del 2011.

El segundo fue el proyecto de Ley SOPA denominado así por sus siglas en Inglés (Stop Online Piracy Act) cuya traducción al Español sería "Acta para detener la piratería en línea" presentado a la Cámara de Representantes el 26 de octubre del 2011.

En el blog académico "Educación y Tecnología para el Cambio Social" de *UNESCO Chair*, se puede encontrar la opinión de esta organización sobre los dos proyectos de Ley antes citados, expresando que son "ampliamente criticados por anteponer de forma injusta los intereses de propiedad intelectual de diferentes industrias a los derechos de la ciudadanía en general, suponiendo una amenaza a la libertad de expresión, a la privacidad, y un freno a la innovación y a la inversión en servicios en Internet".

SOPA y PIPA generaron la reacción de los usuarios de internet en el mundo que veían en estos proyectos de Ley como una censura a la web y una amenaza a la libertad de expresión. Es así que, una serie de compañías e instituciones tal como Google, realizaron campañas en oposición a la aprobación de SOPA; esta compañía recogió una lista de más de 7 millones de personas, solo en Estados Unidos, que se oponían a esta Ley. El día 18 de enero del 2012 se organizó la protesta más grande en la historia de Internet, en la que más de 100 sitios, en que estuvo incluido Wikipedia, participaron en el "apagon digital" durante 24 horas. Reporteros sin Fronteras expresó que dicho apagón permitió movilizar como nunca a internautas del mundo. La protesta rindió sus frutos el 21 de enero del 2012, pues el congresista Lamar Smith, promotor de SOPA, retiró el proyecto de la ley SOPA hasta encontrar "un mayor consenso sobre la solución para poner fin a la piratería en Internet". De igual forma el parlamentario Harry Raid, como vocero de la mayoría partidista del Senado, declaró que la votación del proyecto de Ley PIPA sería postergada hasta que se resuelva la polémica generada al respecto.

Lo anterior incentivó movilizaciones contra el proyecto ACTA cuyas siglas provienen de "Anti-Counterfeiting Trade Agreement" traducido al Español como "Tratado

Comercial Anti-falsificación", que es un tratado multilateral de adhesión voluntaria para la protección de la propiedad intelectual y que tiene como uno de sus objetivos combatir la piratería en Internet. Mediante este tratado se obliga a los ISPs a controlar los datos que se cargan y descargan en Internet y se establecen sanciones como la desconexión de la red, sanciones pecuniarias y prisión para los usuarios considerados infractores. Ante esta reacción, algunos gobiernos suspendieron su ratificación y se piensa que los días de ACTA están contados.

Contrario a estas intenciones de los gobiernos de censurar a los usuarios de Internet, esgrimiendo como justificación los derechos de propiedad intelectual, es digno de encomio la labor que viene desarrollando la UNESCO, que en su Asamblea General número 36 realizada en noviembre del 2011, adoptó la estrategia denominada "Open Access" o "Acceso Abierto", mediante la cual se promueve y apoya el libre acceso en línea a la información científica y al conocimiento para todas las personas, libre de la mayoría de las barreras impuestas por las licencias y los derechos de propiedad intelectual, para promover el intercambio del conocimiento en el plano mundial, la innovación y el desarrollo socioeconómico.

Isabel Viera, oficial del programa de Comunicación e Información de la Oficina de la UNESCO en La Habana, en su intervención en el Taller Latindex para Editores de Revistas Académicas y Científicas de República Dominicana, que tuvo lugar los días 19 y 20 de septiembre del 2011 en Santo Domingo, manifestó que la UNESCO "alienta a los autores, investigadores y científicos a publicar sus trabajos y resultados científicos en revistas especializadas que faciliten la utilización de los mismos de manera libre y que extiendan una licencia para que puedan ser copiados, utilizados y distribuidos por otras personas de manera responsable y reconociendo adecuadamente su autoría".

4.3. Protección de la privacidad y de los datos.

UIT News (2010) opina que los sitios de redes sociales son objetivos muy atractivos para las violaciones de la privacidad y la seguridad. Cualquiera que viole la seguridad de un sitio web puede obtener fácilmente información privada y valiosa sobre un gran número de usuarios y se pregunta esta revista si se acabó la privacidad con el advenimiento de las redes sociales. Agrega que, según varios expertos del sector de las TICs, el posible daño causado a los usuarios por el acceso no autorizado a sus datos, depende de hasta qué punto participan en el sitio web de la red social y del volumen de información que están dispuestos a compartir.

La Rue en su Informe 2011 sobre la promoción y protección del derecho a la libertad de opinión y de expresión, comenta sobre la protección inadecuada del derecho a la intimidad y a la protección de datos. Manifiesta que el derecho a la intimidad es fundamental para la libre expresión personal. De hecho, a lo largo de la historia la voluntad de las personas de participar en debates públicos sobre temas controvertidos ha estado siempre vinculada con la posibilidad de poder hacerlo de forma anónima. Internet permite acceder a información y tomar parte en debates públicos sin tener que revelar la identidad personal, por ejemplo usando seudónimos. A la vez, Internet ofrece nuevos instrumentos y mecanismos por medio de los cuales los actores, tanto estatales como privados, pueden supervisar y reunir información sobre las comunicaciones y actividades de los usuarios de Internet. Estas prácticas pueden constituir una violación del derecho de estos usuarios a la intimidad y, al socavar la confianza del público y la seguridad de Internet, obstruir el libre flujo de información e ideas en línea. El Relator Especial muestra su preocupación por las medidas adoptadas por ciertos Estados contra personas que se comunican por Internet, con frecuencia justificándolas en términos generales por su necesidad para proteger la seguridad nacional o luchar contra el terrorismo. Por ejemplo, algunos Estados han hecho uso de sitios populares de redes

sociales, como Facebook, para detectar y vigilar actividades de defensores de los derechos humanos y miembros de la oposición, y en algunos casos han obtenido nombres de usuarios y contraseñas para acceder a las comunicaciones privadas de usuarios de Facebook.

El Secretario General de la ONU en su informe AA/66/90 presentado a la Asamblea General el 10 de agosto del 2011, respecto al informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión, expresa que si bien Internet ofrece nuevas y mayores oportunidades para la difusión y el acceso a la información e ideas de todo tipo, sería ingenuo y peligroso pasar por alto que simultáneamente puede utilizarse como herramienta para controlar, identificar, localizar y poner en el punto de mira a personas que difunden información crítica u otra información delicada a través de Internet. Por otra parte, la gran cantidad de información personal que se encuentra disponible en línea, en particular, a través de los sitios de las redes sociales, también plantea serias preocupaciones sobre el derecho a la privacidad, por ejemplo: ¿quién tiene acceso a información personal específica?, ¿cómo se utiliza la información?, y si la información se almacena ¿por cuánto tiempo? Se recalca en el informe la importancia de la función de los gobiernos, de garantizar plenamente el derecho a la privacidad de las personas, sin lo cual no se puede disfrutar plenamente del derecho a la libertad de opinión y de expresión.

Mendel, et al. (2012, ps. 20 - 21) reconocen que Internet ha cambiado la naturaleza de la privacidad y que existen nuevas amenazas a la privacidad; afirman que existen nuevas oportunidades para el uso comercial de datos personales. Las redes sociales son sitios web que se centran en construir y/o reflejar relaciones sociales entre las personas. Algunos facilitan la amistad entre personas que ya se conocen fuera de línea, permitiendo a ellos compartir fotos y conversar en línea. Otros se concentran en permitir a las personas hacer nuevos amigos, a menudo con un objetivo particular tal como

relaciones de trabajo (LinkedIn) o prueba de música (Pandora). Cada servicio es diferente pero el formato estandar permite a los usuarios crear su propia página web conteniendo varias piezas de información personal (tales como fecha de nacimiento, ubicación, intereses, nombre). Los autores agregan que los sitios de redes sociales son muy populares con millones de usuarios entre ellos, pero que sin embargo ha estado creciendo la preocupación sobre las violaciones de la privacidad causada por tales sitios.

Mendel, et al. (2010) consideran que la computación en la nube (cloud computing) es una arquitectura de red emergente, donde datos o softwares son guardados en servidores remotos que son accesibles vía Internet en contraposición a un computador personal, y sin embargo la computación en nube también genera preocupaciones desde una perspectiva de privacidad, en vista de que los datos son guardados en un software de una tercera parte, y que la responsabilidad para proteger la información recae en la tercera parte perdiendo el usuario un grado de control. Los autores opinan que los motores de búsqueda desempeñan un rol crucial como intermediarios en Internet, permitiendo a los usuarios encontrar y accesar a contenidos. Ejemplos incluyen a Google, Bing, Ask.com, y Yahoo. Los motores de búsqueda colectan una gran cantidad de información personal. Esta información puede ser identificable personalmente y puede revelar piezas sensitivas de información, tales como las inclinaciones políticas de las personas, orientación sexual, creencias religiosas y problemas médicos. Esta información es usada generalmente para propósitos comerciales, sin embargo, también hay riesgos de divulgación pública de la información.

Mendel, et al. (2010, p. 14) señalan que cada computador, teléfono móvil u otro aparato conectado a Internet tiene una única dirección IP, que proporciona un identificador único para cada aparato y lo que significa a su vez que pueden ser rastreados. La capacidad para localizar cualquier aparato genera nuevos desafíos a la privacidad. De las herramientas que han sido creadas para rastrear a los usuarios de Internet, dos ejemplos

comunes son los cookies (galletas) y los web bugs (balizas web). Los cookies son pequeñas piezas de texto que los navegadores de la web guardan en los computadores de los usuarios. Estos cookies son almacenados en el computador del usuario de Internet cada vez que visitan un sitio web y cuando utilizan su navegador de Internet. Pueden ser usados para rastrear sesiones, guardar preferencias de sitios web, autenticaciones, etc. Los web bugs son pequeños gráficos insertados por terceros en una página web o en un email para recolectar información acerca de las preferencias e inquietudes de los usuarios, y generalmente son invisibles a éstos por su reducido tamaño.

Durante la realización del Forum de la Gobernanza de Internet 2012, realizado en Baku-Azerbaijan (2012), la UNESCO organizó un taller en el que participaron los expertos Andrew Puddephatt y Ben Wagner, quienes sostuvieron que los retos a la protección de la privacidad se han multiplicado debido a la recolección de una mayor cantidad de información de diversos tipos e insistieron en los problemas relacionados con el almacenamiento y análisis de datos, la supervisión por parte de entidades públicas y privadas, y la expansión de mercados de datos personales. Los dos expertos afirmaron que, cuando la libertad de expresión y la privacidad se contradicen, la decisión sobre cuál de las dos prima debe tomarse de acuerdo con el beneficio del interés general. Ambos recalcaron que se necesita una fuerte protección constitucional para asegurar tanto la privacidad como la libertad de expresión. Propusieron que para proteger la privacidad, el derecho penal tenga muchas más limitaciones y que, en cambio, para estas cuestiones, se haga énfasis en las soluciones civiles. Otros participantes en el taller subrayaron la importancia de los esfuerzos por establecer normas para la protección de los datos y de la privacidad.

4.4. Protección de los niños en línea.

El Informe 2011 del Relator Especial de la ONU, Frank La Rue, explica que, aunque la protección de los niños en línea ante contenidos inapropiados puede constituir una meta legítima, la disponibilidad de programas de filtros que los padres y las autoridades académicas pueden emplear para controlar el acceso a determinados contenidos hace menos necesaria, y más difícil de justificar, la intervención del Gobierno, por ejemplo mediante un bloqueo.

El Relator Especial de la ONU observa que la pornografía infantil es una clara excepción en la que se justifican las medidas de bloqueo, siempre que la legislación nacional sea suficientemente precisa y se disponga de salvaguardas eficaces frente a su abuso o uso indebido, entre ellas la supervisión y el examen a cargo de un tribunal u órgano regulatorio independiente e imparcial. Sin embargo, también le preocupa que, frecuentemente los Estados recurran en gran medida a medidas de bloqueo en lugar de centrar su labor en el procesamiento de los responsables de producir y difundir pornografía infantil.

De acuerdo a estudios recientes realizados por la UIT, el 60% de los niños y jóvenes chatean diariamente, cada año uno de cada 5 niños son blanco en Internet de un predador o pedófilo; en Francia, el 72% de los niños navegan solos en la web, y mientras el 85% de sus padres conocen acerca de software de control paternos, únicamente el 30% lo instalan. En el Reino Unido, 57% de usuarios de Internet comprendidos en la las edades de 9 a 19 años dicen que han visto pornografía en línea, 46 % dicen que han dado información que no debían y 33% dicen que ellos han sido intimidados en línea. En China, el 44% de niños dicen que han sido abordados por extraños y 41% habían hablado en línea con extraños sobre sexo, o sobre algo que le han hecho sentir incómodos.

Entre los ataques que pueden sufrir los niños en línea podemos citar el "ciberbullying" y el "grooming". El ciberbullying es una forma de acoso entre iguales, que deriva en una agresión psicológica sostenida y repetida en el tiempo que es cometida por uno o varios escolares contra otro. La víctima, continuamente sometida a vejaciones, insultos o burlas por parte de sus compañeros, puede llegar a un estado de indefensa que puede acarrear duras consecuencias para su desarrollo físico y mental. El grooming es otra forma de acoso deliberado en este caso de un adulto a un niño con el objetivo de establecer una relación o control emocional sobre el menor simulando ser otro niño/a cuya finalidad última es la de abusar sexualmente del menor. Estas conductas comienzan en la red y en una segunda fase transcienden al ámbito físico a través de chantajes e intimidaciones a la víctima. (Revista SUPERTEL No. 13, p. 23).

La iniciativa "Protección de los Niños en Línea" conocida con las siglas COP por su traducción al Inglés (Child Online Protection) es parte de la Agenda Global de Ciberseguridad (Global Cybersecurity Agenda) de la UIT que tiene como propósito fomentar la cooperación internacional dirigida a proporcionar estrategias para encontrar soluciones tendentes a mejorar la confianza y la seguridad en la Sociedad de la Información, Agenda a la que se referirá en el Capítulo siguiente. Los objetivos de la COP son: identificar riesgos y vulnerabilidades de los niños en el ciberespacio, crear conciencia, desarrollar herramientas para ayudar a minimizar los riesgos y compartir conocimientos y experiencias.

Child Online Protection (2009, p. 4) señala que, con el fin de formular una estrategia nacional centrada en la seguridad de los niños en línea, los responsables de elaborar las políticas necesitan considerar estrategias basadas en áreas claves. Por ejemplo, una de ellas es la revisión del marco legal existente para determinar si existe todo el poder legal necesario para proteger a las personas menores a 18 años, que se encuentran en línea en todas las plataformas disponibles de Internet; otra es, establecer que todo acto contra un

niño que es ilegal en el mundo real, es también ilegal en línea, y que, las leyes para la protección de los datos en línea y la privacidad para los menores de edad legales son también adecuadas; y establecer mecanismos que provean un medio fácilmente entendible para reportar contenidos ilegales encontrados en la red, por ejemplo, una línea caliente nacional, la cual tenga la capacidad para responder inmediatamente y remover los materiales ilegales o hacerlos inaccesibles.

4.5. Discurso de odio.

Se considera que el "discurso de odio" (hate speech) son expresiones que incitan a la discriminación, hostilidad o violencia en contra de una o más personas en virtud de pertenecer a un grupo determinado, sea este una nación, raza, o religión. La difusión por Internet del "discurso de odio" también ha estimulado a tratar de regular el contenido en línea.

El Artículo 20, numeral 2 del Convenio Internacional de Derechos Civiles y Políticos señala que "toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia estará prohibida por la ley".

El Relator Especial de la ONU, Frank La Rue en su informe 2011 observa que muchas formas de discurso de odio no se ajustan al nivel de gravedad establecido en el artículo 20, párrafo 2 del Pacto Internacional de Derechos Civiles y Políticos y que, el derecho a la libertad de expresión implica que se debería poder examinar, debatir y criticar abiertamente, incluso de forma agresiva e irrazonable, ideas, opiniones, creencias e instituciones, incluidas las religiosas, siempre y cuando esto no constituya apología del odio que incita a la hostilidad, discriminación o violencia contra una persona o un grupo de individuos.

Dutton, et al. (2011, p. 61) opinan que así como Internet es un mecanismo para extender la democracia, es también un caldo de cultivo para la incitación al odio por parte de grupos que lo han utilizado para promover su causa. Los autores consideran que aunque la mayoría de las personas tiende a aceptar que se trata de una consecuencia negativa de Internet, algunos piensan que la regulación inadecuada del discurso de odio en línea, puede llevar a la supresión del derecho a la libertad de expresión.

Capítulo 5

Seguridad informática, políticas mundiales y prácticas nacionales.

5.1. Plan de Acción C5 de la Cumbre Mundial de la Sociedad de la Información: Creación de confianza y seguridad en la utilización de las TICs.

El Plan de Acción aprobado en Ginebra durante la Primera Fase de la CMSI en el 2003, contiene las líneas de acción concretas (denominadas con letras C) para construir una Sociedad de la Información en un nivel nacional, regional e internacional. Una de estas líneas de acción es la C5 titulada "Creación de confianza y seguridad en la utilización de las TICs", la misma que enfatiza que la confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información. Los enunciados de esta línea de acción son:

a) Propiciar la cooperación entre los gobiernos dentro de las Naciones Unidas, y con todas las partes interesadas en otros foros apropiados, para aumentar la confianza del usuario y proteger los datos y la integridad de la red; considerar los riesgos actuales y potenciales para las TIC, y abordar otras cuestiones de seguridad de la información y de las redes.

b) Los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC, definiendo directrices que tengan en cuenta los esfuerzos existentes en estos ámbitos; estudiando una legislación que permita investigar y juzgar efectivamente la utilización indebida; promoviendo esfuerzos efectivos de asistencia mutua; reforzando el apoyo institucional a nivel

internacional para la prevención, detección y recuperación de estos incidentes; y alentando la educación y la sensibilización.

c) Los gobiernos y otras partes interesadas deben fomentar activamente la educación y la sensibilización de los usuarios sobre la privacidad en línea y los medios de protección de la privacidad.

d) Tomar medidas apropiadas contra el envío masivo de mensajes electrónicos no solicitados ("spam") a nivel nacional e internacional.

e) Alentar una evaluación interna de la legislación nacional con miras a superar cualquier obstáculo al uso efectivo de documentos y transacciones electrónicas, incluido los medios electrónicos de autenticación.

f) Seguir fortaleciendo el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TICs, con iniciativas o directrices sobre el derecho a la privacidad y la protección de los datos y de los consumidores.

g) Compartir prácticas óptimas en el ámbito de la seguridad de la información y la seguridad de las redes, y propiciar su utilización por todas las partes interesadas.

h) Invitar a los países interesados a establecer puntos de contacto para resolver incidentes en tiempo real, y desarrollar una red cooperativa entre estos puntos de contacto de forma que se comparta información y tecnologías para intervenir en caso de estos incidentes.

i) Alentar el desarrollo de nuevas aplicaciones seguras y fiables que faciliten las transacciones en línea.

j) Alentar a los países interesados a que contribuyan activamente en las actividades en curso de las Naciones Unidas tendentes a crear confianza y seguridad en la utilización de las TICs.

5.2. Agenda sobre la ciberseguridad global: medidas legales, medidas técnicas y de procedimiento, estructuras institucionales, creación de capacidades y cooperación internacional.

De acuerdo con el informe 2011 del Relator Especial de la ONU Frank La Rue, los ciberataques, que son intentos de invalidar o poner en peligro el funcionamiento de un sistema informático, constan de medidas tales como intrusiones piratas en cuentas o redes informáticas y suelen adoptar la forma de ataques distribuidos de denegación del servicio, en el marco de los cuales se emplea un grupo de computadores para inundar con solicitudes de acceso a un servidor web en el que se aloja el sitio web atacado, a raíz de lo cual este se cae y queda inaccesible durante un período. Como ocurre con los bloqueos programados, a veces estos ataques se lanzan en momentos políticos clave. Explica La Rue que, aunque la determinación del origen de los ciberataques y de la identidad del autor suele ser técnicamente difícil, cabe señalar que los Estados están obligados a proteger a las personas de injerencias de terceros que menoscaben el disfrute del derecho a la libertad de opinión y de expresión. Esta obligación positiva de protección supone que los Estados deben adoptar medidas apropiadas y eficaces para investigar los actos cometidos por terceros, exigir a los responsables que rindan cuentas de esos actos y adoptar medidas para que estos no se repitan en el futuro.

La UIT lanzó en marzo del 2007 la Agenda para la Ciberseguridad Global (Global Cybersecurity Agenda) que es un marco para la cooperación internacional destinada a fortalecer la confianza y seguridad en la Sociedad de la Información. El Secretario General de la UIT creó un Grupo de Expertos de Alto Nivel sobre Ciberseguridad (GEANC) compuesto por representantes de los gobiernos, la industria, las organizaciones internacionales e instituciones académicas y de investigación, encargados de ofrecer asesoramiento y orientación al Secretario General de la UIT en materia de estrategias para promover la ciberseguridad. Este grupo de expertos atrajo a grandes especialistas de empresas como AT&T, Intel, Microsoft, Interpol o Verisign, así

como a altos representantes de los sectores público, académico y privado del mundo entero, que contribuyeron con sus ideas para decidir cómo afrontar mejor las crecientes dificultades de seguridad del mundo en línea. Su principal objetivo era crear estrategias para elaborar una legislación modelo sobre ciberdelincuencia, que sea mundialmente aplicable y se adapte a las legislaciones nacionales y regionales existentes.

Los miembros del GEANC han señalado la importancia de que los gobiernos y las empresas del sector privado colaboren para asegurarse que la policía y el poder judicial dispongan de las herramientas apropiadas para proteger al público contra las actividades delictivas, pero siempre protegiendo los derechos humanos fundamentales y la vida privada de las personas.

EL GEANC ha puesto de relieve que es importante disponer de estructuras organizacionales nacionales, regionales e internacionales apropiadas para proteger la ciberseguridad y luchar contra la ciberdelincuencia. Su función consiste en integrar las actividades de varios organismos, ahorrar valiosos recursos e impedir la duplicación de esfuerzos. Recomiendan que cada país debe poder determinar su propia estrategia y sus estructuras organizacionales para atender a sus necesidades de ciberseguridad nacional, y promover la asistencia a través de la cooperación regional o internacional. El grupo recomienda un “marco organizacional de ciberseguridad” flexible que los países puedan adaptar a sus circunstancias particulares. Los centros regionales de vigilancia, aviso y respuesta a incidentes deberían prestar servicio en varios países.

El GEANC ha observado también que la creación de capacidades en el campo de la ciberseguridad exige recursos financieros, técnicos y humanos específicos, así como una cooperación internacional.

La Agenda para la Ciberseguridad Global (ACG) tiene por objeto alcanzar las siete metas estratégicas siguientes:

a) Preparar estrategias que promuevan el desarrollo de una legislación modelo sobre ciberdelito, que resulte aplicable a escala mundial y sea compatible con las medidas legislativas ya adoptadas en los diferentes países y regiones.
b) Definir estrategias mundiales para crear las adecuadas estructuras institucionales nacionales y regionales, así como definir las correspondientes políticas para luchar contra el ciberdelito.
c) Diseñar una estrategia que permita establecer un conjunto mínimo y mundialmente aceptado de criterios de seguridad y planes de acreditación para equipos, aplicaciones y sistemas informáticos.
d) Definir estrategias para crear un marco mundial con miras a vigilar, alertar y responder ante incidentes y garantizar así la coordinación transfronteriza en lo que concierne a las iniciativas nuevas y existentes.
e) Diseñar estrategias mundiales tendentes a crear y apoyar un sistema de identidad digital genérico y universal y las correspondientes estructuras institucionales para garantizar el reconocimiento internacional de credenciales digitales.
f) Concebir una estrategia global para facilitar la creación de capacidad humana institucional con el fin de promover los conocimientos técnicos y prácticos en todos los sectores y las esferas antes mencionadas.
g) Formular propuestas para establecer un marco conducente a una estrategia mundial multipartita que fomente la cooperación, el diálogo y la coordinación internacionales en todas las esferas precitadas.

Para alcanzar esas metas, la ACG se basa en los cinco pilares siguientes a fin de orientar sus sectores de actividad:

1. Medidas legales
2. Medidas técnicas y de procedimientos
3. Estructuras institucionales
4. Creación de capacidades
5. Cooperación internacional.

Medidas legales: El establecimiento de la infraestructura legal apropiada es una componente integral de cualquier estrategia nacional sobre ciberseguridad. En efecto la ACG contempla que la adopción por todos los países de legislaciones apropiadas en contra del mal uso de las TICs con fines delictivos u otros propósitos, incluida las actividades realizadas con la intención de afectar la integridad de las infraestructuras nacionales de información crítica, es esencial para lograr la ciberseguridad mundial.

Medidas técnicas y de procedimientos: Este pilar se centra en las medidas destinadas a tratar las vulnerabilidades de los productos informáticos, con objeto de concebir sistemas, protocolos y normas de acreditación aceptables a escala mundial. La AGC reconoce que las TIC son una herramienta vital en la sociedad de la información. Sin embargo, continúan siendo explotadas por los usuarios malévolos y este fenómeno está intrínsecamente ligándose al crimen organizado en Internet. Las vulnerabilidades en aplicaciones de software son deliberadamente buscadas con el fin de crear malware (software malicioso) que pueden permitir acceso y modificaciones no autorizadas, lo que compromete la integridad, autenticidad y confidencialidad de las redes y sistemas de las TICs. Con la creciente sofisticación del malware, estas amenazas no pueden ser sobrestimadas y podrían tener graves consecuencias si las infraestructuras de información crítica son afectadas. Las organizaciones de normalización juegan un papel fundamental en el tratamiento de las vulnerabilidades de seguridad de los protocolos. Junto a numerosas recomendaciones fundamentales sobre seguridad, la UIT ha analizado los requisitos de seguridad, directrices de seguridad para los diseñadores de protocolos,

especificaciones de seguridad para los sistemas basados en IP, así como directrices para identificar ciberamenazas y contramedidas para la prevención de riesgos. La UIT también es la plataforma internacional para el desarrollo de protocolos que protejan las redes actuales y de próxima generación (NGN).

Estructuras institucionales: Los sistemas de vigilancia y alerta y la respuesta a incidentes son esenciales para responder a los ciberataques. Este pilar, por consiguiente, tiene la finalidad de crear estructuras y estrategias orgánicas para ayudar a impedir, detectar y responder a ataques contra infraestructuras esenciales de la información. La AGC sostiene que la falta de estructuras institucionales para el tratamiento de ciberincidentes (ataques, fraude, destrucción de información, diseminación de contenidos inadecuados) es un verdadero problema para dar una respuesta adecuada a las ciberamenazas. Al respecto la UIT realiza una labor de coordinación con varios Estados Miembros de la UIT, centrándose en la ayuda para el establecimiento de equipos nacionales encargados de los incidentes informáticos.

Creación de capacidad: En el marco de la ACG, este pilar tiene por objeto elaborar estrategias para mejorar los conocimientos y capacidades a fin de aumentar la importancia de la ciberseguridad en las agendas de políticas nacionales. La ACG plantea que se necesita promover la creación de capacidad con el fin de desarrollar una cultura sustentable y proactiva de ciberseguridad puesto que las personas son el eslabón más débil de la cadena. Uno de los desafíos fundamentales de la ciberseguridad es educar al usuario final. Entender y ser consciente de los peligros potenciales son factores esenciales para que el usuario final se beneficie de las TICs de forma segura.

Cooperación internacional: La ciberseguridad es tan internacional y trascendental como Internet. La ACG reconoce que Internet y las TICs han facilitado la interconexión entre países de una forma como no era posible antes. Los países no pueden cerrar fácilmente

sus fronteras a amenazas entrantes y tampoco pueden frenar las que proceden de su interior. Aunque los intentos por solucionar estos desafíos a nivel nacional e internacional son importantes, las soluciones deben estar armonizadas más allá de las fronteras nacionales ya que la ciberseguridad es tan global y tiene un alcance similar al de Internet. Ello exige necesariamente la cooperación internacional, no sólo a nivel gubernamental sino también entre la industria, organizaciones no gubernamentales e internacionales. La AGC recomienda, por lo tanto, que las soluciones necesitan ser armonizadas a través de todas las fronteras. Esto implica necesariamente la cooperación, no solo a nivel gubernamental sino también con la industria, organizaciones no gubernamentales y las organizaciones internacionales. La ciberseguridad requiere todo tipo de medidas, por esta razón, la AGC busca aprovechar la potencialidad de la colaboración de las múltiples partes interesadas con el fin de alcanzar estrategias globales para mejorar la ciberseguridad.

Como parte de la Agenda sobre Ciberseguridad Global, la UIT junto con otras agencias del Sistema de las Naciones Unidas, lanzó en noviembre de 2008 la iniciativa "Protección de los Niños en Línea" (Child Online Protection) como una colaboración internacional destinada a promover la ciberseguridad de los niños y proporcionar directrices para un comportamiento seguro en línea.

La Conferencia de Plenipotenciarios de la UIT realizada en Guadalajara en el año 2010 adoptó la Resolución 181 mediante la cual se define la ciberseguridad como:

> *"el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los*

usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad."

5.3. Centro de Respuesta Global.

El Centro de Respuesta Global (CRG) es la plataforma mundial para el sistema de alerta temprana y el principal centro de recursos sobre ciberamenazas para la comunidad mundial, que proporciona servicios de respuesta de emergencia y mecanismos de divulgación de conocimientos en un entorno seguro.

El Centro de Respuesta Global (CRG) está equipado con una sala de crisis, modernísimos equipos informáticos y de comunicaciones, un centro de operaciones de seguridad totalmente funcional y siempre activo, un centro seguro de datos totalmente redundante, instalaciones para los trabajadores que hacen turnos, un centro de radiodifusión propio y una galería de visitas para personalidades. El CRG desempeña pues un papel fundamental en la consecución del objetivo de la ACG de adoptar medidas técnicas para luchar contra las nuevas ciberamenazas y la evolución de las mismas. Los dos elementos más destacados del CRG son NEWS (sistema de alerta temprana en red) y ESCAPE (plataforma de aplicación de colaboración electrónicamente segura para expertos). El programa NEWS ayuda a los países miembros de la UIT a identificar rápidamente ciberamenazas y proporciona información

esencial sobre las medidas que sean adoptadas para mitigarlas. El programa ESCAPE es uno de los instrumentos y sistemas especializados que dispondrán los Estados miembros de la UIT. Se trata de un sistema electrónico con el que ciberexpertos autorizados de varios países pueden unir recursos y colaborar a distancia en un entorno seguro y fiable. ESCAPE permite reunir rápidamente recursos y conocimientos de muchos países diferentes y, de este modo, los países, individual y colectivamente, pueden responder inmediatamente a ciberamenazas, especialmente en situaciones de crisis. ESCAPE tiene su sede central en Cyberjaya, en los alrededores de Kuala Lumpur (Malasia) y fue inaugurada el 20 de marzo del 2010.

5.4. Ciberseguridad en la Agenda Nacional.

Algunas iniciativas regionales ya han recomendado que los Estados miembros de la UIT establezcan centros de ciberseguridad nacionales de respuesta, tales como equipos nacionales encargados de los incidentes informáticos, observando que todavía hay un nivel bajo de preparación contra emergencias informáticas en muchos países, en particular en los países en desarrollo, y que un alto nivel de interconectividad de redes TICs podrían verse afectado por un ataque a redes de los países menos preparados.

5.5. Creación de una estrategia nacional de ciberseguridad.

La Comisión de Estudio 1 del Sector de Desarrollo de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-D, 2010) sostiene que

> *"El diseño y la implementación de un plan nacional de ciberseguridad hace necesario adoptar una estrategia global que entrañe un amplio análisis inicial de la adecuación de las prácticas nacionales de un país y la consideración de la función desempeñada por todas las partes interesadas (autoridades públicas, sector privado y ciudadanos) en este asunto. Por motivos de seguridad nacional*

y para preservar el bienestar económico, los gobiernos deben posibilitar, promover y garantizar la protección de sus infraestructuras de información esenciales. Actualmente, esas infraestructuras son comunes a varios sectores industriales y sobrepasan las fronteras nacionales."

La Comisión de Estudio 1 de la UIT-D recomienda que el plan nacional debe tener como metas: incorporar en las políticas nacionales la cuestión de la ciberseguridad/protección de las infraestructuras de la información esenciales y reconocer la necesidad de tomar medidas en el plano nacional y de cooperar internacionalmente; preparar una estrategia nacional para proteger las infraestructuras de información esenciales y el ciberespacio contra ataques electrónicos y físicos; y, participar en las acciones internacionales que se emprendan para coordinar las actividades nacionales relativas a la prevención, respuesta y recuperación ante incidentes informáticos y a la preparación contra los mismos.

La Comisión de Estudio 1 de la UIT-D señala que si bien las metas precitadas son comunes a todos los países, las medidas específicas que habrá que tomar para implementar dichos objetivos corresponden a las necesidades y circunstancias únicas de cada país. En muchas naciones es el Estado el que deberá adoptar estas medidas, las cuales se citan a continuación:

- Persuadir a los actores clave del Estado de la necesidad de adoptar medidas nacionales para contrarrestar las amenazas y vulnerabilidades de la ciberinfraestructura nacional mediante debates de política.
- Identificar un dirigente y una institución que dirijan a nivel nacional los esfuerzos necesarios; determinar en qué sector público conviene crear un equipo de respuesta en caso de incidentes de seguridad informática (Computer Security Incident Response Team -CSIRT), al que habría que conferir atribuciones

nacionales; identificar las instituciones que responderán de cada uno de los aspectos de la estrategia nacional.

- Identificar a los correspondientes expertos y formuladores de políticas en las autoridades gubernamentales y el sector privado, así como sus funciones.
- Identificar disposiciones de cooperación entre los participantes y dirigidas a éstos.
- Establecer mecanismos de cooperación entre las entidades públicas y privadas en el plano nacional.
- Identificar los interlocutores internacionales y promover esfuerzos internacionales para abordar diferentes aspectos de la ciberseguridad, lo que incluye actividades de intercambio de información y asistencia.
- Establecer un proceso integrado de gestión de riesgos para identificar los esfuerzos de protección que se requieran con el fin de garantizar la ciberseguridad, así como definir un orden de prioridades entre dichos esfuerzos.
- Evaluar y revaluar periódicamente el estado de los esfuerzos de ciberseguridad y diseñar prioridades de programa.
- Identificar requisitos de formación y los medios para satisfacerlos.

El Ing. Fabián Jaramillo, Superintendente de Telecomunicaciones del Ecuador, anunció el 9 de mayo del 2012 a la comunidad internacional que asistía al evento LACNIC XVII realizado en Quito, la próxima implementación del Centro de Respuesta a Incidentes Informáticos del Ecuador (CERT o CSIRT), para permitir que los usuarios ecuatorianos sean protegidos en su navegación por Internet.

La idea de un Centro de Respuesta a Incidentes Informáticos debe ser: detectar e identificar la amenaza, bloquearla, monitorizarla, reportar, guardar registros y evidencias de la amenaza, responderla, pedir información a los organismos o actores involucrados dentro de la respuesta a la amenaza de ser necesario, hacer uso de la infraestructura

disponible y necesaria y comunicar a los demás equipos de apoyo o CSIRT's conectados, para así mitigar las posibles consecuencias que produce un incidente de seguridad informática y promover la recuperación eficaz y efectiva de la información que fue sujeto del incidente, para luego crear un registro almacenado y generar la información respectiva y generar experiencia para compartirla con otros miembros integrados en las redes de confianza. Para el desarrollo de este proyecto se ha contado con la cooperación del gobierno de Corea, mediante una consultoría que se desarrolló en un período de 3 meses, desde el mes de julio al mes de septiembre de 2011, y en la cual se definieron los lineamientos principales que serán el sustento para la conformación de las bases del centro de respuesta a incidentes. Se tenía planificado ejecutar este proyecto hasta fines del año 2012. (Revista SUPERTEL No. 13, ps. 6 - 13).

El Superintendente de Telecomunicaciones en su rendición de cuentas correspondiente al año 2012 efectuada el 20 de enero del 2013, manifestó que con el fin de impulsar la investigación y el control, se ha impulsado nuevos proyectos como el Centro de Respuesta a Incidentes Informáticos, diseñados para combatir los ciberdelitos (ataques informáticos).

Un promedio de siete delitos informáticos por día se registraron en el Ecuador el 2012; la Fiscalía General registró a nivel nacional en los primeros seis meses de ese año, 1.354 casos de delitos informáticos financieros de los cuales 563 denuncias corresponden a la provincia de Pichincha, 275 a Guayas y 131 a Santa Elena. La Fiscalía General del Ecuador recibió 3.129 denuncias por delitos informáticos en el año 2011, cifra que se ha incrementado comparadas con las recibidas en el 2009 (168), y en el 2010 (1.099). Un estudio realizado por las empresas GMS y Kaspersky estableció que las pérdidas económicas por delitos informáticos en el Ecuador ascendieron a un millón de dólares entre 2009 y 2010. (Diario El Universo, edición del 26 de agosto del 2012).

Cabe mencionar que la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del Ecuador, Ley 2002-67, publicada en el Registro Oficial No. 455 del 17 de abril del 2002, le dedica el Título V a las "Infracciones Informáticas" y es así que mediante el Art. 58, efectúa reformas al Código Penal agregando 2 artículos a continuación del Art. 202 de dicho Código donde se tipifica y sanciona las infracciones informáticas. También en el Art. 59 de la Ley 2002-67 se tipifica y penaliza la destrucción maliciosa de documentos contenidos en un sistema de información o red electrónica, modificando el Art. 262 del Código Penal; a través del Art. 60 se tipifica y penaliza la falsificación electrónica agregando un artículo a continuación del Art. 353 del Código Penal; mediante el Art. 61 se tipifican y penalizan los daños informáticos agregando 2 artículos después del Art. 415 del Código Penal; mediante el Art. 62 se sanciona la apropiación ilícita utilizando fraudulentamente sistemas de información o redes electrónicas agregando 2 artículos después del Art. 553 del Código Penal; mediante el Art. 63 se sanciona la estafa utilizando medios electrónicos o telemáticos agregando un segundo inciso al Art. 563 del Código Penal, y finalmente se tipifica como contravención de tercera clase los que violaren el derecho a la intimidad en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos agregando un numeral al Art. 606 del Código Penal.

Capítulo 6

Análisis de casos de estudio que podrían constituir una amenaza a la libertad de expresion en línea.

6.1. WikiLeaks.

WikiLeaks es una organización registrada como WikiLeaks.org el 4 de octubre del 2006, fundada y liderada por Julian Assange, nacido el 3 de julio de 1971 en Townsville-Australia, programador, hacker, promotor de software libre y creador de programas de cifrado.

WikiLeaks es una plataforma cuyo objetivo es llevar noticias e información al público. Ofrecen una forma innovadora, segura y anónima para las fuentes de fugas de información a sus periodistas. WikiLeaks ha litigado y triunfado frente a los ataques legales y políticos diseñados para silenciar a su organización editorial, sus periodistas y sus fuentes anónimas. Ha combinado tecnologías de alta seguridad con periodismo y principios éticos. Aceptan fuentes anónimas proveyendo buzones de seguridad respaldados con tecnologías más avanzadas de encriptado de información. WikiLeaks ha liberado cronológicamente más de 100 archivos clasificados o restringidos del Departamento de Estado de los Estados Unidos sobre “políticas de detenidos” seguidas por más de 10 años, que incluye procedimientos de operación estándar de campos de detenidos de Irak y Cuba (Base de Guantánamo) y manuales de interrogación. WikiLeaks ha publicado desde noviembre del 2010, más de 250.000 cables filtrados de las embajadas de Estados Unidos, diario de guerra conteniendo 391.832 reportes de la

guerra y ocupación en Irak (registros de la guerra de Irak), diario de guerra de Afganisthan, un video militar de EE.UU clasificado titulado “matanza colateral” tomado desde el puesto de tiro del cañón a bordo de un helicóptero Apache y que muestra una matanza indiscriminada de una docena de personas en un suburbio iraquí de Nueva Bagdad, incluidos 2 periodistas de la Agencia Reuters y algunos otros documentos secretos.
(http://wikileaks.org/About.html, visto el 20 de marzo del 2013)

Domscheit-Berg (2011, ps. 251-252), quien durante dos años y medio (2007 al 2010) fue el principal colaborador de Julian Assange y portavoz de WikiLeaks bajo el seudónimo Daniel Schmitt, señala que entre las primeras publicaciones de WikiLeaks se cuentan las efectuadas en: noviembre del 2007, sobre los manuales de la Bahía de Guantánamo; enero del 2008, de cientos de documentos sobre la sucursal del banco Sueco Julius Bär en las Islas Caiman; marzo de 2008, la Biblia secreta de la Cienciología; mayo del 2008, el primer manual de una hermandad estudiantil americana; diciembre del 2008, documentos del Servicio de Inteligencia Federal sobre la lucha contra la corrupción en Kosovo y la colaboración con los medios alemanes; marzo del 2009, el banco de datos de los patrocinadores del senador Coleman de los Estados Unidos; 6.700 informes del Servicio de Investigación del Congreso de Estados Unidos; noviembre del 2009, mensajes de buscapersonas del 11-S; contratos de Toll Collect (peaje para camiones) en Alemania; expediente contra una empresa farmacéutica alemana; diciembre del 2009, el informe Feldjjäger sobre el bombardeo de dos vehículos cisterna en Kudus, Afganistan.

Domscheit-Berg (2011, p. 148) manifiesta que el 5 de abril del 2010 se publicó el documental *asesinato colateral* y que solo en YouTube se llegó a diez millones de reproducciones. Manifesta el autor que el video que muestra cómo unos soldados norteamericanos disparaban contra civiles iraquíes desde un helicóptero militar y que

cobró la vida de 2 periodistas de Reuters, constituyó la consagración de WikiLeaks. Agrega Domscheit-Berg, que los soldados norteamericanos también disparaban contra los civiles que se bajaron de un minibús para auxiliar a los dos periodistas y al resto de víctimas y que "los comentarios cínicos que acompañaban sus disparos provocaron la indignación del mundo y ofrecieron una imagen real de algo que se vendía como una guerra que limpia".

Domscheit-Berg (2011, p. 150) expresa que el peor momento de la historia de WikiLeaks fue la detención en mayo del 2010 del analista de inteligencia Bradley Manning, que estuvo destacado en Irak, acusado por el Gobierno de Estados Unidos de haber extraído de los servidores del ejército estadounidense el video utilizado en el documental *asesinato colateral*.

El 20 de agosto del 2010, en Suecia se formuló una acusación contra Julian Assange por dos casos de tentativa de violación y se emitió una orden de captura que poco después es retirada.

Domscheit-Berg (2011, ps. 218-227) señala que el 22 de octubre del 2010 WikiLeaks publicó 391.832 documentos sobre la guerra en Irak, que se trataban de documentos militares del período comprendido entre 2004 y 2009 y que a partir del 28 de noviembre del 2010 publicó comunicaciones secretas entre 274 embajadas norteamericanas de todo el mundo y el Departamento de Estado desde 1996 hasta finales de febrero del 2010, creando especialmente para el efecto, la página *cablegate.org.*

Domscheit-Berg (2011, p. 235) comenta los intentos de Estados Unidos de llevar a Assange y a otros colaboradores de WikiLeaks a la justicia para impedir futuras publicaciones, y menciona que podría ser encausado en EE.UU en virtud de la llamada Ley de Espionaje, para lo cual el Ministerio de Justicia debería demostrar que Assange

actuó con la intención de hacer daño a los Estados Unidos. El Departamento de Estado intenta demostrar que Julian Assange tuvo una participación activa en la adquisición de la información de la información del video de *asesinato colateral* y poder acusarlo de cómplice del soldado Mannning, quién aún no ha sido juzgado. Domscheit-Berg opina que "nadie debería ser perseguido por haber proporcionado información al público, ya se trate de un informador o de una plataforma de noticias confidenciales como WikiLeaks".

El 1 de diciembre del 2010 Interpol emitió una Red Notice, que es una orden de captura internacional, contra Julian Assange; en la Red Notice se puede leer que la categoría de ofensa por la que es requerido por la Oficina Internacional de Enjuiciamiento Público de Gotemburgo-Suecia, es delito sexual (sex crime). El 7 de diciembre Assange se entregó detenido a la Policía de Londres y el 14 de diciembre del 2010 fue puesto en libertad bajo fianza.

Julian Assange, ante un pedido de extradición solicitado por Suecia ante la Corte Suprema Británica que había fallado a favor de este pedido y negado una posterior apelación el 30 de mayo del 2012, se refugió el 19 de junio del 2012 en la Embajada de Ecuador en Londres y pidió asilo diplomático al Gobierno de Ecuador denunciando mediante una carta dirigida al Presidente Rafael Correa, una persecución en su contra. La preocupación de Assange es que una vez que se encuentre en Suecia, el Gobierno de Estados Unidos pueda solicitar su extradición y ser juzgado por espionaje en este país.

El 16 de agosto del 2012 el Gobierno del Ecuador aceptó dar asilo diplomático a Julian Assange, pero Gran Bretaña se ha negado a otorgar el salvoconducto respectivo para que pueda salir hacia el Ecuador.

En una alocución dirigida a más de un centenar de periodistas el 20 de agosto del 2012, desde el balcón de la Embajada del Ecuador pidió al Presidente Obama hacer "lo

correcto" y que "Estados Unidos debe renunciar a su caza de brujas contra WikiLeaks", agregando que Estados Unidos podría llevar al mundo a una era de opresión al periodismo. Agregó que los Estados Unidos "deben comprometerse ante el mundo a que no perseguirá a los periodistas por arrojar luz sobre los crímenes secretos de los poderosos". Agradeció al Ecuador por la valentía demostrada al concederle el asilo. El abogado defensor de Assange es el ex Juez español Baltazar Garzón. (Diario El Universo, edición del 20 de Agosto del 2012)

Después de analizar el presente caso de estudio, independientemente de las investigaciones que realice la fiscalía Sueca respecto a las acusaciones contra Julian Assange y los resultados a los que pueda arribar que ocasionen o no su juzgamiento, se presentan indicios de que podría existir una amenaza a la libre expresión en Internet al generarse una represión contra los informantes de WikiLeaks y para dicha organización, con el propósito de ejercer una medida de coerción que evite futuras publicaciones de documentos secretos filtrados, como es la situación de la detención de Manning y una supuesta intención de extraditar a Assange a los Estados Unidos para ser juzgado por espionaje.

6.2. Espionaje cibernético en China.

Como vimos en 4.1, China fue considerado en el año 2012 un país "no libre" en el uso de Internet (Fredoom House) y como "enemigo de Internet" (Reporteros sin Fronteras).

Moloney, et al. (2011, ps. 4 a 9) afirman que China tiene el mayor número de usuarios de Internet en el mundo, estimado en 330 millones incluyendo a 70 millones de blogueros, pero también tiene la censura más sofisticada y agresiva del mundo. Sostienen los autores que el Gobierno de la República Popular China emplea una variedad de métodos de control de expresiones y contenidos en línea, entre los que se

incluye el bloqueo de sitios web y filtraje de palabras claves; regulando y monitoreando a los proveedores de servicio de Intenet, cibercafés y sistemas de boletines electrónicos universitarios; registrando websites y blogs; y realizando arrestos ocasionales de "ciberdisidentes" de alto perfil. Los bloqueos de sitios web, sitios de redes sociales y sitios para compartir archivos incluyen a Radio Free Asia, los sitios web internacionales de derechos humanos, muchos de los periódicos taiwaneses, Facebook, Twitter, y YouTube.

Moloney, et al. observan que algunos activistas de derechos humanos y algunos responsables de la elaboración de las políticas norteamericanas, han expresado su preocupación en que compañías de Estados Unidos dedicadas al negocio de Internet, han vendido a China servicios de Internet o tecnologías que han apoyado al Gobierno de la República Popular China en restringir información y comunicación y en el monitoreo e identificación de usuarios de Internet.

Los autores comentan que grupos de vigilancia de medios de información y congresistas norteamericanos han sostenido que algunas compañías americanas de tecnologías de información como Yahoo!, Microsoft, Google y Sistemas Cisco han proporcionado directa y sostenidamente, colaboración a los esfuerzos del Gobierno Chino para el control político y censura en Internet. En efecto, explican los autores, Yahoo! ha sido acusado por complicidad en el arresto de al menos 4 usuarios chinos de Internet por proveer información de su cuenta de correo electrónico a las autoridades del Gobierno Chino. En el 2005, Microsoft cerró en el sitio MSN Spaces la cuenta del bloguero político Zhao Jing (conocido como Michael Anti) ante el requerimiento del Gobierno Chino, después que de Zhao había expresado su apoyo en su blog para un boicot a *Beiging News* por el arresto de uno de sus editores. Activistas de derechos humanos también han criticado a Microsoft por bloquear palabras tales como "democracia" de MSN Space. Recientemente, Microsoft también ha sido acusada de colaborar con las

políticas de censura de China en el desarrollo de su nuevo motor de búsqueda *Bing*. Las actividades de Google en China han reflejado un intento de la compañía en cumplir con las políticas del Gobierno Chino, mientras limita su rol en la censura; cabe mencionar que el motor de búsqueda de Google China, es el segundo más ampliamente utilizado en China, después de *Baidu*, una compañía China. En junio del 2009 el ministro de Relaciones Exteriores de China acusó a Google de violar la Ley China por permitir a los usuarios de Internet de su país a accesar a "contenidos vulgares" y el servicio de Google China fue interrumpido por unos pocos días, lo cual fue visto por algunos analistas como una respuesta del Gobierno a una evidente resistencia de someterse a nuevas disposiciones de censura. En enero del 2010, Google amenazó con dejar de censurar su motor de búsqueda o terminar sus operaciones en China, habiendo afirmado que en diciembre de 2009, hackers chinos habían atacado su servicio Gmail y su red corporativa, así como los sistemas informáticos de muchos otras grandes corporaciones norteamericanas en China.

Dutton, et al. (2011, p. 69) comentan que en marzo del 2010, Google suspendió la censura en su servicio de búsqueda. A partir de entonces los usuarios de Internet que visitaban *Google.cn* eran derivados a *Google.com.hk*, donde Google ofrece resultados de búsquedas no censuradas, entregados vía servidores alojados en Hong Kong en idioma chino simplificado. Como la restricción China de los contenidos no aplica a los servicios en Hong Kong, Google siente que esta solución era consistente con la Ley China. China aparentemente acepta esta solución.

Moloney, et al. agregan, de acuerdo con algunos reportes, que Cisco Systems ha vendido a China algunos miles de servidores, lo cual contribuyó a facilitar al Gobierno Chino la censura de contenidos en Internet y monitorear a usuarios de Internet. Según otros informes, Cisco vendió tecnologías a la fuerza policial de China que puede ser usada

para la recolección y uso de información de datos personales e imágenes, historia de navegación en la web y correos electrónicos.

Manifiestan los autores que durante la visita efectuada a China en noviembre del 2009, el Presidente Barack Obama expresó su apoyo a un acceso a Internet sin restricciones y su desaprobación a la censura. En enero del 2010, la ex secretaria de Estado Hillary Clinton, en un discurso sobre la libertad de Internet, urgió a las compañías norteamericanas a oponerse a la censura en sus operaciones en el exterior y anunció que la Global Internet Freedom Task Force (Fuerza de Trabajo de Libertad Global de Internet) sería revigorizada; ella pidió también al Gobierno Chino que realice una investigación de los ciberataques sufridos en diciembre del 2009 por las compañías norteamericanas en China y transparente sus resultados.

Faris y Villenueve (2011, p. 14) afirman que China usa el bloqueo IP para obstruir el acceso a por lo menos 300 direcciones IP. Este bloqueo es efectuado a nivel de puertos internacionales, lo cual afecta a todos los usuarios de las redes de sus respectivos ISPs. El bloqueo de direcciones IP entre los dos proveedores troncales, China Netcom y China Telecom, son significativamente similares.

El Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, observa en su informe de mayo del 2011, que el gobierno de China exige a los proveedores de servicios de Internet y a las plataformas web que vigilen a sus usuarios, y los consideran directamente responsables del contenido subido por los usuarios. Las empresas que incumplen esta obligación se exponen a perder su licencia comercial. La Rue expresa que esta exigencia a los intermediarios menoscaba gravemente el disfrute del derecho a la libertad de opinión y de expresión por parte de los usuarios de Internet, pues da lugar a una censura privada de autoprotección excesivamente amplia, a menudo sin transparencia y sin las debidas

garantías procesales. Cabe mencionar que se consideran intermediarios, desde los proveedores de servicios de Internet a los motores de búsqueda, y desde los servicios de blogs a las plataformas de comunidades en línea.

Se puede concluir con el análisis efectuado de este caso de estudio, que los usuarios de Internet en la República Popular China no gozan plenamente de una libertad de expresión en línea, pues están expuestos a controles que permiten identificarlos y sufrir represiones, así como también experimentan filtrajes y bloqueos de sitios web que desde el punto de vista del gobierno Chino, atentan contra su seguridad interna.

6.3. Situación política en Medio Oriente.

En el período 2010 al 2013 se han producido una serie de movimientos sociales en los países árabes, conocida como la "primavera árabe", y que desembocaron en seis rebeliones populares: Túnez, Egipto, Libia, Bahréin, Siria y Yemen. Estas revueltas populares se iniciaron con la inmolación de Mohamed Bouazizi el 17 de diciembre del 2010, un vendedor ambulante que se incineró frente a la sede de la Gobernación de Sidi Buzid, en Túnez, en protesta por las graves condiciones económicas que afectaban el país y por la represión policial, cuando el pueblo reclamaba porque se mejoren sus condiciones de vida, exigiendo equidad, trabajo, justicia social y un cambio democrático. El país estaba gobernado por Zine El Abidine, dictador y presidente de la República desde 1987.

Reporteros sin Fronteras (2011, ps. 4 a 5) manifiesta que la muerte de Bouazizi, desencadenó una ola de ira popular contra las fuerzas del orden. Las autoridades impusieron un silencio mediático total. Reseña, Reporteros sin Fronteras, que frente al silencio de los medios de comunicación tradicionales, Facebook y Twitter tomaron el relevo. Utilizado por una cuarta parte de la población, Facebook acogió comentarios, fotos y videos de los acontecimientos. Los videos de aficionados tomados con cámaras

fotográficas digitales fueron durante tres semanas las únicas imágenes a las que tuvieron acceso los tunecinos y el resto del mundo. En Twitter, el hashtag #sidibouzid fue difundido por los usuarios tunecinos, árabes y occidentales, mostrando un movimiento de solidaridad que llegó a ser internacional. A partir de enero del 2010 las autoridades reforzaron la censura en Internet; Facebook fue censurada por primera vez durante varios días; los sitios en los que se difundían videos, como Flickr, YouTube, Dailymotion y Vimeo, estaban bloqueados desde hacía meses. La policía también emprendió una campaña para piratear las cuentas Facebook con el fin de conocer las contraseñas de activistas e infiltrarse en las redes de periodistas ciudadanos, formadas en torno a los acontecimientos de Sidi Buzid. Numerosas cuentas de correo electrónico fueron pirateadas.

La revuelta tunecina obligó al ex presidente Ben Ali a dejar el poder el 14 de enero de 2011 y a huir del país. Este movimiento se propagó rápidamente a través de países de la región. El nuevo gobierno anunció la total libertad de información y de expresión como principio fundamental de su gestión.

Añade Reporteros sin Fronteras (2011, p. 6) que animados por la revolución tunecina, los egipcios salieron a las calles el 25 de enero de 2011, con ocasión del "Día de la Policía" protestando contra el régimen de Hosni Mubarak que gobernaba el país desde hace 30 años. Comenta Reporteros sin Fronteras, que ese mismo día, Twitter fue bloqueado, así como el sitio de streaming denominado *bambuser.com*. El hashtag *#jan25*, en referencia al primer día de las manifestaciones, circuló ampliamente en la red social. El 26 de enero el acceso a Facebook fue altamente restringido. Se registraron problemas de disminución de la velocidad de conexión de Internet. La noche del 27 de enero de 2011 las autoridades egipcias cortaron las redes de Internet y de la telefonía móvil; sin embargo los netciudadanos encontraron varias formas de usar twitter y subir videos a YouTube. Google y Twitter se asociaron en la lucha contra la censura

instalando una aplicación que permitía convertir los mensajes vocales en tweets y también se usaron los medios tradicionales de telecomunicaciones. El servicio de Internet se restableció el 2 de febrero de 2011, luego de 5 días de bloqueo. Después de 18 días de violentas represiones, el 11 de febrero del 2011 Hosni Mubarack abandonó el poder y se instaló un Consejo Supremo de las Fuerzas Armadas.

Reporteros sin Fronteras (2011, p. 8) comenta que inspirados por las revoluciones tunecinas y egipcias, la insurrección libia comenzó el 15 de febrero de 2011 en Bengasi. Los revolucionarios libios se tomaron Trípoli meses más tarde, a finales de agosto de 2011, poniendo fin al régimen de Muamar el Gadafi, quien fue asesinado el 20 de octubre del 2011. A medida que las noticias sobre la caída de dictadores en Túnez y en Egipto se difundían en el territorio libio, se propagaban en Facebook las llamadas a protestar. Entonces, el acceso a las redes sociales empezó a registrar serias perturbaciones. Ante la ausencia de medios de comunicación internacionales, los ciudadanos libios improvisaron la labor informativa con la ayuda de sus teléfonos móviles y cámaras fotográficas, tomando imágenes de las manifestaciones y de la represión. El régimen perturbaba fuertemente la Red con la ayuda del principal proveedor de acceso a Internet, cuyo propietario era Mohamed Gadafi, uno de los hijos de Muamar el Gadafi. Todas las conexiones telefónicas, las líneas fijas y móviles, habrían sido suspendidas alrededor del 21 de febrero del 2011.

También las protestas pro-democráticas llegaron a mediados de febrero del 2011 al país Bahréin, de apenas 1,2 millones de habitantes, observa Reporteros sin Fronteras, donde las autoridades se esfuerzaron por controlar la información sobre las manifestaciones, produciéndose detenciones de netciudadanos y blogueros. El 9 de abril de 2011, el netciudadano Zakariya Rashid Hassan murió cuando se encontraba detenido, probablemente tras haber sido torturado, siete días después de su arresto acusado por "incitación al odio", "publicación de noticias falsas", "promoción del sectarismo" y

“llamado al derrocamiento del régimen en los foros en línea”. Su crimen: haber administrado un foro de discusión.

Reporteros sin Fronteras (2011, p. 12) menciona que en marzo del 2011 los sirios, inspirados por sus vecinos tunecinos y egipcios, salieron a las calles para reclamar cambios democráticos. El régimen de Bachar Al-Assad ha respondido con violencia a este movimiento de protesta, limitando la movilización y la transmisión de imágenes y videos; el régimen realizó de manera regular cortes temporales de las redes de telecomunicaciones (telefonía móvil e Internet) en las localidades donde transcurrían las manifestaciones. Los medios de comunicación y las ONGs trataron de remediarlo distribuyendo teléfonos celulares satelitales entre ciertos habitantes de ciudades de difícil acceso o blanco de cortes frecuentes de la red. El ejército persiguió a los ciberdisidentes en las redes sociales, crearon cuentas de Twitter para parasitar la información proporcionada por el hashtag #Syria, enviando cientos de tweets cuyas palabras clave condujeron a resultados deportivos o fotos satelitales del país.

Reporteros sin Fronteras (2011, p. 14) destacó que el movimiento de protesta pro democrática en Yemen comenzó el 11 de febrero de 2011, cuando los yemeníes salieron a las calles de Sanaa para celebrar la caída del presidente egipcio Hosni Mubarak y reclamar la dimisión de su gobierno. El presidente Ali Abdallah Saleh endureció las medidas en vigor con el fin de impedir la difusión de imágenes de la represión y de imponer una censura total.

Argelia, Jordania y Líbano también han sido escenario de protestas pro democráticas ante un descontento generalizado por actos de corrupción, despotismo, injusticias, desigualdades sociales y graves problemas económicos.

Se puede concluir de este caso de estudio que, Internet y las redes sociales han jugado y están jugando un rol fundamental en la primavera árabe, para que las personas puedan manifestar su insatisfacción por la violación de sus derechos fundamentales; y que, los gobiernos han utilizado medios de bloqueo y persecución a los usuarios de Internet como una de las formas de controlar los actos de protesta; incluyendo el bloqueo de las versiones en línea de los periódicos o los sitios informativos independientes. Todo esto demuestra que, la libertad de expresión en línea, ha sido vulnerada en los países donde se han producido las protestas pro democráticas a la que se ha referido en esta sección.

Después del análisis efectuado de los 3 casos de estudio propuestos en este capítulo, que ha permitido conocer con un significativo detalle las formas de filtraje, bloqueo de sitios web y de redes sociales, vigilancia y represión de usuarios de Internet, que se practican lamentablemente en países donde se censura Internet, se puede concluir que no se vislumbra que en los próximos años exista libertad de expresión en línea en todos los países del mundo.

Capítulo 7

Libertad de expresión en línea en el Ecuador.

7.1. Derechos a la libertad de expresión consagrados en la Constitución de la República.

Se realizará un análisis de la Constitución de la República del Ecuador vigente desde su publicación en el Registro Oficial No. 449 del 20 de octubre del 2008, para determinar todos los preceptos constitucionales donde se consagran los derechos a la libertad de expresión y al acceso a las tecnologías de la información y la comunicación que es el medio para gozar de una libertad de expresión en línea y para construir la Sociedad de la Información en el país.

La primera mención se la encuentra en el artículo 11, numeral 3, que dispone que los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos, serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte. Se ha analizado detalladamente en el Capítulo 3 de la presente tesis que la libertad de expresión está consagrada en varios instrumentos internacionales tales como la Declaración Universal de los Derechos Humanos, el Convenio Internacional sobre los Derechos Civiles y Políticos y en la Convención Americana sobre Derechos Humanos. Se ha concluido también, en el desarrollo del Capítulo antes mencionado, que la comunidad internacional ha reconocido que la libertad de expresión se aplica a Internet, del mismo modo que a todos los medios de comunicación, garantizada por la normativa internacional de los derechos humanos. Se puede establecer por lo tanto que el numeral

3 del artículo 11 de la Constitución ecuatoriana, garantiza la libertad de expresión y por consecuencia la libertad de expresión en línea.

Una referencia expresa al derecho de la libre expresión en Internet y al derecho de acceso o conexión a Internet, se puede encontrar en los artículos 16, 17, 18 y 20 del Capítulo segundo "Derechos del buen vivir" del Título II "Derechos".

En efecto, el artículo 16 dispone que todas las personas, en forma individual o colectiva, tengan derecho al acceso universal a las tecnologías de información y comunicación, a la creación de medios de comunicación social, y al acceso y uso de todas las formas de comunicación visual, auditiva y sensorial. Se consagra en este artículo, el derecho al acceso a Internet para todos los ecuatorianos. Es oportuno mencionar que el Plan del Buen Vivir 2009–2013 hace mención que la Constitución, dentro de los derechos del "Buen Vivir" reconoce a todas las personas, en forma individual o colectiva, el derecho al acceso universal a las tecnologías de información y comunicación, y pone énfasis en aquellas personas y colectividades que carecen o tengan acceso limitado a dichas tecnologías, y obliga al Estado a "incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales". Se manifiesta también que el Estado debe asegurar que la infraestructura para conectividad y telecomunicaciones cubra todo el territorio nacional de modo que las TICs estén al alcance de toda la sociedad de manera equitativa. Aunque las alternativas de conectividad son varias (wireless, satélite, fibra óptica), la garantía de la tecnología más adecuada, debe propiciarse desde la identificación de los requerimientos de los beneficiarios. El Plan del Buen Vivir proclama que, "*La construcción de la Sociedad del Buen Vivir tiene implícito el tránsito hacia la Sociedad de la Información y el Conocimiento, pero considerando el uso de las TICs, no solo como medio para incrementar la productividad del aparato productivo, sino como instrumento para generar igualdad de oportunidades, para fomentar la*

participación ciudadana, para recrear la interculturalidad, para valorar nuestra diversidad, para fortalecer nuestra identidad plurinacional; en definitiva, para profundizar en el goce de los derechos establecidos en la Constitución y promover la justicia en todas sus dimensiones".

El artículo 17, Numeral 2, señala que el Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada. Es decir ratifica el derecho al acceso al Internet y al fomentar la pluralidad de la comunicación, podemos colegir que la creación de periódicos en línea, foros de discusión y todo medio de difusión mediante el uso de las redes sociales, está garantizada por este artículo.

El artículo 18 expresa que todas las personas, en forma individual o colectiva, tienen derecho a buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior y acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información. Es obvio que este artículo garantiza la libertad de expresión sin censura, con la condición de que cuando se produzca información esta sea responsablemente generada. Igualmente se consagra en este artículo la libertad de información a la que tienen derecho los ciudadanos ecuatorianos.

El artículo 20, a su vez, dispone que el Estado garantizará la cláusula de conciencia a toda persona, así como el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación. Se puede concluir que, el derecho a la privacidad en Internet está incluido en este precepto constitucional.

El artículo 66, Numeral 6 del Capítulo Sexto "Derechos de libertad" del mismo Título II "Derechos", reconoce y garantiza a las personas el derecho a opinar y expresar su pensamiento libremente y en todas sus formas y manifestaciones. El Numeral 7 de este artículo, reconoce y garantiza el derecho de toda persona agraviada por informaciones sin pruebas o inexactas, emitidas por medios de comunicación social, a la correspondiente rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario. El Numeral 19 a su vez, reconoce y garantiza el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. Finalmente el Numeral 21, reconoce y garantiza el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación. Es evidente que, los preceptos antes detallados, consagran el derecho a la protección de datos y el derecho a la intimidad o privacidad que es un elemento fundamental para la libre expresión personal.

Es oportuno comentar como un paréntesis al análisis que se ha realizado sobre los artículos 16 y 66 de la Constitución, la preocupación que ha producido a los usuarios de Internet en el Ecuador, la expedición por parte del Consejo Nacional de

Telecomunicaciones (CONATEL) mediante Resolución No. TEL-477-16-CONATEL-2012 del 11 de julio del 2012, del "Reglamento para los Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y Valor Agregado", publicado en el Suplemento del Registro Oficial 750 del 20 de julio del 2012. A pesar de invocarse en los "Considerandos", precisamente, el mandato de los artículos 16 y 66 de la Constitución a la que se ha referido anteriormente, incluye en el artículo 29.9 como una de las obligaciones de los prestadores de servicios de telecomunicaciones y de valor agregado de Internet, el remitir a solicitud de la Superintendencia de Telecomunicaciones, información relativa a direcciones IP asignadas a sus abonados/clientes-usuarios, en los plazos, términos y condiciones establecida por dicha entidad para el efecto. Esta disposición atenta contra la privacidad de los usuarios de Internet, contraviniendo este derecho consagrado en la Constitución justamente en los artículos invocados en los considerandos del Reglamento, pues sin la necesidad de utilizar ninguna herramienta sofisticada de software, como se practica en los países en los cuales la libertad de expresión en Internet no está garantizada, el Estado puede identificar con facilidad y reprimir a cualquier usuario que desde su punto de vista atente contra la seguridad del país. Aún más, se contrapone con lo dispuesto en los artículos 14 y 39 de la propia Ley Reformatoria de la Ley Especial de Telecomunicaciones, también invocados en los "Considerandos" del Reglamento de Abonados en mención, mediante los cuales se proclama que, el Estado garantiza el derecho al secreto y a la privacidad del contenido de las telecomunicaciones.

Cabe citar que en una entrevista concedida a Diario Hoy el 27 de julio del 2012, el Ing. José Pileggi, ex Presidente del CONATEL, al ser entrevistado respecto a la vigencia del Reglamento de Abonados y en particular al artículo 29.9, manifestó que "El acceso al IP, ya sea de parte del Estado o una persona, aunque no pueda acceder a la información, disminuye las defensas del usuario de los servicios de telecomunicaciones y valor agregado". Agrega el Ing. Pileggi, que la afectación radica en la discrecionalidad del usuario, pues no se sabe quién va a manejar toda esta información. Incluso se puede

crear una base de datos en la que conste la dirección IP del cliente y que esta pueda ser mal utilizada, tal como en ocasiones ocurre ahora con los correos no deseados que caen en la bandeja spam (basura). Considera el Ing. Pileggi que dicha disposición debe ser revisada, porque el propio Gobierno también se puede ver afectado. Comenta además el Ing. Pileggi, que "se debe tomar en cuenta que una dirección IP implica que una información pueda ser rastreada de manera más fácil. Supóngase, porque la atribución se la dan al propio superintendente, pero antes de ella debe pasar por terceras personas, ¿y si estas no son probas y quieren esa información?. Por lo tanto, este tema necesita ser aclarado lo más pronto posible para evitar confusiones".

En el artículo 91 de la Sección cuarta "Acción de acceso a la información pública", Capítulo tercero "Garantías jurisdiccionales" del Título III "Garantías Constitucionales" de la Constitución, se señala que la acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por la autoridad competente y de acuerdo con la ley. Se puede establecer que la libertad de información está ratificada mediante este artículo.

El artículo 384 de la Sección séptima "Comunicación Social", Capítulo primero "Inclusión social" del Título VII "Régimen del Buen Vivir", dispone que el sistema de comunicación social asegurará el ejercicio de los derechos de la comunicación, la información y la libertad de expresión, y fortalecerá la participación ciudadana. El sistema se conformará por las instituciones y actores de carácter público, las políticas y la normativa; y los actores privados, ciudadanos y comunitarios que se integren voluntariamente a él. El Estado formulará la política pública de comunicación, con

respeto irrestricto de la libertad de expresión y de los derechos de la comunicación consagrados en la Constitución y los instrumentos internacionales de derechos humanos. La ley definirá su organización, funcionamiento y las formas de participación ciudadana. Puede apreciarse que este artículo establece el marco legal del sistema de comunicación social del Ecuador, donde está inserto el derecho fundamental de la libertad de expresión, plasmado no solo en artículos precedentes de la Constitución, sino también en los instrumentos jurídicos internacionales a los que se ha hemos referido con detalle en el Capítulo 3 de la presente tesis.

El artículo 387, Numeral 1, de la Sección octava "Ciencia, tecnología, innovación y saberes ancestrales", Capítulo primero "Inclusión social" del Título VII "Régimen del Buen Vivir", señala que será responsabilidad del Estado, facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo. Podemos establecer que mediante este artículo, el Estado se compromete a cumplir el mandato de la Cumbre Mundial de la Sociedad de la Información, que se basa en el respeto pleno y en la defensa de los derechos humanos universales, y en cuya implementación, las tecnologías de la información y la comunicación se constituyen en la herramienta fundamental para construir la Sociedad de la Información.

Del análisis efectuado se puede concluir categóricamente que, en la Carta Magna del Ecuador, está garantizado el derecho de todos los ecuatorianos y ecuatorianas para gozar plenamente de la libertad de expresión, libertad de acceso a Internet, libertad de Internet, libertad de información, a la privacidad o intimidad y a la protección de datos personales.

7.2. Análisis de la nueva Ley Orgánica de Comunicación y las amenazas contra la libertad de expresión en línea.

De acuerdo con el contenido del artículo 384 de la Constitución analizado en 7.1, el Estado formulará la política pública de comunicación, con respeto irrestricto de la libertad de expresión y de los derechos de la comunicación consagrados en la Constitución y los instrumentos internacionales de derechos humanos.

La Disposición Transitoria Primera, Numeral 3, de la Constitución de la República del Ecuador dispone que, en el plazo máximo de trescientos sesenta días contados desde su puesta en vigencia, se deberá aprobar la Ley de Comunicación. Este plazo se venció el 20 de octubre del 2009.

La Ley Orgánica de Comunicación fue aprobada por la Asamblea Nacional el 14 de junio del 2013 y entró en vigencia cuando fue publicada en el Tercer Suplemento del Registro Oficial No. 22 del día martes 25 de junio del 2013.

Se hará a continuación el análisis del contenido de esta Ley con el fin de determinar si sus disposiciones constituyen una amenaza a la privacidad y protección de datos de los usuarios de Internet.

El artículo 4 titulado “Contenidos personales en Internet” expresa que esta ley no regula la información u opinión que de modo personal circule por Internet, pero que esta disposición no excluye las acciones penales o civiles a las que haya lugar por las infracciones a otras leyes que se cometan a través del Internet. Esta disposición excluye del ámbito de la Ley Orgánica de Comunicación los contenidos personales difundidos por Internet más no las publicaciones en línea que efectúen los medios de comunicación social.

El artículo 5 señala que para efectos de la Ley Orgánica de Comunicación, se considera medios de comunicación social a las personas, empresas y organizaciones públicas, privadas y comunitarias, que prestan el servicio público de comunicación masiva usando como herramienta medios impresos o servicios de radio, televisión y audio por suscripción, cuyos contenidos pueden ser generados o replicados por el medio de comunicación a través de internet. Este contenido confirma el comentario efectuado respecto al artículo 4.

El artículo 18 señala que "queda prohibida la censura previa por parte de una autoridad, funcionario público, accionista, socio, anunciante o cualquier otra persona que en ejercicio de sus funciones o en su calidad revise, apruebe o desapruebe los contenidos previos a su difusión a través de cualquier medio de comunicación, a fin de obtener de forma ilegítima un beneficio propio, favorecer a una tercera persona y/o perjudicar a un tercero. Los medios de comunicación tienen el deber de cubrir y difundir los hechos de interés público. La omisión deliberada y recurrente de la difusión de temas de interés público constituye un acto de censura previa. Quienes censuren previamente o ejecuten actos conducentes a realizarla de manera indirecta, serán sancionados administrativamente por la Superintendencia de la Información y Comunicación con una multa de 10 salarios básicos unificados, sin perjuicio de que el autor de los actos de censura responda judicialmente por la comisión de delitos y/o por los daños causados y por su reparación integral". La determinación de cuáles son los temas de interés público que deben ser difundidos podría ser un acto discrecional por parte del Superintendente de la Información y Comunicación. De darse la censura previa, ésta también se aplicaría a las ediciones en línea de los medios de comunicación social.

En el artículo 19 se define "responsabilidad ulterior" como "la obligación que tiene toda persona de asumir las consecuencias administrativas posteriores a difundir contenidos que lesionen los derechos establecidos en la Constitución y en particular los derechos de

la comunicación y la seguridad pública del Estado, a través de los medios de comunicación."

El artículo 20 señala que, los comentarios formulados al pie de las publicaciones electrónicas de los medios de comunicación legalmente constituidos, serán responsabilidad personal de quienes lo efectúen, a menos que los medios omitan, entre otras acciones, generar mecanismos de registro de datos personales que permitan su identificación, como nombre, correo electrónico, cédula de ciudadanía o identidad.

El análisis conjunto de los artículos 5, 18, 19 y 20 permite establecer que puede configurarse una amenaza a la privacidad y protección de datos de los usuarios de Internet, aunque no en las redes sociales, pero sí en los medios de comunicación social en línea. En algunos Estados los gobiernos han esgrimido la salvaguarda de la seguridad interna del país como justificación de medidas de filtraje, identificación y represión de ciberciudadanos y en el bloqueo de las versiones en línea de los medios de comunicación social.

El artículo 35 titulado "Derecho al acceso universal a las tecnologías de la información y comunicación" dispone que todas las personas tienen derecho a acceder, capacitarse y usar las tecnologías de información y comunicación para potenciar el disfrute de sus derechos y oportunidades de desarrollo". Uno de los derechos embebidos en la Sociedad de la Información es precisamente el disfrute de los derechos humanos, en particular de la libertad de expresión y por ende de la libertad de expresión en línea. Se puede entonces concluir que, el texto de este artículo puede ser utilizado para defender implícitamente el derecho de la libertad de expresión en línea y puede considerarse como una garantía y no una amenaza.

Cabe mencionar que el 28 de junio del 2013 ha sido presentada ante la Corte Constitucional una demanda de inconstitucionalidad de la Ley Orgánica de Comunicación, la misma que se encuentra en trámite.

Es oportuno mencionar que en la evaluación sobre el estado de la libertad de expresión en Ecuador contenida en 30 páginas en el Informe Anual 2012 de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), se establece que existe un caso que tienen relación con la libertad de expresión en línea. La observación No. 195 manifiesta que la Relatoría Especial ha sido informada que el Secretario Nacional de Comunicación mediante misiva enviada a diario El Comercio le habría advertido el 18 de septiembre del 2012 sobre su intención de iniciar investigaciones penales en razón de comentarios publicados en la versión *online* del diario, y que se "reservaba el derecho de solicitar la información de las personas cuyos comentarios pueden ser difamatorios, ofensivos o lesivos y que puedan configurar en algún delito, para lo cual la Justicia será la que determine la responsabilidad de la persona y de ser el caso el resarcimiento por los daños y perjuicios ocasionados". A raíz de esta comunicación, el diario El Comercio habría suprimido la opción de comentarios en su sitio Web.

7.3. Aplicación del método Delphi.

Entre las principales razones por las cuales se seleccionó el método Delphi para validar las hipótesis planteadas en la presente investigación, se pueden citar las siguientes:

- No se disponen de datos nacionales concernientes a las preguntas de investigación para su análisis respectivo.
- Se requiere convalidar el análisis efectuado por la autora, basado en el marco conceptual, en el análisis de datos secundarios y en la revisión de casos de

estudio, con la opinión de un grupo de personas que disponen de un elevado conocimiento de la materia investigada.

- La encuesta se realiza de una manera anónima pues ningún experto conoce la identidad de los demás miembros del grupo, con lo cual se evita los efectos de líderes.
- La utilización del correo electrónico facilita el envío del cuestionario a los expertos y la recepción de sus respuestas, en tantas rondas como sea necesario.
- No se precisa la presencia física de los expertos para realizar la encuesta, cuyo tiempo disponible es generalmente limitado.

7.3.1. Elección de los miembros del grupo de expertos.

A fin de alcanzar un valor de confiabilidad aceptable de Cronbach's Alpha $\rho = 0.8$ de acuerdo con la Figura en 2.3, se decidió integrar el grupo de expertos con 11 miembros, todos ellos con una gran experiencia en el tópico de la presente investigación.

A continuación se detallará la hoja de vida resumida de cada uno de ellos:

1. **Eric Samson**

   Licenciado en Periodismo y Ciencias de la Información del Centro Universitario de Enseñanza del Periodismo de la Universidad de Strasburgo - Francia. Máster en Periodismo Digital de la Universidad Autónoma de Madrid – España. Representante en el Ecuador de la Organización "Reporteros sin Fronteras". Reportero/talento de varias emisiones de los canales de TV franceses (France 2 y France 3) y de varias estaciones locales de Radio Francia. Corresponsal en el Grupo Andino de Naciones de Radio Francia Internacional, Radio Francia, Radio Canadá, Radio Suisse Romande, de los diarios franceses La Croix y Le Journal du Dimanche. Creador del blog "Periodismo Público AmLat" destinado a la promoción de la filosofía del Periodismo Público en el Ecuador y América Latina. Actual Coordinador de la

carrera de Periodismo Multimedios del Colegio de Comunicación y Artes Contemporáneas de la Universidad San Francisco de Quito, ex fundador y coordinador de la carrera de Medios Masivos de Comunicación del Colegio de Tecnologías Aplicadas y de la carrera de Comunicación Ambiental.

1. **José Pileggi Véliz**

Ingeniero en Electricidad. Magíster en Administración de Empresas (MBA). Cargos desempeñados: Presidente del Consejo Nacional de Telecomunicaciones (CONATEL). Presidente de la Comisión Interamericana de Telecomunicaciones (CITEL). Representante del Ecuador ante la Comisión de Autoridades Andinas de Telecomunicaciones (CAATEL). Miembro del Directorio de la Empresa Mundial de Satélites INTELSAT, en representación de Ecuador, Venezuela, México y Cuba. Presidente Fundador del Fondo para Desarrollo de Telecomunicaciones Rurales y Urbano marginales (FODETEL). Presidente Fundador de la Comisión Nacional de Conectividad del Ecuador. Presidente del Directorio de EMETEL. Presidente del Directorio de la Empresa Eléctrica Los Rios (EMELGUR). Miembro del Directorio de HIDROPAUTE S.A.. Director de la Comisión de Estudios para el Desarrollo de la Cuenca del Río Guayas (CEDEGE). Gerente General de Pileggi Construcciones Cia- Ltda. (actual). Fue Presidente del Colegio Regional de Ingenieros Eléctricos y Electrónicos del Litoral (CRIEEL).

2. **Paúl Rojas Vargas**

Ingeniero en Electrónica. Magíster en Gerencia de Redes y Telecomunicaciones. Cargos desempeñados: Superintendente de Telecomunicaciones. Miembro del Consejo Nacional de Radio y Televisión (CONARTEL). Gerente Técnico Nacional de Ecuatronix Cia. Ltda.. Gerente General de ADVICOM Cia. Ltda. (actual).

3. **Freddy Villao Quezada**

Doctor en Filosofía (Ph.D.) de la Universidad de Griffith – Australia (tesis doctoral: *Realization of the Asia – Pacific Vision of the Information Society in the APEC Member Economies*). Doctor en Jurisprudencia. Doctor en Diplomacia y Organizaciones Internacionales. Magíster en Ciencias Internacionales y Diplomacia. Abogado. Licenciado en Ciencias Sociales, Políticas y Económicas. Ingeniero en Electrónica. Cargos desempeñados: Gerente de IETEL R2. Director Principal del Directorio de PACIFICTEL S.A. Director Principal del Directorio de la Compañía Telecomunicaciones Móviles del Ecuador (TELECSA) S.A. Vicepresidente de Regulación e Interconexión de ANDINATEL S.A. Coordinador Nacional del CONATEL. Asesor del Fondo de Solidaridad. Asesor del Presidente Ejecutivo de ANDINATEL S.A. Asesor del Presidente del Directorio de TELECSA. Asesor del Rector de la ESPOL. Jefe del Departamento de Ayudas a la Navegación del Instituto Oceanográfico de la Armada (INOCAR). Profesor Titular Principal de la ESPOL y de la Universidad de Guayaquil (actual).

4. **Julio Martínez-Acosta**

Magíster en Derecho Económico. Abogado y Doctor en Jurisprudencia. Licenciado en Ciencias Sociales y Políticas. Cargos desempeñados: Secretario General del CONATEL. Director General Jurídico de la Secretaría Nacional de Telecomunicaciones (SENATEL). Coordinador Nacional del CONATEL. Secretario Nacional de Telecomunicaciones (E). Jefe de Asesoría Jurídica en el Ministerio de Educación. Subsecretario de Empleo y recursos Humanos del Ministerio del Trabajo. Ministro del Trabajo (E). Presidente del SECAP. Libre ejercicio profesional (actual).

5. **Octavio Roca de Castro**

Abogado. Magíster en Ciencias Internacionales y Diplomacia. Cargos desempeñados: Rector (E) de la Universidad del Pacífico. Decano de la Facultad de

Jurisprudencia de la Universidad del Pacífico. Asesor de la Contraloría General del Estado. Profesor del Instituto de Postgrado en Ciencias Internacionales "Dr. Antonio Parra Velasco" de la Universidad de Guayaquil. Profesor de la Academia de Guerra Naval. Procurador de la Universidad de Guayaquil (actual).

6. **Edgar Leyton Quezada**

Ingeniero Eléctrico con especialización en Electrónica. Cargos desempeñados: Director de Tecnologías de la Información del Ministerio de Telecomunicaciones y Sociedad de la Informacion (MINTEL). Director General de Gestión del FODETEL Intendente de Telecomunicaciones Región Costa de la Superintendencia de Telecomunicaciones. Gerente de ANDINATET S.A. Gerente Regional de SURATEL. Subgerente de Telecomunicaciones de BANRED S.A. Gerente Regional de PARADYNE S.A. Gerente Técnico y Supervisor de INFORMATICA S.A (FILANBANCO). Director de Inversiones del Ministerio Coordinador de los Sectores Estratégicos (MICSE) (actual).

7. **Carlos Horacio Galecio Samaniego**

Periodista y Licenciado en Comunicación Social. Maestrante de la UEES en Dirección y Gestión de Empresas de Servicios. Cargos desempeñados: Jefe Nacional de Información en Ecuavisa. Miembro de la Unidad Especial de Investigación en Diario El Universo. Editor de la sección Gran Guayaquil y redactor de las secciones Gran Guayaquil, Economía y Política en Diario El Universo. Premios internacionales por reportajes sobre biodiversidad. Director de Televistazo (Emisión estelar) en Ecuavisa (actual).

8. **María Elina Cedeño Pincay**

Licenciada en Comunicación Social. Maestrante de la UEES en Comunicación y Marketing. Cargos desempeñados: Redactora en Diario El Universo en las secciones

Política y Gran Guayaquil. Relacionista Pública en la Universidad de Especialidades Espíritu Santo (actual).

9. **Selene Johanna Vera Rodríguez**

Licenciada en Comunicación Social. Maestrante de la UDLA en Dirección de Comunicación. Cargos desempeñados: Cuatro años de experiencia en medios privados como reportera, redactora, fotógrafa y editora encargada en Radio City, El Universo y Metroquil. Cuatro años dedicados a la Comunicación Corporativa en el Municipio de Guayaquil. Community Manager en Interagua C. Ltda. (actual).

10. **Andrés Flores Soto**

Ingeniero en Ciencias Computacionales especialización Sistemas Tecnológicos. Cargos desempeñados: Administrador Web en ESPOL. Coordinador de Redes y Soporte Técnico de ESPOL TV. Desarrollador de Sistemas Hospitalarios en OMNIHOSPITAL. Operador del Centro de Computo de MEDIANET S.A. Senior Elastix Project Developer de APLISOFT –Software (actual).

7.3.2. Cuestionario enviado a los miembros del grupo de expertos: primera ronda

A partir del 9 de junio del 2013, se enviaron correos electrónicos a cada uno de los miembros del grupo de expertos, conteniendo el cuestionario correspondiente a la primera ronda, utilizando el siguiente texto:

> "Internet, hoy en día, proporciona un sistema insuperable para la comunicación pública de la ciencia y la tecnología de una forma interconectada e interoperable, a nivel mundial.
>
> Los gobiernos del mundo reconocieron en la Cumbre Mundial de la Sociedad de la Información (2003) que las Tecnologías de la Información y la Comunicación (TIC) permiten a la población tener acceso a la información y al conocimiento en

cualquier lugar del mundo y de manera prácticamente instantánea. La comunidad científica está aprovechando las ventajas de las comunicaciones instantáneas utilizando las herramientas modernas que ofrece la web 2.0, como las redes sociales, blogs, wikis, grupos de discusión, webcasts, conferencias virtuales y sistemas de mensajería instantánea, entre otras. La difusión de los resultados de la ciencia y la tecnología efectuada tradicionalmente a través de libros y revistas especializadas impresas en papel se ha trasladado a la web, al publicarse simultáneamente en versiones electrónicas. Las bases de datos bibliográficas con formato electrónico consultadas a través de Internet facilitan notablemente la actividad de la investigación científica y de la academia. Igualmente los repositorios o archivos digitales científicos tienen como objetivo fundamental difundir por Internet de una manera más visible, los resultados de la investigación científica. Hoy las redes sociales son portadoras de nuevas formas de interacción social, de diálogo, intercambio y colaboración.

Las TICs se constituyen en la herramienta fundamental para la construcción de la Sociedad de la Información, por lo tanto es vital que esté garantizada la libertad de Internet como un derecho fundamental de todas las personas.

Mi tesis previa a la obtención de mi título de Magíster en Comunicación Pública de la Ciencia y Tecnología en la ESPOL investiga si en el entorno mundial y en el Ecuador se dispone del marco legal que garantice la libertad de expresión en línea, si se reconoce la libertad de expresión en línea como un derecho universal de todas las personas y si existe libertad de Internet en todos los países del mundo.

Como un método de investigación estoy utilizando la técnica Delphi que consiste en la selección de un grupo de expertos a los que se les consulta su opinión mediante un cuestionario sobre situaciones referidas a acontecimientos futuros,

mediante dos o más sucesivas rondas, en las que se mantiene el anonimato de los miembros del grupo, a fin de llegar a un eventual consenso por parte de los participantes. Los resultados estadísticos de cada ronda son puestos en consideración de todos los miembros del grupo, con el fin de conocer si se mantienen en sus respuestas o las modifican exponiendo sus razones para el efecto.

En este sentido quiero en primer lugar expresarle mi agradecimiento por aceptar mi invitación de integrar el grupo de expertos y solicitarle muy comedidamente la contestación del siguiente cuestionario, con cualquiera de las siguientes repuestas:

Fuertemente de acuerdo = 5
De acuerdo = 4
Neutral = 3
En desacuerdo = 2
Fuertemente en desacuerdo = 1

CUESTIONARIO:

1.- La libertad de expresión en línea será un derecho de todas las personas, en consideración de que la libertad de expresión está consagrada en el Art. 19 de la Declaración Universal de los Derechos Humanos (1948), en el Art. 19 del Convenio Internacional sobre los Derechos Civiles y Políticos (1966), en el Art. 13 de la Convención Americana sobre Derechos Humanos (1969), y de que la Declaración Conjunta (2011) del Relator Especial de Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, de la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) de la Organización de Estados Americanos (OEA), de la Representante

de la Organización para la Seguridad y la Cooperación en Europa (OSCE) para la Libertad de los Medios de Comunicación, y de la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), adoptó como uno de los principios generales que la libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. ( )

2. A pesar de que organismos no gubernamentales como "OpenNet Initiative" y "Freedom House" han efectuado estudios sobre la libertad de Internet en el mundo que concluyen que en el año 2012, en varios países se han producido asesinatos, arrestos y ataques brutales contra blogeros, se ha efectuado una manipulación proactiva de contenidos web, se practica el filtraje de Internet, bloqueo de sitios web y direcciones IP, y se han expedido leyes que restringen la libertad de expresión en línea; y, como "Reporteros sin Fronteras" que identificó en el año 2012 a 12 países "enemigos de Internet", en los próximos años habrá libertad de expresión en línea en todos los países del mundo. ( )

3. El Centro de Respuesta Global (CRG), que es la plataforma mundial implementada en el año 2010 por la Unión Internacional de Telecomunicaciones (UIT) que constituye el sistema de alerta temprana y el principal centro de recursos sobre ciberamenazas para la comunidad mundial, y que tiene como uno de sus objetivos ayudar a los países a identificar rápidamente las ciberamenazas y proporcionar información esencial sobre las medidas que deben ser adoptadas para mitigarlas, brindará la protección y confianza necesaria contra las ciberamenazas que afectan a los usuarios de Internet. ( )

4. La Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea, considerando:

•Que el artículo 16 dispone que todas las personas, en forma individual o colectiva, tienen derecho al acceso universal a las tecnologías de información y comunicación, a la creación de medios de comunicación social, y al acceso y uso de todas las formas de comunicación visual, auditiva y sensorial;

•Que el artículo 18 expresa que todas las personas, en forma individual o colectiva, tienen derecho a buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior y acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas;

•Que el artículo 20, a su vez, dispone que el Estado garantizará la cláusula de conciencia a toda persona, así como el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación; y,

•Que el artículo 66, Numeral 6 del Capítulo Sexto titulado "Derechos de libertad", reconoce y garantiza a las personas el derecho a opinar y expresar su pensamiento libremente y en todas sus formas y manifestaciones. ( )

5. El Art. 29.9 del "Reglamento de Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y de Valor Agregado" emitido por el CONATEL, que dispone que una de las obligaciones de los prestadores de servicios de telecomunicaciones y de valor agregado de Internet es remitir a solicitud de la Superintendencia de Telecomunicaciones información relativa a direcciones IP asignada a sus abonados/clientes-usuarios, atentará contra la privacidad de los usuarios de Internet. ( )

6. La disposición contenida en el Art. 20 de la Ley Orgánica de Comunicación del Ecuador, que obliga a que los medios de comunicación en línea generen mecanismos de registro de datos personales que permitan la identificación de quienes comenten en sus publicaciones en línea, constituirá una amenaza a la privacidad y protección de datos de los usuarios en Internet. ( )

7. Considerando que en los primeros 6 meses del año 2012, la Fiscalía General del Estado registró 1354 casos de delitos informáticos financieros, equivalente a 7 delitos informáticos por día, existirán amenazas de ciberataques a los usuarios de Internet en el país. ( )

Atentamente,

Lcda. Lady Rodríguez Dumes"

7.3.3. Resultados de la primera ronda de preguntas

Una vez que recibidas las repuestas de todos los 11 miembros del grupo de expertos, se procedió a evaluar estadísticamente los resultados obtenidos utilizándose para este propósito el software SPSS.

En la Tabla 7.1 se observa la estadística descriptiva de las respuestas dadas por los expertos a cada una de las 7 preguntas que le fueron formuladas.

Tabla 7.1: Estadística descriptiva de las respuestas de la primera ronda

Statistics

		Internet será un derecho de todas las personas (Pregunta 1)	En los próximos años habrá libertad de expresión en línea en el mundo (Pregunta 2)	Centro de Respuesta Global (CRG) brindará protección y confianza contra los ciberataques que afectan a los usuarios de Internet (Pregunta 3)	Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea (Pregunta 4)	Reglamento de Abonados de Ecuador atentará contra la privacidad de los usuarios de Internet (Pregunta 5)	Ley Orgánica de Comunicación de Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet (Pregunta 6)	Existirán amenazas de ciberataques a los usuarios de Internet en el país (Pregunta 7)
N	Valid	11	11	11	11	11	11	11
	Missing	0	0	0	0	0	0	0
Mean		4.82	2.55	3.36	4.00	3.27	3.55	4.82
Median		5.00	2.00	3.00	4.00	4.00	4.00	5.00
Mode		5	2	3[a]	4	4[a]	4	5
Std. Deviation		.405	1.128	.924	1.095	1.555	1.368	.405
Variance		.164	1.273	.855	1.200	2.418	1.873	.164
Range		1	3	3	3	4	4	1
Minimum		4	1	2	2	1	1	4
Maximum		5	4	5	5	5	5	5
Percentiles	25	5.00	2.00	3.00	4.00	2.00	2.00	5.00
	50	5.00	2.00	3.00	4.00	4.00	4.00	5.00
	75	5.00	4.00	4.00	5.00	5.00	5.00	5.00

a. Multiple modes exist. The smallest value is shown

Fuente: Cálculos de la autora

Del análisis de la Tabla 7.1 se puede establecer que existe un amplio consenso en las respuestas correspondientes a las preguntas 1 y 7, por lo que no será necesario someter estas preguntas a una segunda ronda. Se efectuará a continuación un análisis estadístico de las respuestas obtenidas en estas dos preguntas.

Pregunta 1:

La hipótesis nula (H_o) y la hipótesis alternativa (H_1) planteadas en la sección 2.1 correspondiente a la pregunta 1 formulada a los expertos son:

$H_{0:}$ La libertad de expresión en línea no será un derecho de todas las personas.

Es decir:

$H_{0:}$ $\mu \leq 2$

H_1: La libertad de expresión en línea será un derecho de todas las personas.

Es decir:

$H_{1:}$ $\mu \geq 4$

De la Tabla 7.1 se puede establecer que existe un amplio consenso en que Internet será un derecho de todas las personas puesto que el quartil Q1 (25%), la mediana (50%) y el quartil Q3 (75%) coinciden con el valor 5 (fuertemente de acuerdo), lo que significa que el espacio interquartil es 0 (Q3-Q1). El valor mínimo es 4 (de acuerdo) y el valor máximo es 5 (fuertemente de acuerdo). La desviación estándar es pequeña teniendo un valor de 0.405 y el valor medio (mean) es 4.82.

La Tabla 7.2 muestra la frecuencia de las respuestas obtenidas para la pregunta 1, en donde se puede apreciar que el 81.8% de las respuestas fue 5 (fuertemente de acuerdo) y 18.2% (de acuerdo), concluyéndose que el 100% de los expertos consideran que Internet será un derecho de todas las persona.

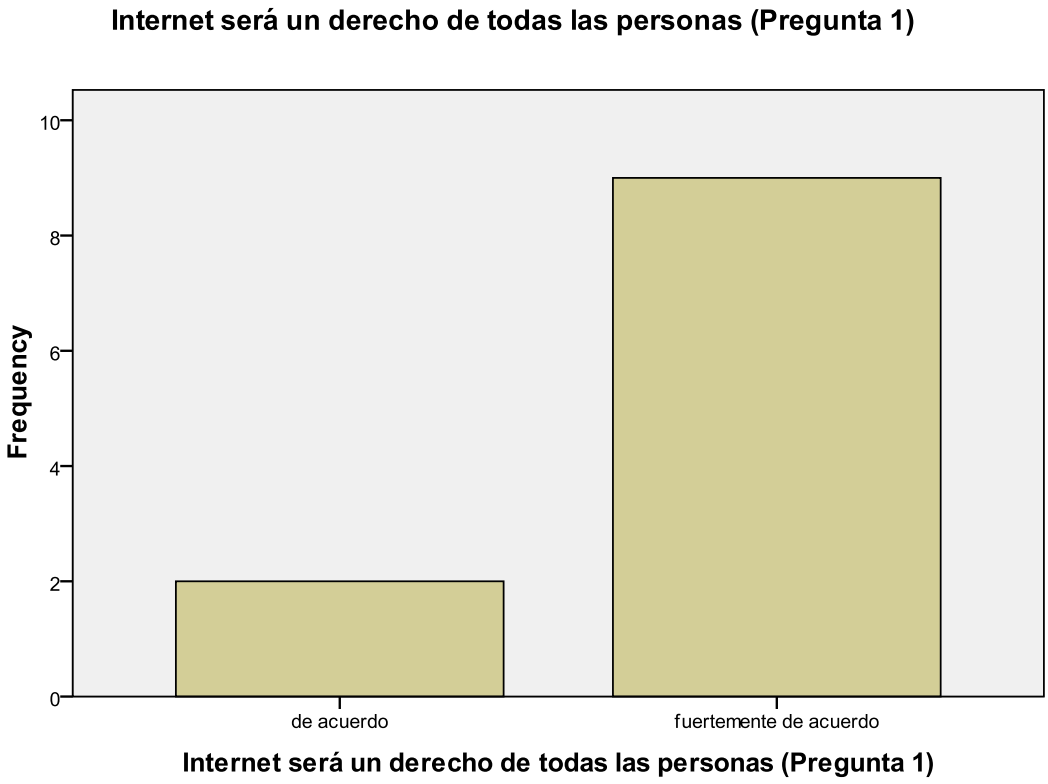
Tabla 7.2: Frecuencia de las respuestas de la pregunta 1

Internet será un derecho de todas las personas (Pregunta 1)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	de acuerdo	2	18.2	18.2	18.2
	fuertemente de acuerdo	9	81.8	81.8	100.0
	Total	11	100.0	100.0	

Fuente: Cálculos de la autora

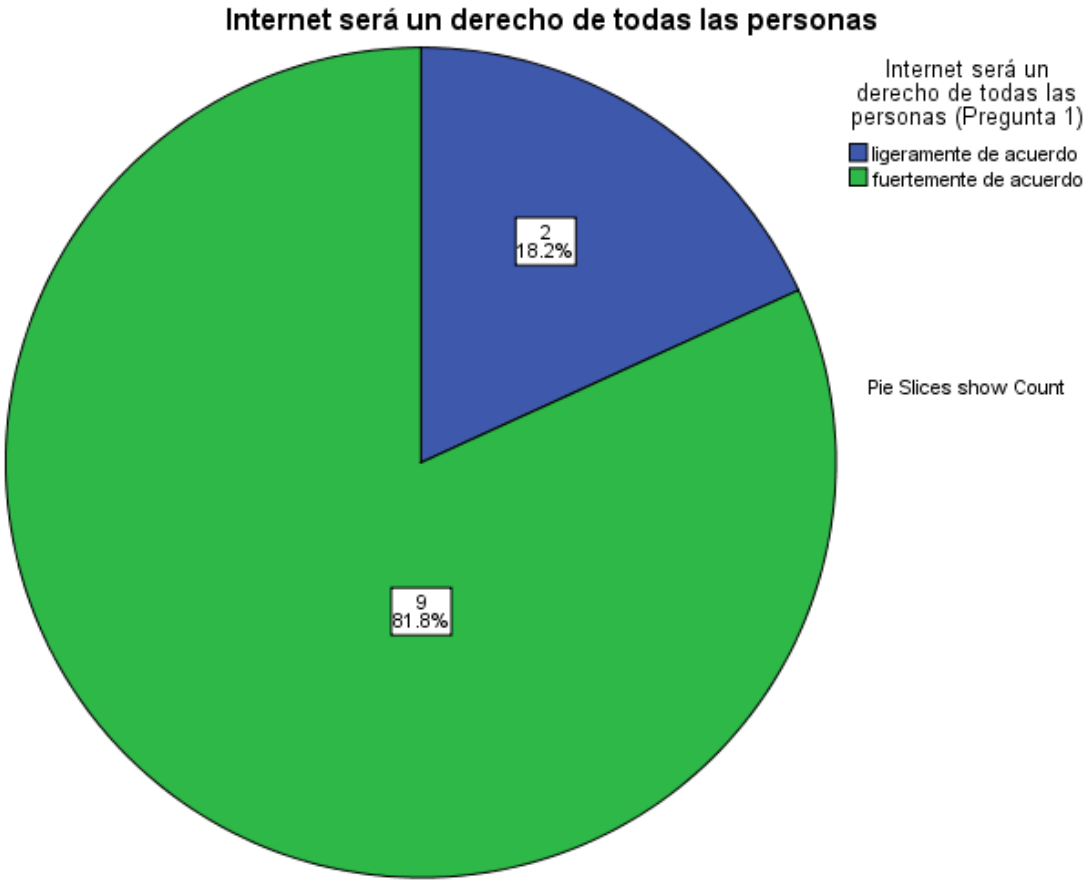
La Figura 7.1 muestra la distribución de frecuencia de las respuestas obtenidas en diagrama de barras para la pregunta 1.



Fuente: Cálculos de la autora

Figura 7.1: Diagrama de barras para la pregunta 1

La Figura 7.2 muestra el diagrama de torta de las respuestas obtenidas para la pregunta 1.

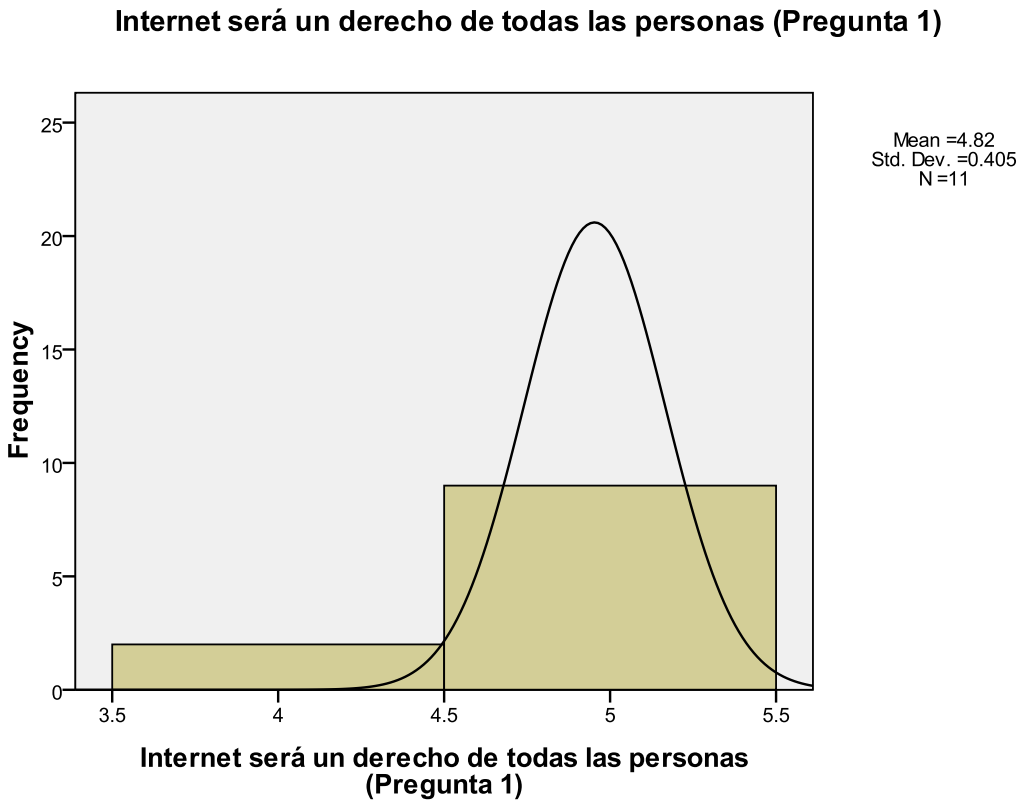


Fuente: Cálculos de la autora

Figura 7.2: Diagrama de torta para la pregunta 1

Cabe mencionar que el diagrama de torta para una pregunta similar realizada a nivel internacional en 26 países (en el que no estuvo incluido Ecuador) mostrado en la Figura 3.2, investigación que fue realizada por la BBC World Service en el año 2010, dio como resultado que el 79% estaban de acuerdo en que Internet debe ser un derecho fundamental de todas las personas.

La Figura 7.3 muestra el histograma y la curva normal de distribución para la pregunta 1.



Fuente: Cálculos de la autora

Figura 7.3: Histograma y curva normal para la pregunta 1

Para la pregunta 1 existe suficiente evidencia estadística para rechazar la hipótesis nula (H_0) y en su lugar aceptar la hipótesis alternativa (H_1), esto es, que Internet será un derecho de todas las personas. No es necesario para el presente caso realizar la "prueba t de una muestra" para probar la verosimilitud de $H_{0.}$

Cabe mencionar que esta conclusión también fue alcanzada previamente en el Capítulo 3.

Pregunta 7:

La hipótesis nula (H_o) y la hipótesis alternativa (H_1) planteadas en la sección 2.1 correspondiente a la pregunta 7 formulada a los expertos son:

H_0: No existirán amenazas de ciberataques a los usuarios de Internet en el país.

Es decir:

$H_{0:}$ $\mu \leq 2$

H_1: Existirán amenazas de ciberataques a los usuarios de Internet en el país.

Es decir:

$H_{1:}$ $\mu \geq 4$

De la Tabla 7.1 se puede establecer que existe un amplio consenso en que existirán en Ecuador amenazas de ciberataques puesto que el quartil Q1 (25%), la mediana (50%) y el quartil Q3 (75%) coinciden con el valor 5 (fuertemente de acuerdo), lo que significa que el espacio interquartil es 0 (Q3-Q1). El valor mínimo es 4 (de acuerdo) y el valor máximo es 5 (fuertemente de acuerdo). La desviación estándar es pequeña teniendo un valor de 0.405 y el valor medio (mean) es 4.82.

La Tabla 7.3 muestra la frecuencia de las respuestas obtenidas para la pregunta 7, en donde se puede apreciar que el 81.8% de las respuestas fue 5(fuertemente de acuerdo) y 18.2% (de acuerdo), concluyéndose que el 100% de los expertos consideran que existirán en Ecuador amenazas de ciberataques a los usuarios de Internet en el país.

.

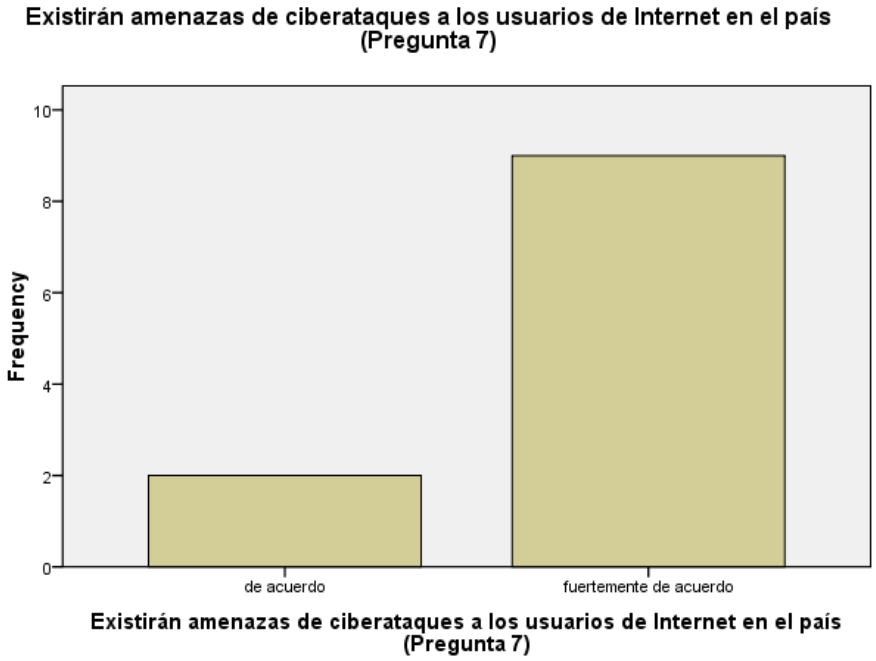
Tabla 7.3: Frecuencia de las respuestas de la pregunta 7

Existirán amenazas de ciberataques a los usuarios de Internet en el país (Pregunta 7)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	de acuerdo	2	18.2	18.2	18.2
	fuertemente de acuerdo	9	81.8	81.8	100.0
	Total	11	100.0	100.0	

Fuente: Cálculos de la autora

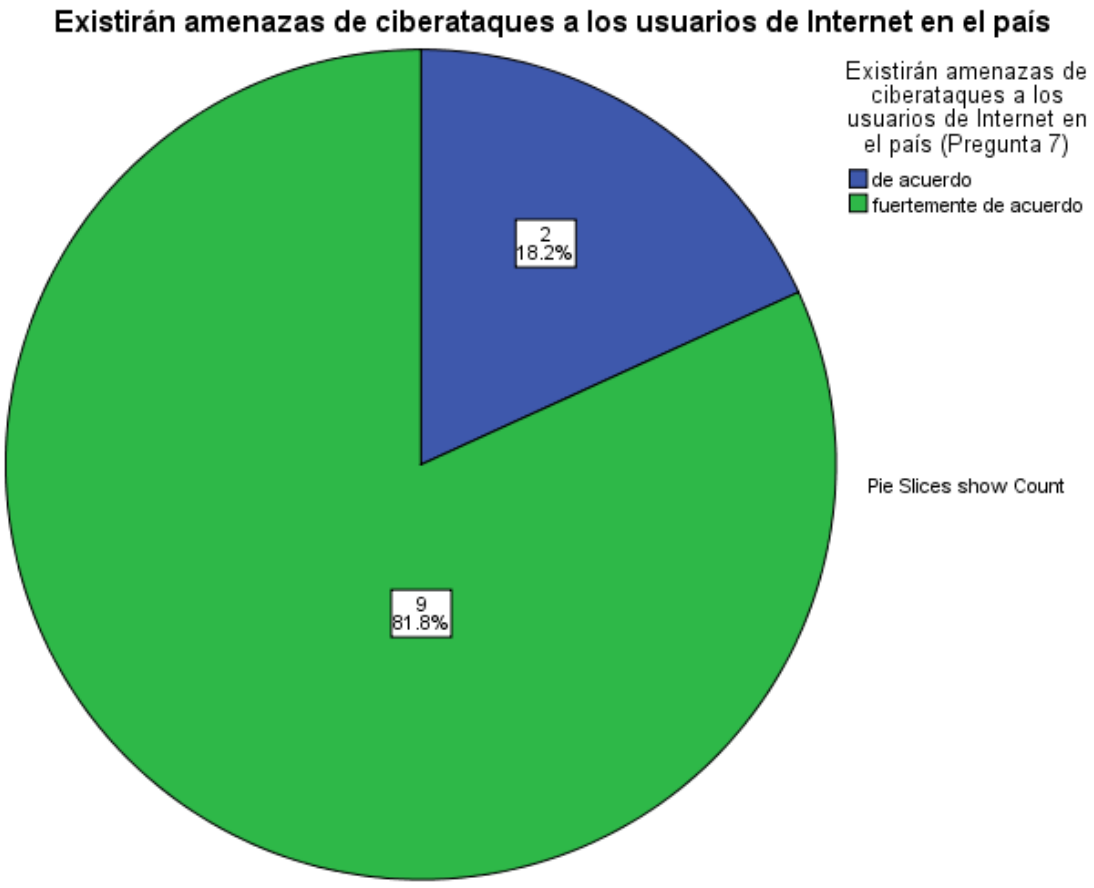
La Figura 7.4 muestra la distribución de frecuencia de las respuestas obtenidas en diagrama de barras para la pregunta 7.



Fuente: Cálculos de la autora

Figura 7.4: Diagrama de barras para la pregunta 7

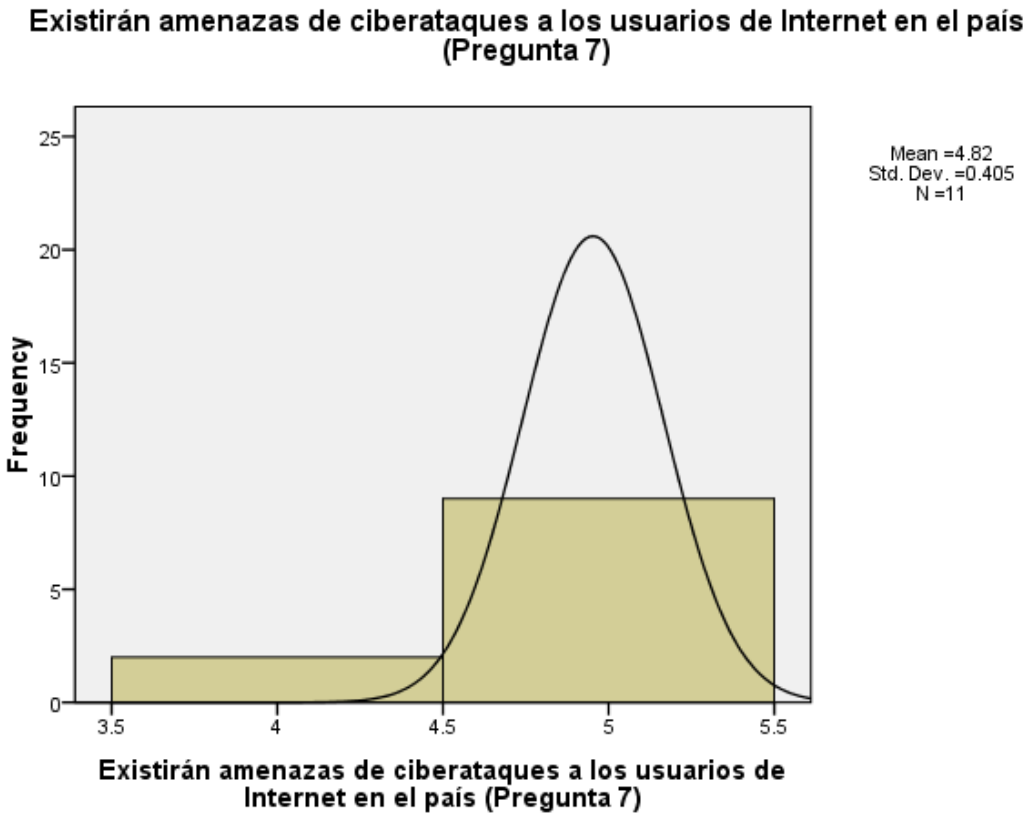
La Figura 7.5 muestra el diagrama de torta de las respuestas obtenidas para la pregunta 7.



Fuente: Cálculos de la autora

Figura 7.5: Diagrama de torta para la pregunta 7

La Figura 7.6 muestra el histograma y la curva normal de distribución para la pregunta 7.



Fuente: Cálculos de la autora

Figura 7.6: Histograma y curva normal para la pregunta 7

Para la pregunta 7 existe suficiente evidencia estadística para rechazar la hipótesis nula (H_0) y en su lugar aceptar la hipótesis alternativa (H_1), esto es, que existirán amenazas de ciberataques a los usuarios de Internet en el país. No es necesario para el presente caso realizar la "prueba t de una muestra" para probar la verosimilitud de H_0.

Cabe mencionar que a esta conclusión también se llegó en el análisis previo efectuado en la sección 5.5.

7.3.4. Resultados de la segunda ronda de preguntas

A partir del 1 de julio del 2013, se enviaron correos electrónicos a cada uno de los miembros del grupo de expertos, conteniendo el cuestionario correspondiente a la segunda ronda, utilizando el siguiente texto:

> "Me es muy grato hacerle conocer en el documento adjunto el resultado de las respuestas de los 11 profesionales que integran el grupo de expertos sobre la investigación que estoy realizando sobre la libertad de expresión en línea. De acuerdo con el método de investigación Delphi, luego de hacer conocer a todos los expertos la opinión del grupo, se les solicita que revisen sus respuestas para ratificarlas o reconsiderarlas. El objetivo de este procedimiento es disminuir el espacio intercuartil de la frecuencia de las respuestas y tratar de incrementar el consenso.
>
> Del análisis de los resultados se puede establecer que las preguntas 1 y 7 lograron un amplio consenso por lo que no serán sometidas a una segunda ronda. En este sentido mucho les agradeceré pronunciarse sobre la ratificación o modificación de sus respuestas en lo correspondiente a las preguntas 2, 3, 4, 5 y 6, que las vuelvo a transcribir con este propósito".

Una vez que se recibieron las repuestas de los miembros del grupo de expertos, se procedió a evaluar estadísticamente los resultados obtenidos.

En la Tabla 7.4 se observa la estadística descriptiva de las respuestas dadas por los expertos a cada una de las restantes 5 preguntas que le fueron formuladas en una segunda ronda.

Tabla 7.4: Estadística descriptiva de las respuestas de la segunda ronda

Statistics

		En los próximos años habrá libertad de expresión en línea en el mundo (Pregunta 2)	Centro de Respuesta Global (CRG) brindará protección y confianza contra los ciberataques que afectan a los usuarios de Internet (Pregunta 3)	Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea (Pregunta 4)	Reglamento de Abonados de Ecuador atentará contra la privacidad de los usuarios de Internet (Pregunta 5)	Ley Orgánica de Comunicación de Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet (Pregunta 6)
N	Valid	11	11	11	11	11
	Missing	0	0	0	0	0
Mean		2.36	3.36	4.00	3.55	3.82
Median		2.00	4.00	4.00	4.00	4.00
Mode		2	4	4	4	4[a]
Std. Deviation		1.027	.809	1.095	1.368	1.328
Variance		1.055	.655	1.200	1.873	1.764
Range		3	2	3	4	4
Minimum		1	2	2	1	1
Maximum		4	4	5	5	5
Percentiles	25	2.00	3.00	4.00	2.00	3.00
	50	2.00	4.00	4.00	4.00	4.00
	75	3.00	4.00	5.00	5.00	5.00

a. Multiple modes exist. The smallest value is shown

Fuente: Cálculos de la autora

Se efectuará a continuación un análisis estadístico de las respuestas obtenidas en estas 5 preguntas restantes (Preguntas 2 a 5).

Pregunta 2

La hipótesis nula (H_o) y la hipótesis alternativa (H_1) planteadas en la sección 2.1 correspondiente a la pregunta 2 formulada a los expertos son:

H_0: En los próximos años no habrá libertad de expresión en línea en todos los países del mundo.

Es decir:

$H_{0:}$ $\mu \leq 2$

H_1: En los próximos años habrá libertad de expresión en línea en todos los países del mundo

Es decir:

$H_{1:}$ $\mu \geq 4$

La Tabla 7.5 muestra la frecuencia de las respuestas obtenidas para la pregunta 2 en la segunda ronda, en la donde se puede apreciar que 7 (63.6%) de los 11 expertos opinaron que en los próximos años no habrá libertad de expresión en línea en el mundo, 2 (18.2%) expresaron su neutralidad y 2 (18.2%) manifestaron estar en desacuerdo.

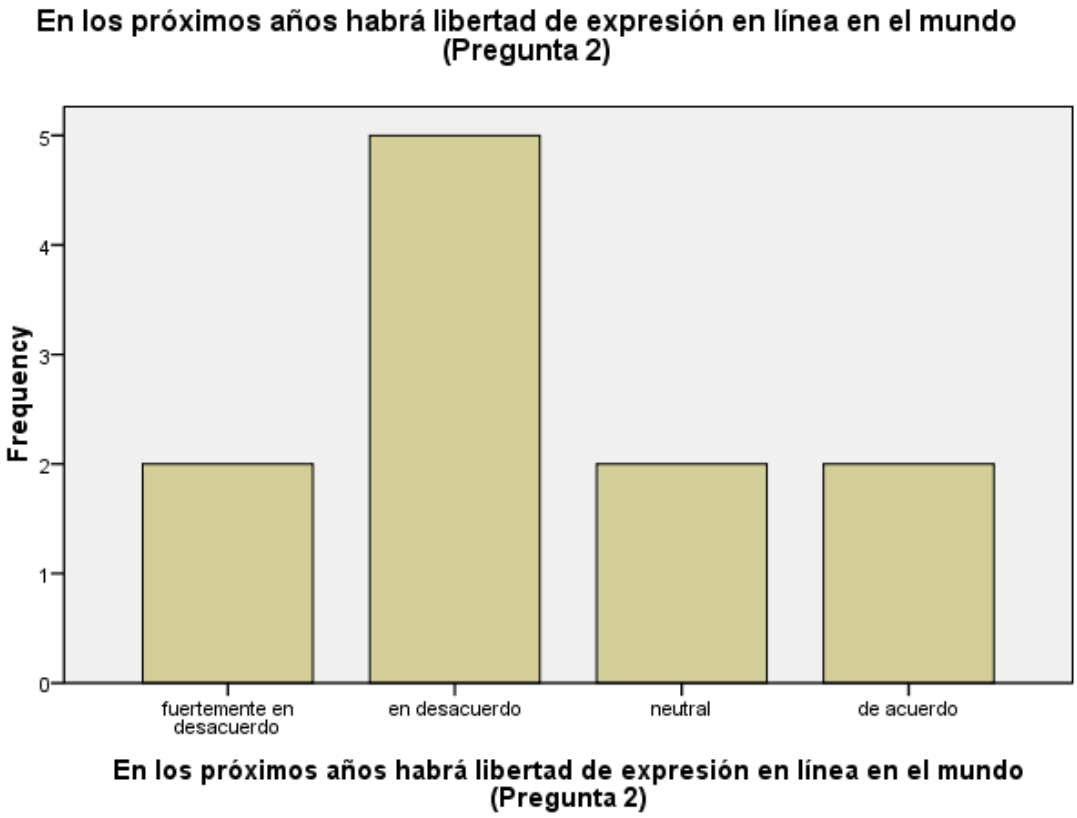
Tabla 7.5: Frecuencia de las respuestas de la pregunta 2 (segunda ronda)

En los próximos años habrá libertad de expresión en línea en el mundo (Pregunta 2)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	fuertemente en desacuerdo	2	18.2	18.2	18.2
	en desacuerdo	5	45.5	45.5	63.6
	neutral	2	18.2	18.2	81.8
	de acuerdo	2	18.2	18.2	100.0
	Total	11	100.0	100.0	

Fuente: Cálculos de la autora

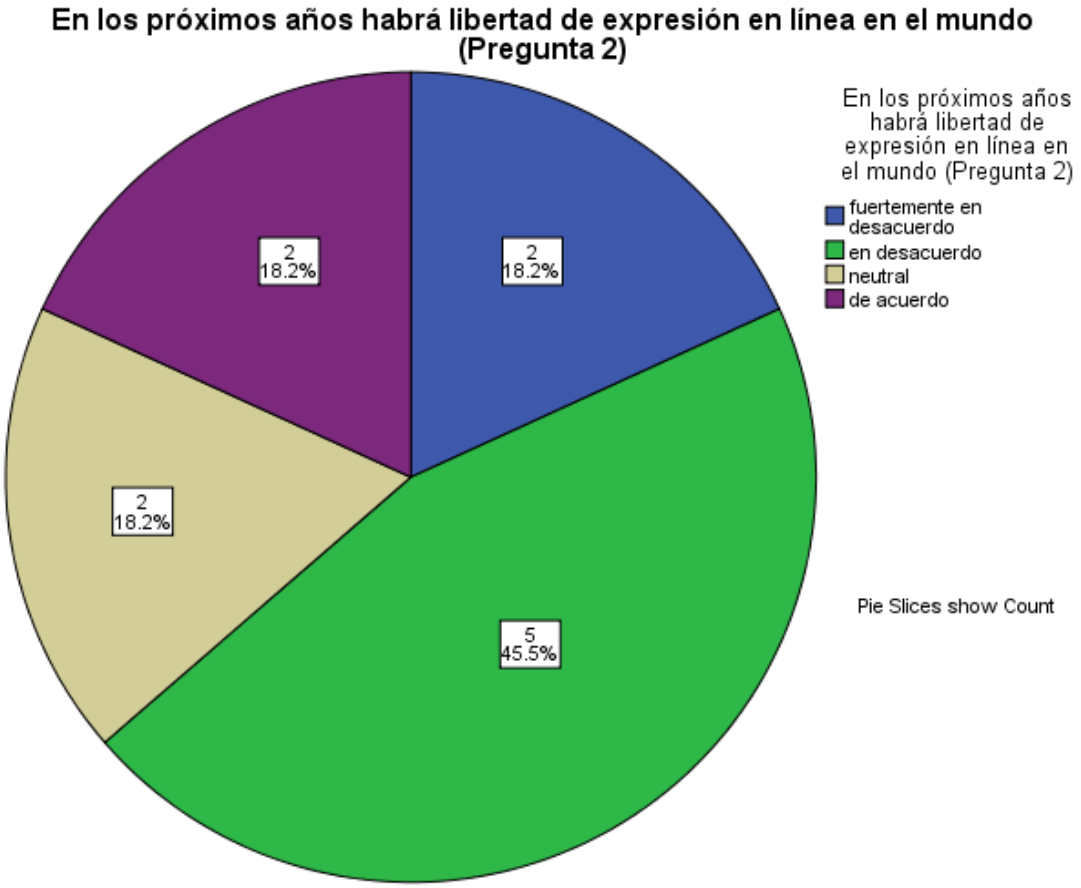
La Figura 7.7 muestra la distribución de frecuencia de las respuestas obtenidas en diagrama de barras para la pregunta 2 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.7: Diagrama de barras para la pregunta 2 (segunda ronda)

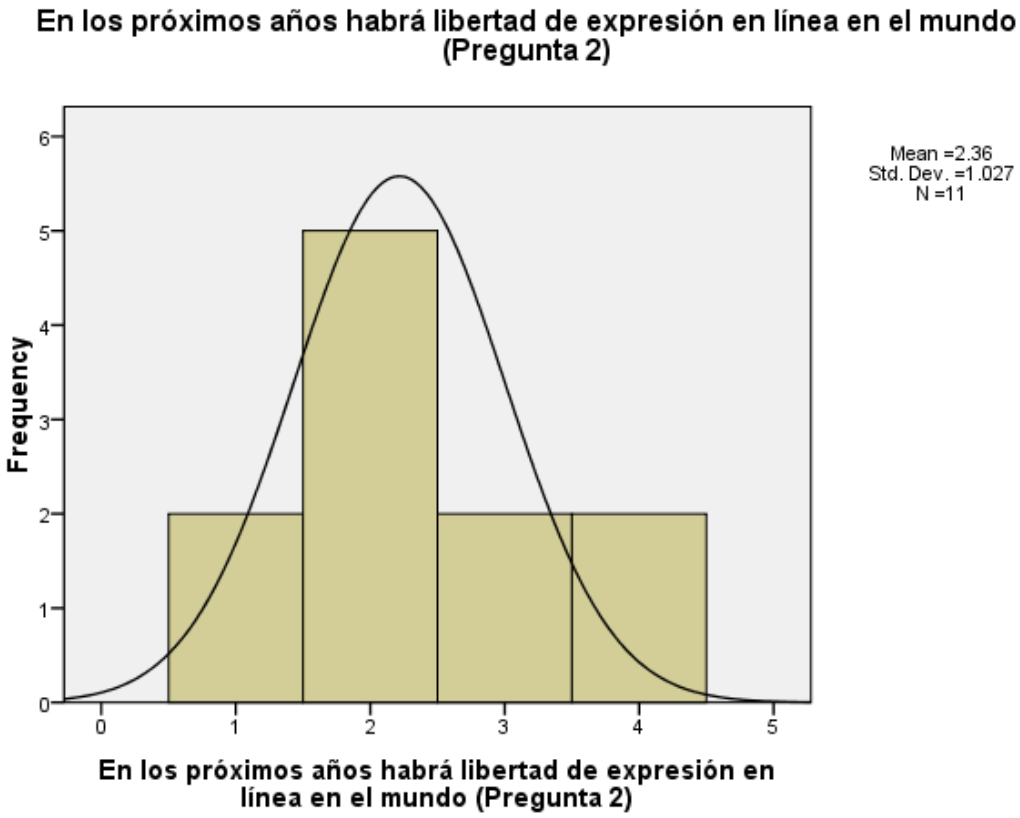
La Figura 7.8 muestra el diagrama de torta de las respuestas obtenidas para la pregunta 2 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.8: Diagrama de torta para la pregunta 2 (segunda ronda)

La Figura 7.9 muestra el histograma y la curva normal de distribución para la pregunta 2.



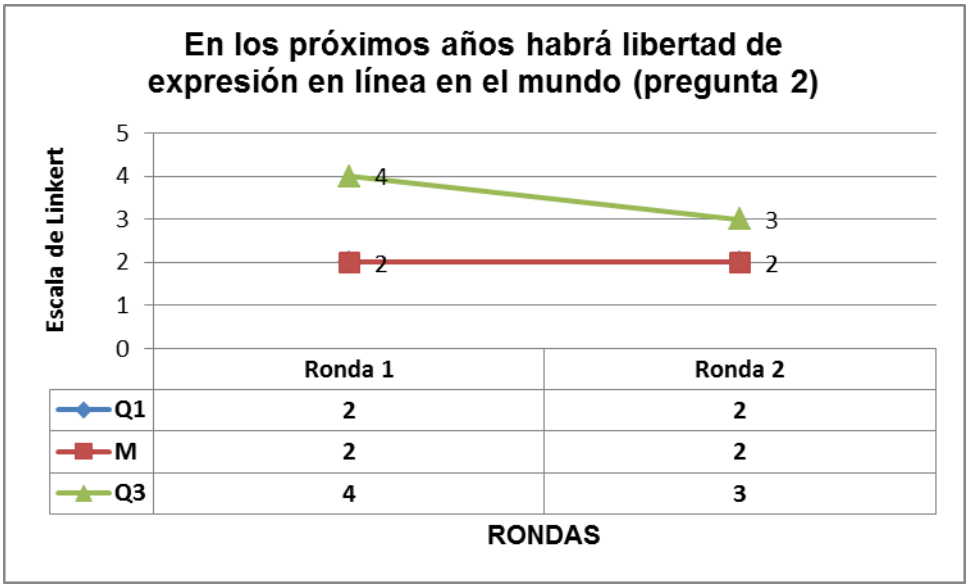
Fuente: Cálculos de la autora

Figura 7.9: **Histograma y curva normal para la pregunta 2**

De las Tablas 7.1 y 7.4 se obtienen los valores del quartil Q1 (25%), la mediana (50%) y el quartil Q3 (75%) tanto para la primera como para la segunda ronda.

En la Figura 7.10 se muestran los valores obtenidos para estos cálculos estadísticos correspondientes a la pregunta 2 y en la cual se puede observar que la línea de Q1 coincide con la línea de la mediana y que el espacio intercuartil (Q3 – Q1) se reduce desde un valor de 2 obtenido en la primera ronda a un valor de 1 en la segunda ronda, así como también que la mediana se mantiene en el valor constante de 2. De este análisis se

puede concluir preliminarmente que existe una aproximación del consenso del grupo de expertos al valor de 2, equivalente a validar la hipótesis nula H_0. Sin embargo esta conclusión deberá ser sometida a confirmación más adelante mediante la realización de la "prueba t de una muestra".



Fuente: Cálculos de la autora

Figura 7.10: Resultados de la primera y segunda rondas para la pregunta 2

En la Tabla 7.6 se muestran las estadísticas para la "prueba t de una muestra" realizada para los resultados obtenidos en la pregunta 2.

Tabla 7.6: **Estadísticas para prueba t de una muestra (pregunta 2)**

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
En los próximos años habrá libertad de expresión en línea en el mundo (Pregunta 2)	11	2.36	1.027	.310

Esta Tabla indica que: existen 11 observaciones (número de expertos), el valor promedio de la muestra ($\bar{x}$) es de 2.36, la desviación estándar es de 1.027 y el error estándar del promedio es 0.310; este último valor corresponde al denominador de la fórmula para calcular t que se incluyó en la sección 2.1 [$t = \frac{\bar{x} - \mu}{\frac{S}{\sqrt{n}}}$].

En la Tabla 7.7 se muestran los valores de la "prueba t de una muestra" para los resultados obtenidos para la pregunta 2 en la segunda ronda, utilizando un intervalo de confianza del 95%, es decir que el nivel de significancia es de $\alpha = 0.05$. En vista de que la hipótesis nula es $H_{0:}\ \mu \leq 2$, el valor a probar es 2. La prueba t es una prueba de una cola (one-tailed test).

Tabla 7.7: Valores de la prueba t de una muestra con un valor a probar igual a 2 (pregunta 2)

One-Sample Test

	Test Value = 2					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
En los próximos años habrá libertad de expresión en línea en el mundo (Pregunta 2)	1.174	10	.267	.364	-.33	1.05

Esta tabla muestra que el valor observado de t es 1.174 con 10 grados de libertad (n – 1). El valor crítico de t se lo obtiene de la tabla estadística de valores críticos de t; en dicha tabla se puede determinar que para 10 grados de libertad y un nivel de significancia de $\alpha = 0.05$, el valor crítico de t es 1.812 (ver Anexo 2). Siendo el valor promedio de la muestra ($\bar{x}$=2.36) mayor que el valor a probar (μ=2), el valor de t es positivo, por lo tanto la región crítica para la prueba de una cola se encontrará en la región de la cola

superior (ver Figura 2.1). En este sentido si el valor observado de t es mayor al valor t crítico se debe rechazar la hipótesis nula.

En el presente caso el valor observado de t es de 1.174 el cual es menor que el valor crítico t de 1.812, encontrándose dentro del intervalo de confianza, por lo que se debe aceptar la hipótesis nula.

Se concluye que existe suficiente evidencia estadística para aceptar la hipótesis nula (H_0) y en su lugar rechazar la hipótesis alternativa (H_1), es decir que en los próximos años no habrá libertad de expresión en línea en el mundo, como ya se percibía cuando se analizaron los casos de estudio sobre las amenazas a la libertad de expresión en línea en el Capítulo 6.

Pregunta 3

La hipótesis nula (H_o) y la hipótesis alternativa (H_1) planteadas en la sección 2.1 correspondientes a la pregunta 3 formulada a los expertos son:

H_0: El Centro de Respuesta Global no brindará la protección y confianza necesarias contra las ciberamenazas que afectan a los usuarios de Internet.

Es decir:

$H_{0:}$ $\mu \leq 2$

H_1: El Centro de Respuesta Global brindará la protección y confianza necesarias contra las ciberamenazas que afectan a los usuarios de Internet.

Es decir:

$H_{1:}$ $\mu \geq 4$

La Tabla 7.8 muestra la frecuencia de las respuestas obtenidas para la pregunta 3 en la segunda ronda, en donde se puede apreciar que 6 (54.5%) de los 11 expertos opinaron estar de acuerdo con que el Centro de Respuesta Global (CRG) brindará protección y confianza contra los ciberataques que afectan a los usuarios de Internet, 3 (27.3%) expresaron su neutralidad y 2 (18.2%) manifestaron estar en desacuerdo.

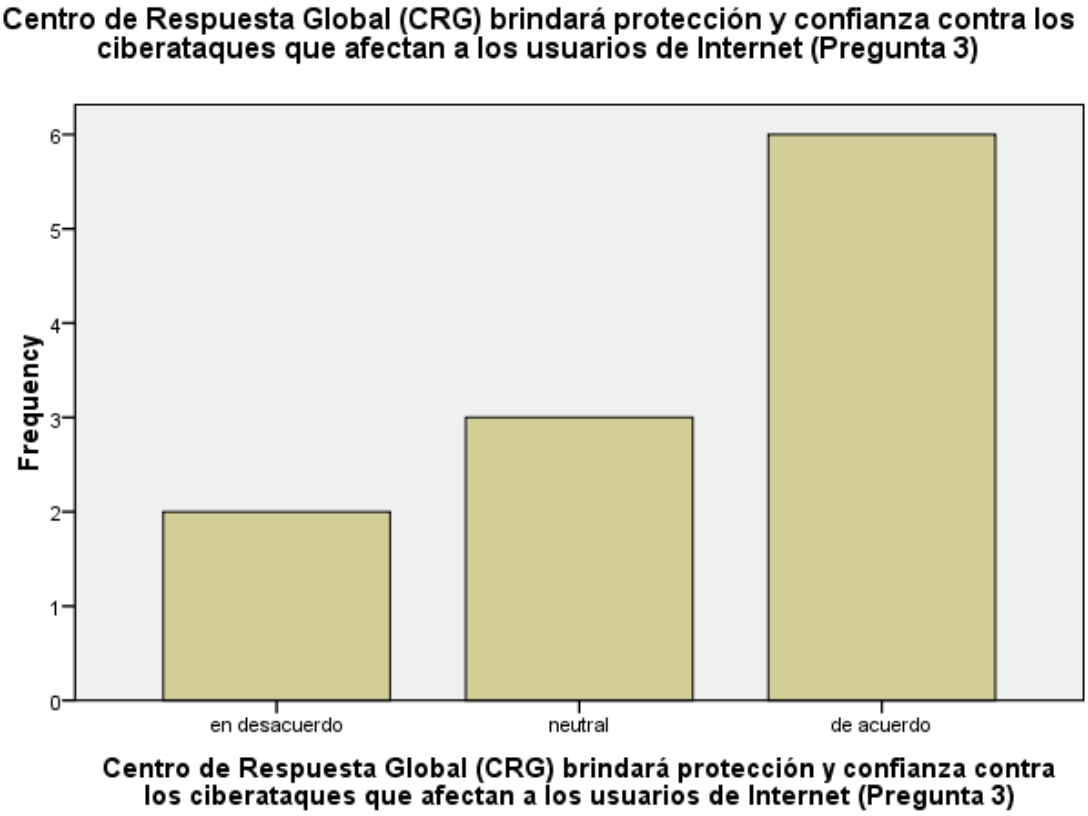
Tabla 7.8: Frecuencia de las respuestas de la pregunta 3 (segunda ronda)

Centro de Respuesta Global (CRG) brindará protección y confianza contra los ciberataques que afectan a los usuarios de Internet (Pregunta 3)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	en desacuerdo	2	18.2	18.2	18.2
	neutral	3	27.3	27.3	45.5
	de acuerdo	6	54.5	54.5	100.0
	Total	11	100.0	100.0	

Fuente: Cálculos de la autora

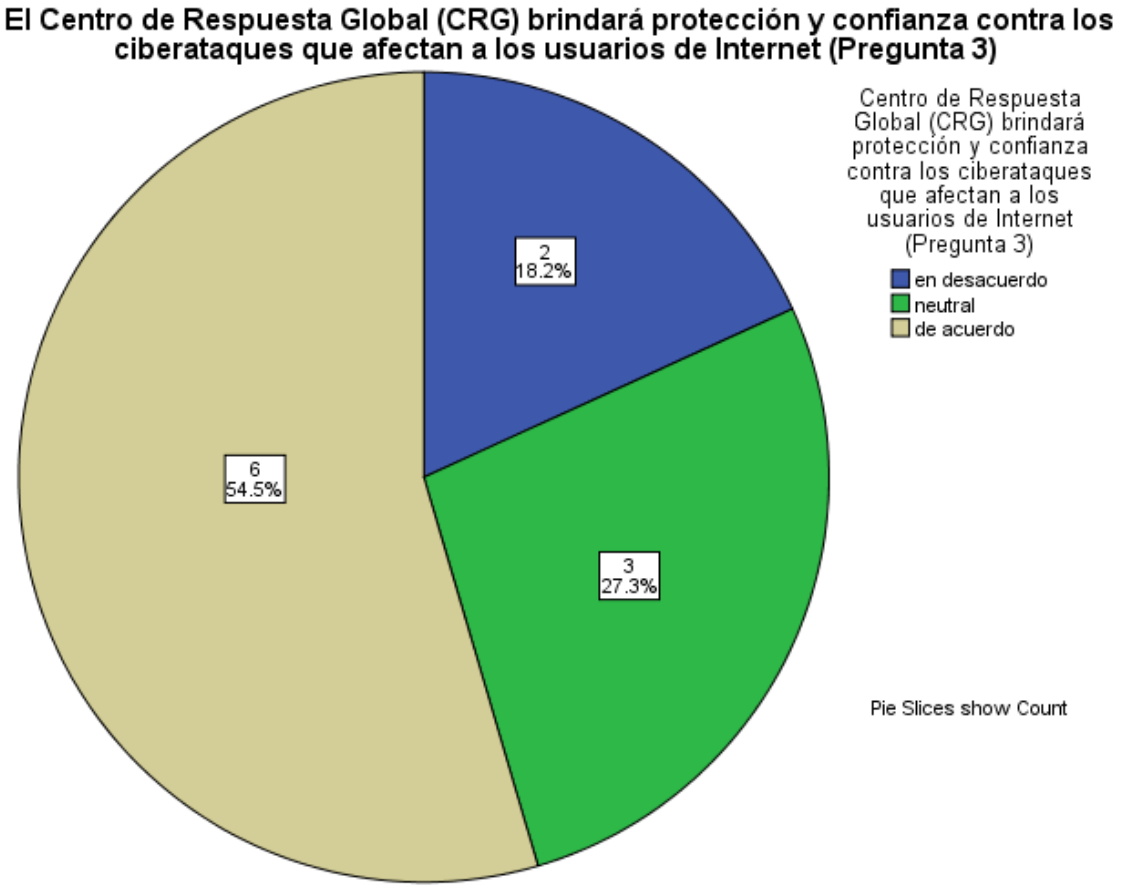
La Figura 7.11 muestra la distribución de frecuencia de las respuestas obtenidas en diagrama de barras para la pregunta 3 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.11: Diagrama de barras para la pregunta 3 (segunda ronda)

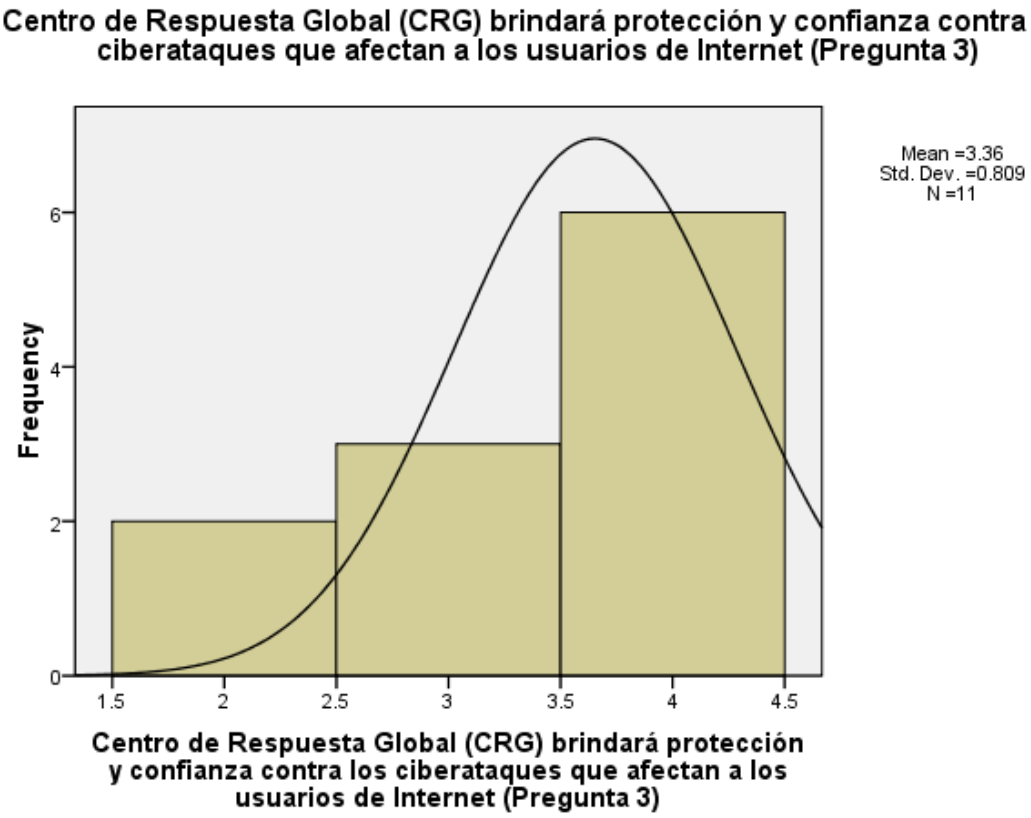
La Figura 7.12 muestra el diagrama de torta de las respuestas obtenidas para la pregunta 3 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.12: Diagrama de torta para la pregunta 3 (segunda ronda)

La Figura 7.13 muestra el histograma y la curva normal de distribución para la pregunta 3.



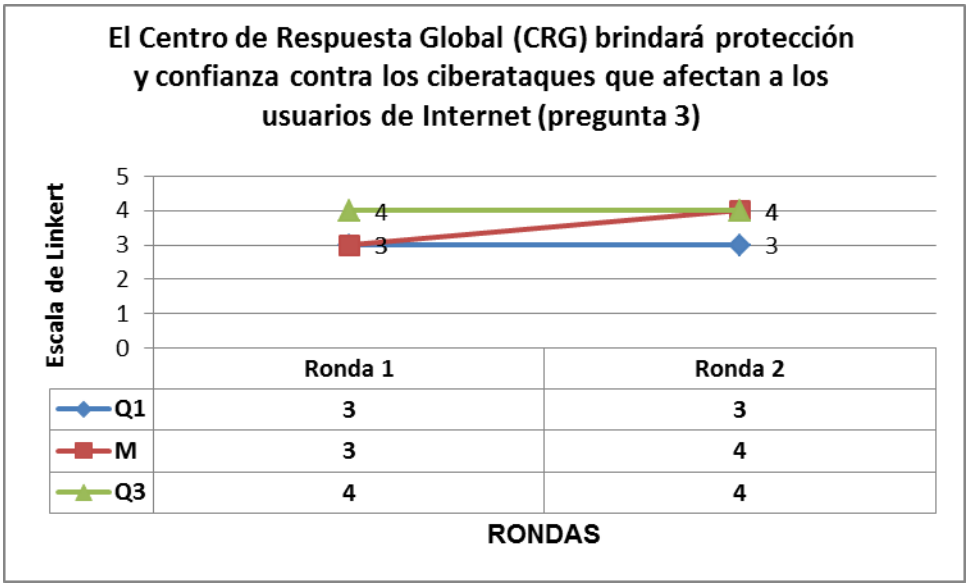
Fuente: Cálculos de la autora

Figura 7.13: **Histograma y curva normal para la pregunta 3**

De las Tablas 7.1 y 7.4 se obtienen los valores del quartil Q1 (25%), la mediana (50%) y el quartil Q3 (75%) tanto para la primera como para la segunda ronda.

En la Figura 7.14 se muestran los valores obtenidos para estos cálculos estadísticos correspondientes a la pregunta 3 y en la cual se puede observar que el espacio intercuartil (Q3 – Q1) se mantiene constante en el valor 1 entre la primera y segunda ronda, aunque la mediana se incrementa de 3 a 4. De este análisis se puede concluir preliminarmente que de que existe una aproximación del consenso del grupo de expertos al valor de 4, equivalente a validar la hipótesis alternativa H_1. Sin embargo esta

conclusión deberá ser sometida a confirmación más adelante mediante la realización de la "prueba t de una muestra".



Fuente: Cálculos de la autora

Figura 7.14: Resultados de la primera y segunda rondas para la pregunta 3

En vista de que en esta pregunta existe un porcentaje considerable de respuestas neutrales (27.3%) que podrían influenciar erróneamente a favor ya sea de la hipótesis nula o de la alternativa, se consideró conveniente eliminar este tipo de respuestas para la realización de la "prueba t de una muestra".

En la Tabla 7.9 se muestran las estadísticas para la "prueba t de una muestra" realizada para los resultados obtenidos en la pregunta 3.

Tabla 7.9: Estadísticas para prueba t de una muestra (pregunta 3)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Centro de Respuesta Global (CRG) brindará protección y confianza contra los ciberataques que afectan a los usuarios de Internet (Pregunta 3)	8	3.50	.926	.327

Fuente: Cálculos de la autora

Esta Tabla indica que: existen 8 observaciones (número de expertos menos 3 que votaron neutral), el valor promedio de la muestra ($\bar{x}$) es de 3.50, la desviación estándar es de 0.926 y el error estándar del promedio es 0.327.

En la Tabla 7.10 se muestran los valores de la "prueba t de una muestra" para los resultados obtenidos para la pregunta 3 en la segunda ronda, utilizando un intervalo de confianza del 95%, es decir que el nivel de significancia es de $\alpha = 0.05$, y sin considerar las respuestas neutrales. En vista de que la hipótesis nula es $H_{0:}\ \mu \leq 2$, el valor a probar es 2.

Tabla 7.10: Valores de la prueba t de una muestra con un valor a probar igual a 2 (pregunta 3)

One-Sample Test

	Test Value = 2					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Centro de Respuesta Global (CRG) brindará protección y confianza contra los ciberataques que afectan a los usuarios de Internet (Pregunta 3)	4.583	7	.003	1.500	.73	2.27

Fuente: Cálculos de la autora

Esta tabla muestra que el valor observado de t es 4.583 con 10 grados de libertad (n – 1). El valor crítico de t se lo obtiene de la tabla estadística de valores críticos de t; en dicha tabla se puede determinar que para 10 grados de libertad y un nivel de significancia de $\alpha = 0.05$, el valor crítico de t es 1.812. Siendo el valor promedio de la muestra ($\bar{x}$=3.50) mayor que el valor a probar (μ=2), el valor de t es positivo, por lo tanto la región crítica para la prueba de una cola se encontrará en la región de la cola superior (ver Figura 2.1). En este sentido si el valor observado de t es mayor al valor t crítico se debe rechazar la hipótesis nula.

En el presente caso el valor observado de t es de 4.583 el cual es mayor que el valor crítico t de 1.812, por lo que se debe rechazar la hipótesis nula.

Con el fin de verificar que se debe aceptar la hipótesis alternativa se realizará a continuación una prueba t para el valor a probar igual a 4.

Siendo el valor promedio de la muestra ($\bar{x}$=3.50) menor que el valor a probar (μ=4), el valor de t es negativo, por lo tanto la región crítica para la prueba de una cola se encontrará en la región de la cola inferior (ver Figura 2.1). En este sentido si el valor observado de t es menor al valor t crítico se debe rechazar la hipótesis alternativa.

En la Tabla 7.11 se muestran los valores de la "prueba t de una muestra" con el valor a probar igual a 4.

Tabla 7.11: Valores de la prueba t de una muestra con un valor a probar igual a 4 (pregunta 3)

One-Sample Test

	Test Value = 4					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Centro de Respuesta Global (CRG) brindará protección y confianza contra los ciberataques que afectan a los usuarios de Internet (Pregunta 3)	-1.528	7	.170	-.500	-1.27	.27

Fuente: Cálculos de la autora

Esta tabla indica que el valor observado de t es igual a -1.528 el cual es mayor que el valor crítico t de -1.812, por lo que se debe aceptar la hipótesis alternativa.

Se concluye que existe suficiente evidencia estadística para rechazar la hipótesis nula y aceptar la hipótesis alternativa, esto es, que el Centro de Respuesta Global (CRG) brindará la protección y confianza necesarias contra las ciberamenazas que afectan a los usuarios de Internet.

Pregunta 4

La hipótesis nula (H_o) y la hipótesis alternativa (H_1) planteadas en la sección 2.1 correspondientes a la pregunta 4 formulada a los expertos son:

H_0: La Constitución de la República del Ecuador no proveerá el marco legal que garantice la libertad de expresión en línea.

Es decir:

$H_{0:}$ $\mu \leq 2$

H_1: La Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea.

Es decir:

$H_{1:}$ $\mu \geq 4$

La Tabla 7.12 muestra la frecuencia de las respuestas obtenidas para la pregunta 4 en la segunda ronda, en la donde se puede apreciar que 9 (81.9%) de los 11 expertos opinaron estar de acuerdo con que la Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea y 2 (18.2%) manifestaron estar en desacuerdo, lo que evidencia un amplio consenso del grupo.

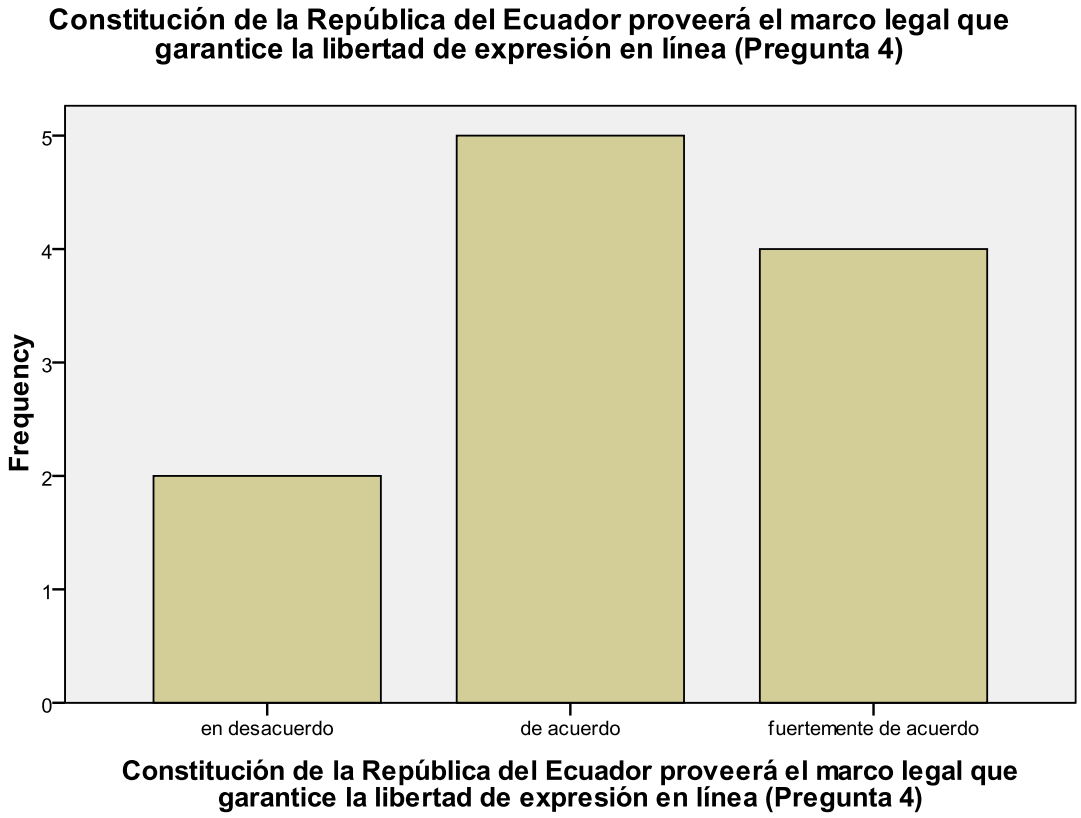
Tabla 7.12: Frecuencia de las respuestas de la pregunta 4 (segunda ronda)

Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea (Pregunta 4)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	en desacuerdo	2	18.2	18.2	18.2
	de acuerdo	5	45.5	45.5	63.6
	fuertemente de acuerdo	4	36.4	36.4	100.0
	Total	11	100.0	100.0	

Fuente: Cálculos de la autora

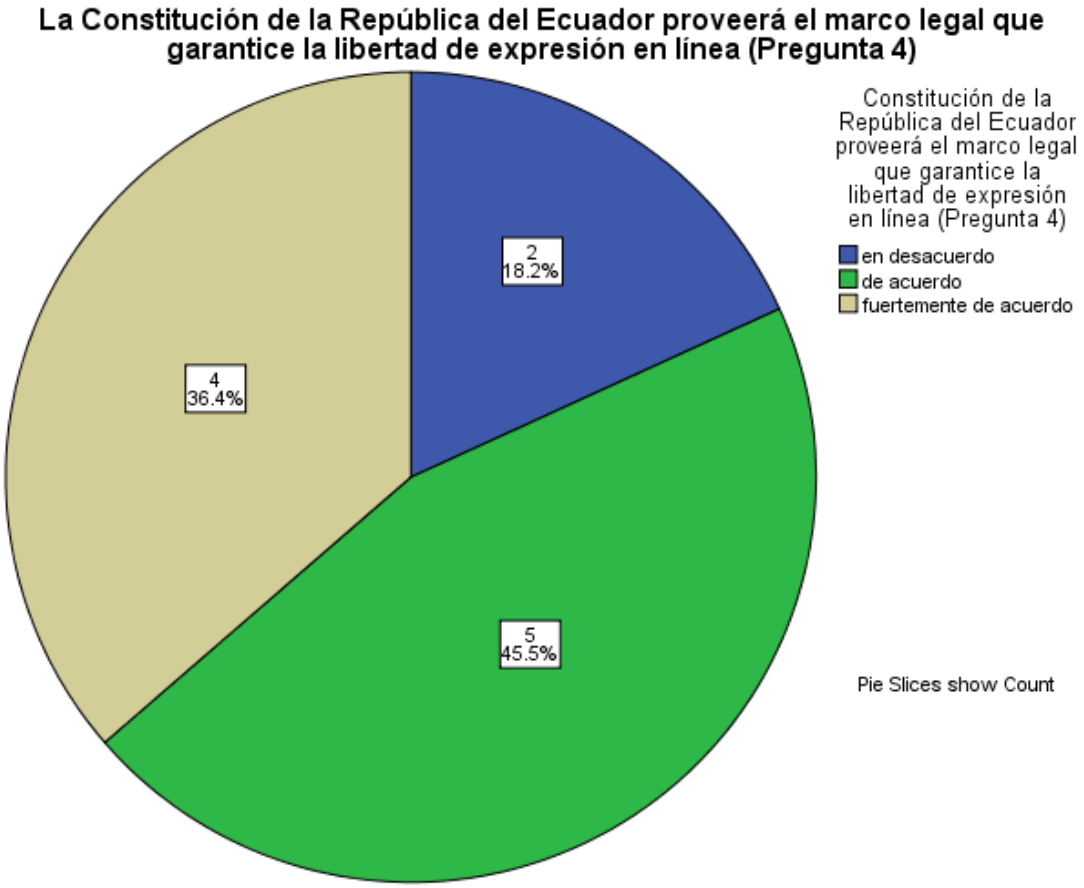
La Figura 7.15 muestra la distribución de frecuencia de las respuestas obtenidas en diagrama de barras para la pregunta 4 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.15: Diagrama de barras para la pregunta 4 (segunda ronda)

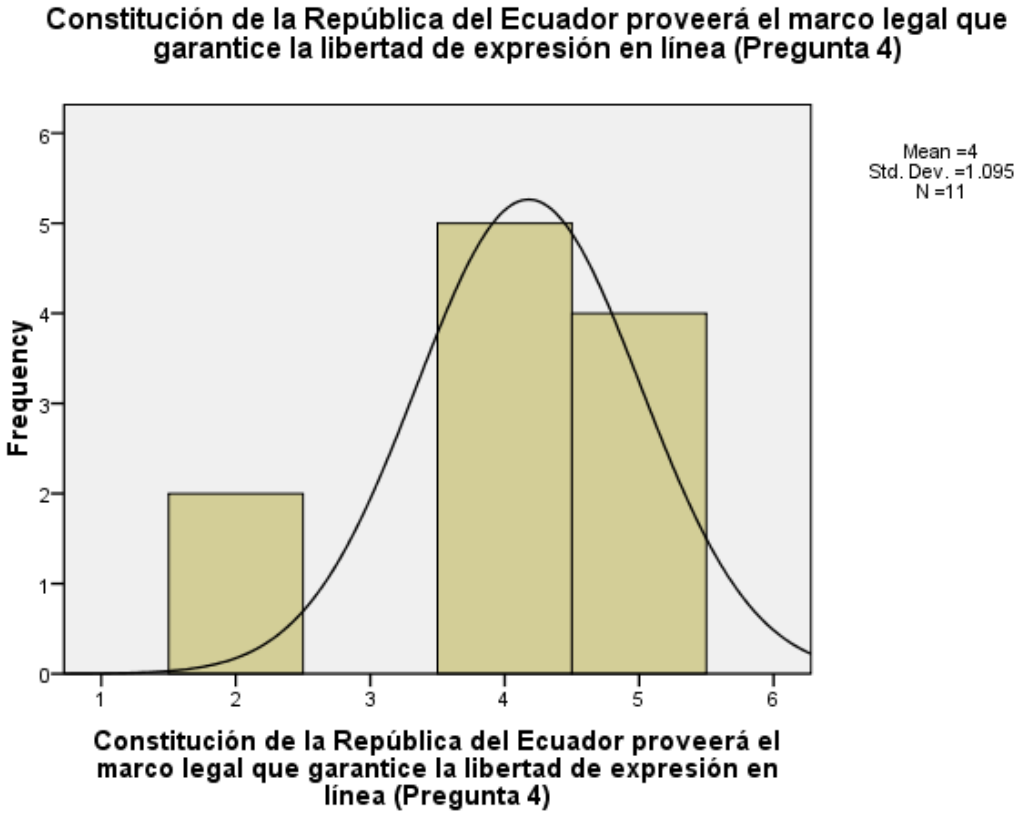
La Figura 7.16 muestra el diagrama de torta de las respuestas obtenidas para la pregunta 4 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.16: Diagrama de torta para la pregunta 4 (segunda ronda)

La Figura 7.17 muestra el histograma y la curva normal de distribución para la pregunta 4.



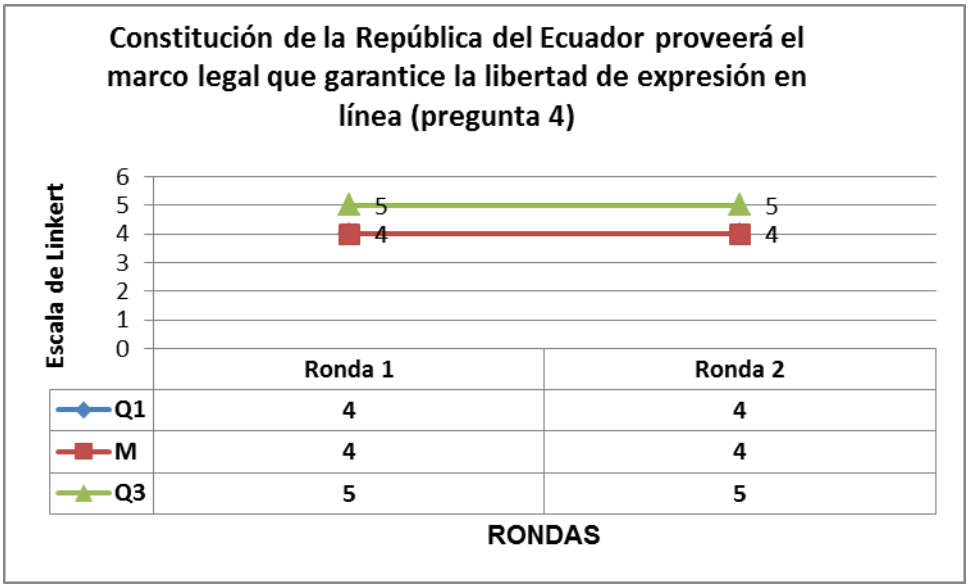
Fuente: Cálculos de la autora

Figura 7.17: **Histograma y curva normal para la pregunta 4**

De las Tablas 7.1 y 7.4 se obtienen los valores del quartil Q1 (25%), la mediana (50%) y el quartil Q3 (75%) tanto para la primera como para la segunda ronda.

En la Figura 7.18 se muestran los valores obtenidos para estos cálculos estadísticos correspondientes a la pregunta 4 y en la cual se puede observar que la línea de Q1 coincide con la línea de la mediana y que el espacio intercuartil (Q3 – Q1) se mantiene constante en el valor 1 entre la primera y segunda ronda, así como la mediana en el valor de 4. De este análisis se puede concluir de que existe un consenso del grupo de expertos

de que la Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea, es decir se puede establecer anticipadamente que la hipótesis nula debe ser rechazada y la hipótesis alternativa ser aceptada, lo cual se someterá a confirmación mediante la realización de la "prueba t de una muestra".



Fuente: Cálculos de la autora

Figura 7.18: Resultados de la primera y segunda rondas para la pregunta 4

En la Tabla 7.13 se muestran las estadísticas para la "prueba t de una muestra" realizada para los resultados obtenidos en la pregunta 4.

Tabla 7.13: Estadísticas para prueba t de una muestra (pregunta 4)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea (Pregunta 4)	11	4.00	1.095	.330

Fuente: Cálculos de la autora

Esta Tabla indica que: existen 11 observaciones (número de expertos), el valor promedio de la muestra ($\bar{x}$) es de 4.00, la desviación estándar es de 1.095 y el error estándar del promedio es 0.330.

En la Tabla 7.14 se muestran los valores de la "prueba t de una muestra" para los resultados obtenidos para la pregunta 4 en la segunda ronda, utilizando un intervalo de confianza del 95%, es decir que el nivel de significancia es de $\alpha = 0.05$. En vista de que la hipótesis nula es $H_{0:}\ \mu \leq 2$, el valor a probar es 2.

Tabla 7.14: Valores de la prueba t de una muestra con un valor a probar igual a 2 (pregunta 4)

One-Sample Test

	Test Value = 2					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea (Pregunta 4)	6.055	10	.000	2.000	1.26	2.74

Fuente: Cálculos de la autora

Esta tabla muestra que el valor observado de t es 6.055 con 10 grados de libertad (n – 1). El valor crítico de t se lo obtiene de la tabla estadística de valores críticos de t; en dicha tabla se puede determinar que para 10 grados de libertad y un nivel de significancia de $\alpha = 0.05$, el valor crítico de t es 1.812. Siendo el valor promedio de la muestra ($\bar{x}$=4.00) mayor que el valor a probar (μ=2), el valor de t es positivo, por lo tanto la región crítica para la prueba de una cola se encontrará en la región de la cola superior (ver Figura 2.1). En este sentido si el valor observado de t es mayor al valor t crítico se debe rechazar la hipótesis nula.

En el presente caso el valor observado de t es de 6.055 el cual es mayor que el valor crítico t de 1.812, por lo que se debe rechazar la hipótesis nula como ya se había establecido preliminarmente y aceptar la hipótesis alternativa.

Se concluye que existe suficiente evidencia estadística para rechazar la hipótesis nula (H_0) y aceptar la hipótesis alternativa (H_1), esto es, que la Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea.

Cabe mencionar que a esta conclusión también se llegó previamente en el análisis efectuado en la sección 7.1.

Pregunta 5

La hipótesis nula (H_o) y la hipótesis alternativa (H_1) planteadas en la sección 2.1 correspondientes a la pregunta 5 formulada a los expertos son:

H_0: El Reglamento de Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y Valor Agregado del Ecuador no atentará contra la privacidad de los usuarios de Internet.

Es decir:

$H_{0:}$ $\mu \leq 2$

H_1: El Reglamento de Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y Valor Agregado del Ecuador atentará contra la privacidad de los usuarios de Internet.

Es decir:

$H_{1:}$ $\mu \geq 4$

La Tabla 7.15 muestra la frecuencia de las respuestas obtenidas para la pregunta 5 en la segunda ronda, en la donde se puede apreciar que 7 (63.7%) de los 11 expertos opinaron estar de acuerdo con que el Reglamento de Abonados de Ecuador atentará contra la privacidad de los usuarios de Internet, 3 (27.3%) estuvieron en desacuerdo y 1 (9.1%) se mantuvo neutral.

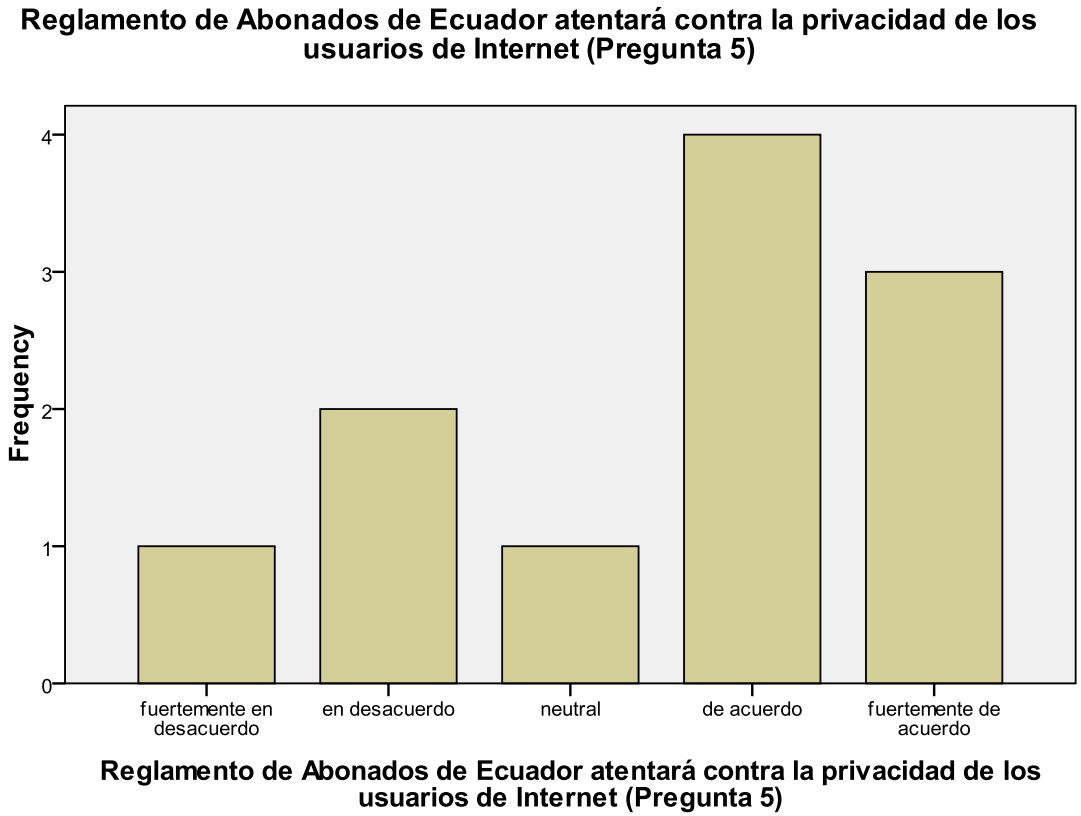
Tabla 7.15: Frecuencia de las respuestas de la pregunta 5 (segunda ronda)

Reglamento de Abonados de Ecuador atentará contra la privacidad de los usuarios de Internet (Pregunta 5)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	fuertemente en desacuerdo	1	9.1	9.1	9.1
	en desacuerdo	2	18.2	18.2	27.3
	neutral	1	9.1	9.1	36.4
	de acuerdo	4	36.4	36.4	72.7
	fuertemente de acuerdo	3	27.3	27.3	100.0
	Total	11	100.0	100.0	

Fuente: Cálculos de la autora

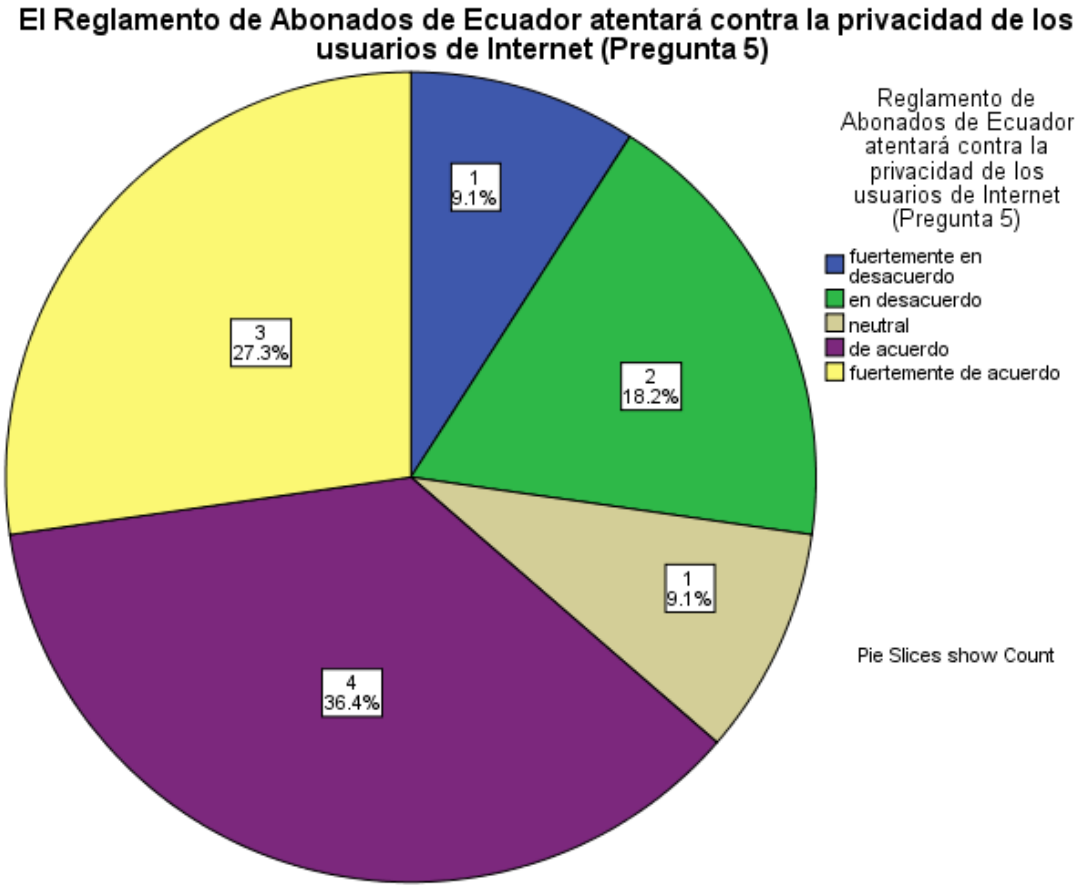
La Figura 7.19 muestra la distribución de frecuencia de las respuestas obtenidas en diagrama de barras para la pregunta 5 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.19: Diagrama de barras para la pregunta 5 (segunda ronda)

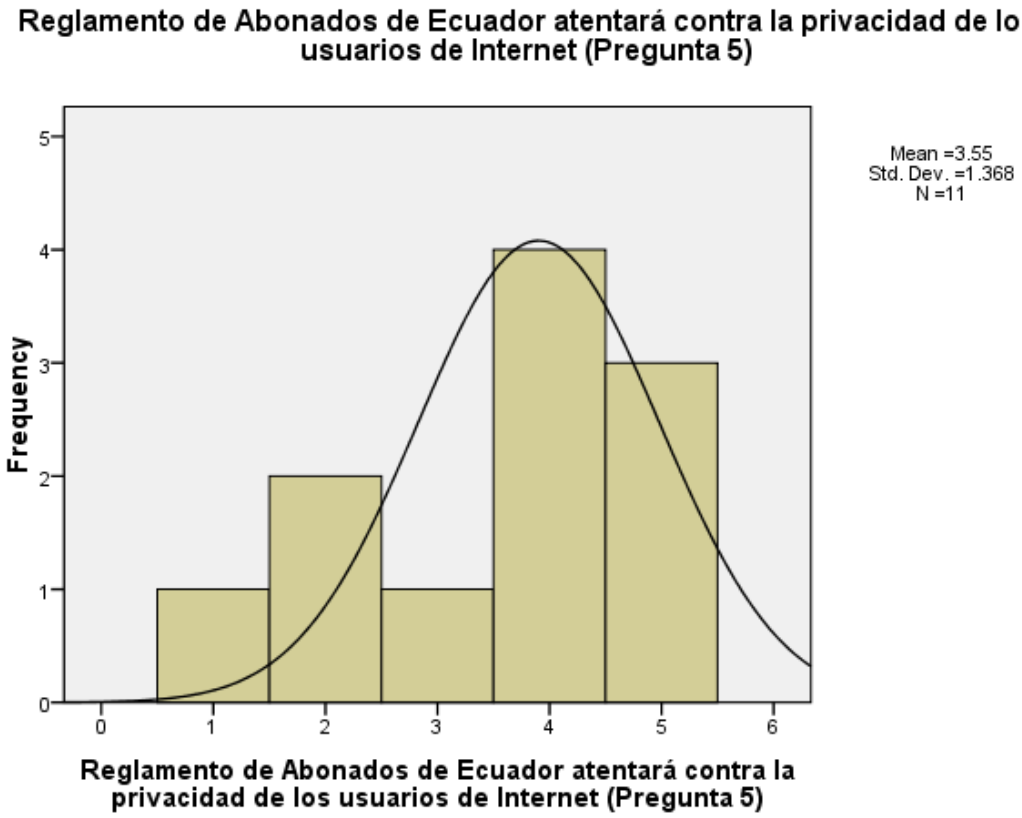
La Figura 7.20 muestra el diagrama de torta de las respuestas obtenidas para la pregunta 5 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.20: Diagrama de torta para la pregunta 5 (segunda ronda)

La Figura 7.21 muestra el histograma y la curva normal de distribución para la pregunta 5.



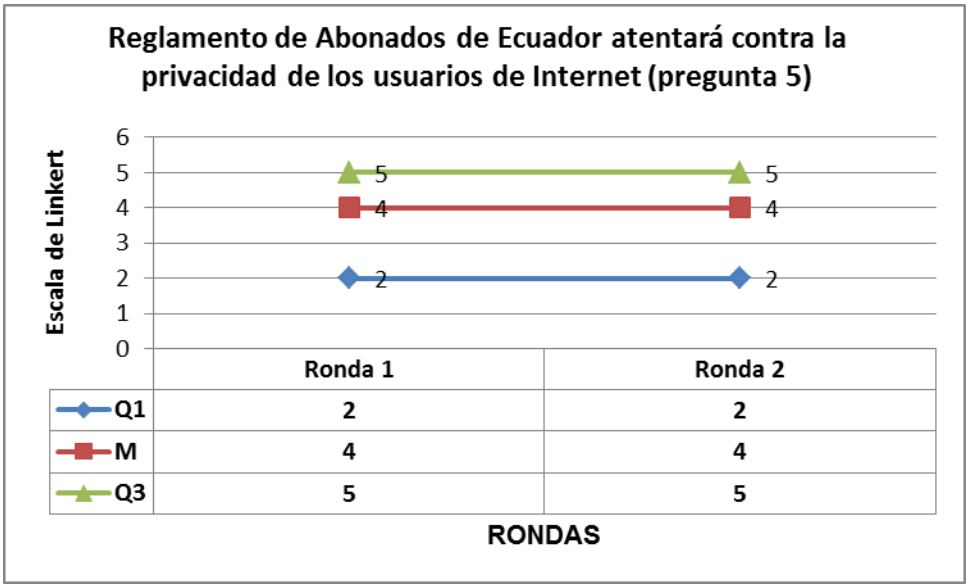
Fuente: Cálculos de la autora

Figura 7.21: **Histograma y curva normal para la pregunta 5**

De las Tablas 7.1 y 7.4 se obtienen los valores del quartil Q1 (25%), la mediana (50%) y el quartil Q3 (75%) tanto para la primera como para la segunda ronda.

En la Figura 7.22 se muestran los valores obtenidos para estos cálculos estadísticos correspondientes a la pregunta 5 y en la cual se puede observar que el espacio intercuartil (Q3 – Q1) se mantiene constante en el valor 3 entre la primera y segunda ronda, así como también la mediana en el valor de 4. De este análisis se puede concluir de que existe un consenso del grupo de expertos de que el Reglamento de Abonados de

Ecuador atentará contra la privacidad de los usuarios de Internet, es decir se puede establecer que la hipótesis nula debe ser rechazada y la hipótesis alternativa ser aceptada, lo cual se someterá a confirmación mediante la realización de la "prueba t de una muestra".



Fuente: Cálculos de la autora

Figura 7.22: Resultados de la primera y segunda rondas para la pregunta 5

En la Tabla 7.16 se muestran las estadísticas para la "prueba t de una muestra" realizada para los resultados obtenidos en la pregunta 5.

Tabla 7.16: Estadísticas para prueba t de una muestra (pregunta 5)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Reglamento de Abonados de Ecuador atentará contra la privacidad de los usuarios de Internet (Pregunta 5)	11	3.55	1.368	.413

Fuente: Cálculos de la autora

Esta Tabla indica que: existen 11 observaciones (número de expertos), el valor promedio de la muestra ($\bar{x}$) es de 3.55, la desviación estándar es de 1.368 y el error estándar del promedio es 0.413.

En la Tabla 7.17 se muestran los valores de la "prueba t de una muestra" para los resultados obtenidos para la pregunta 5 en la segunda ronda, utilizando un intervalo de confianza del 95%, es decir que el nivel de significancia es de $\alpha = 0.05$. En vista de que la hipótesis nula es $H_{0:}\ \mu \leq 2$, el valor a probar es 2.

Tabla 7.17: Valores de la prueba t de una muestra con un valor a probar igual a 2 (pregunta 5)

One-Sample Test

	Test Value = 2					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Reglamento de Abonados de Ecuador atentará contra la privacidad de los usuarios de Internet (Pregunta 5)	3.746	10	.004	1.545	.63	2.46

Fuente: Cálculos de la autora

Esta tabla muestra que el valor observado de t es 3.746 con 10 grados de libertad (n – 1). El valor crítico de t se lo obtiene de la tabla estadística de valores críticos de t; en dicha tabla se puede determinar que para 10 grados de libertad y un nivel de significancia de $\alpha = 0.05$, el valor crítico de t es 1.812. Siendo el valor promedio de la muestra ($\bar{x}$=3.55) mayor que el valor a probar (μ=2), el valor de t es positivo, por lo tanto la región crítica para la prueba de una cola se encontrará en la región de la cola superior (ver Figura 2.1). En este sentido si el valor observado de t es mayor al valor t crítico se debe rechazar la hipótesis nula.

En el presente caso el valor observado de t es de 3.746 el cual es mayor que el valor crítico t de 1.812, por lo que se debe rechazar la hipótesis nula como ya se había establecido preliminarmente y aceptar la hipótesis alternativa.

Para confirmar aún más esta decisión, se puede efectuar una prueba t de una muestra para un valor de prueba de 4, en vista de que H_1: $\mu \geq 4$.

Siendo el valor promedio de la muestra ($\bar{x}$=3.55) menor que el valor a probar (μ=4), el valor de t es negativo, por lo tanto la región crítica para la prueba de una cola se encontrará en la región de la cola inferior (ver Figura 2.1). En este sentido si el valor observado de t es menor al valor t crítico se debe rechazar la hipótesis alternativa.

En la Tabla 7.18 se muestran los valores de la prueba estadística t de una muestra con el valor a probar igual a 4.

Tabla 7.18: Valores de la prueba t de una muestra con un valor a probar igual a 4 (pregunta 5)

One-Sample Test

	Test Value = 4					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Reglamento de Abonados de Ecuador atentará contra la privacidad de los usuarios de Internet (Pregunta 5)	-1.102	10	.296	-.455	-1.37	.46

Fuente: Cálculos de la autora

Esta tabla indica que el valor observado de t es igual a -1.102 que es mayor al valor crítico t de -1.812, por lo que se confirma que se debe aceptar la hipótesis alternativa.

Se concluye que existe suficiente evidencia estadística para concluir que se debe rechazar la hipótesis nula (Ho) y aceptar hipótesis alternativa (H_1), esto es, que el Reglamento de Abonados del Ecuador atentará contra la privacidad de los usuarios de Internet. Cabe mencionar que a esta conclusión también se llegó previamente en el análisis efectuado en la sección 7.1.

Pregunta 6

La hipótesis nula (H_o) y la hipótesis alternativa (H_1) planteadas en la sección 2.1 correspondientes a la pregunta 6 formulada a los expertos son:

H_0: La Ley Orgánica de Comunicación del Ecuador no constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet.

Es decir:

$H_{0:}$ $\mu \leq 2$

H_1: La Ley Orgánica de Comunicación del Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet.

Es decir:

$H_{1:}$ $\mu \geq 4$

La Tabla 7.19 muestra la frecuencia de las respuestas obtenidas para la pregunta 6 en la segunda ronda, en la donde se puede apreciar que 8 (72.8%) de los 11 expertos opinaron estar de acuerdo con que el Reglamento de Abonados de Ecuador atentará contra la privacidad de los usuarios de Internet, 2 (18.2%) estuvieron en desacuerdo y 1 (9.1%) se mantuvo neutral.

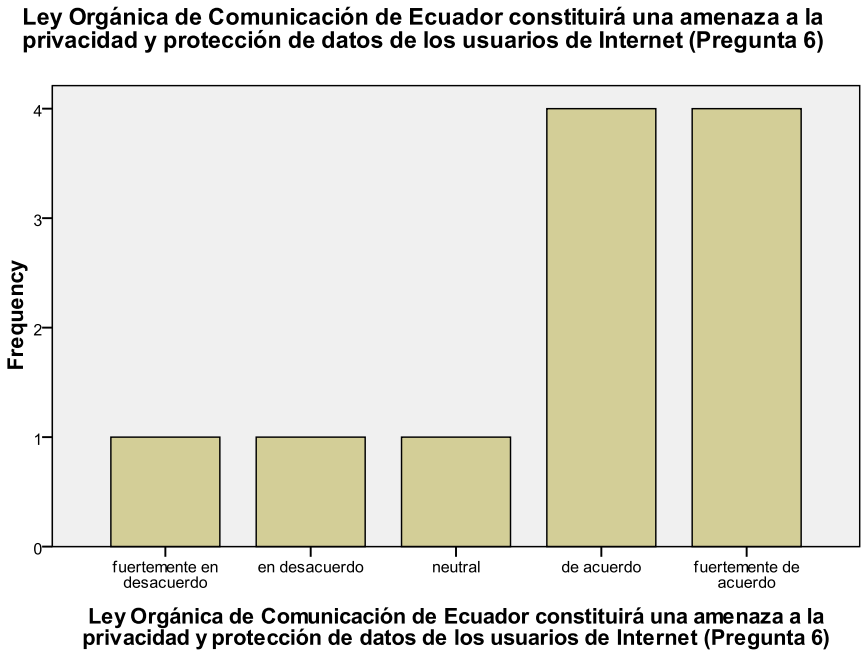
Tabla 7.19: Frecuencia de las respuestas de la pregunta 6 (segunda ronda)

Ley Orgánica de Comunicación de Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet (Pregunta 6)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	fuertemente en desacuerdo	1	9.1	9.1	9.1
	en desacuerdo	1	9.1	9.1	18.2
	neutral	1	9.1	9.1	27.3
	de acuerdo	4	36.4	36.4	63.6
	fuertemente de acuerdo	4	36.4	36.4	100.0
	Total	11	100.0	100.0	

Fuente: Cálculos de la autora

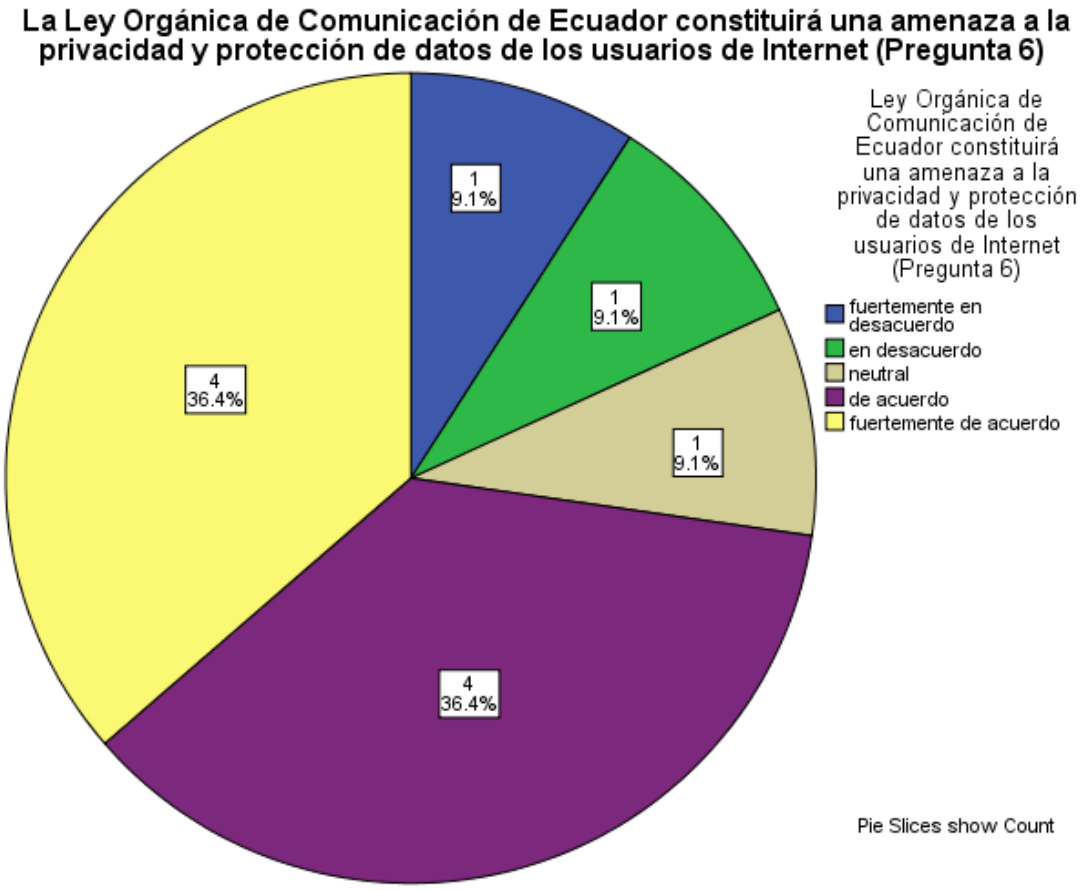
La Figura 7.23 muestra la distribución de frecuencia de las respuestas obtenidas en diagrama de barras para la pregunta 6 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.23: Diagrama de barras para la pregunta 6 (segunda ronda)

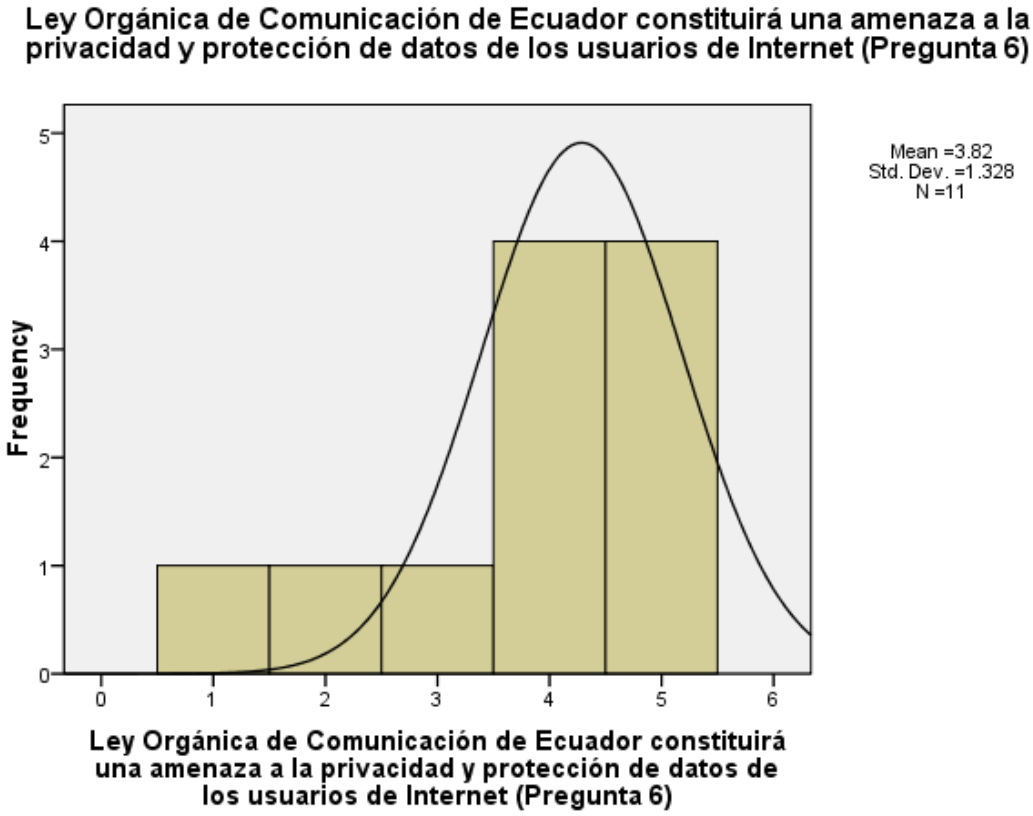
La Figura 7.24 muestra el diagrama de torta de las respuestas obtenidas para la pregunta 6 en la segunda ronda.



Fuente: Cálculos de la autora

Figura 7.24: Diagrama de torta para la pregunta 6 (segunda ronda)

La Figura 7.25 muestra el histograma y la curva normal de distribución para la pregunta 6.



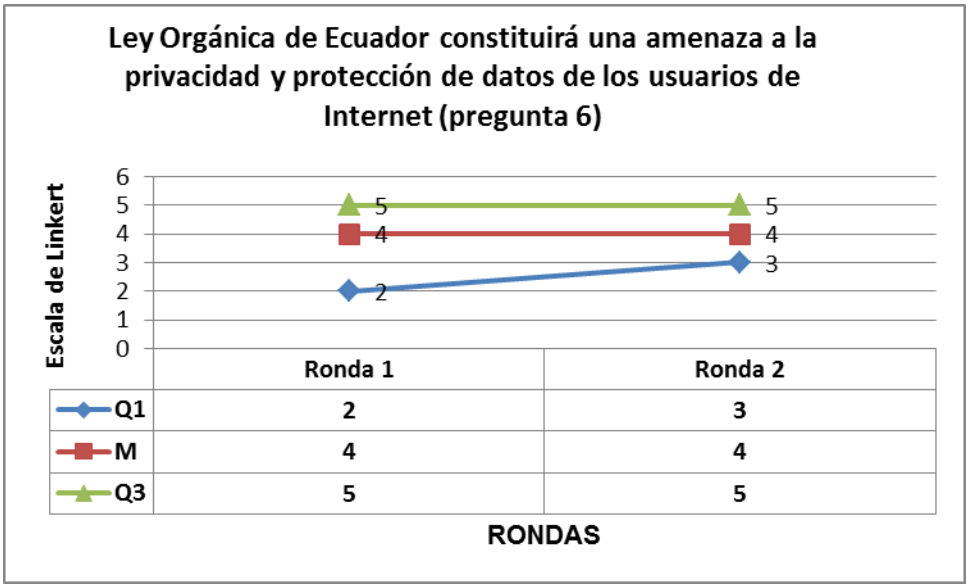
Fuente: Cálculos de la autora

Figura 7.25: **Histograma y curva normal para la pregunta 6**

De las Tablas 7.1 y 7.4 se obtienen los valores del quartil Q1 (25%), la mediana (50%) y el quartil Q3 (75%) tanto para la primera como para la segunda ronda.

En la Figura 7.26 se muestran los valores obtenidos para estos cálculos estadísticos correspondientes a la pregunta 6 y en la cual se puede observar que el espacio intercuartil (Q3 – Q1) se reduce de un valor de 3 a un valor de 2 y que la mediana permanece constante con un valor de 4, entre la primera y la segunda ronda. De este análisis se puede concluir de que existe un consenso del grupo de expertos de que la Ley

Orgánica de Comunicación del Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet, es decir se puede establecer que la hipótesis nula debe ser rechazada y la hipótesis alternativa ser aceptada, lo cual se someterá a confirmación mediante la realización de la "prueba t de una muestra".



Fuente: Cálculos de la autora

Figura 7.26: Resultados de la primera y segunda rondas para la pregunta 6

En la Tabla 7.20 se muestran las estadísticas para la "prueba t de una muestra" realizada para los resultados obtenidos en la pregunta 6.

Tabla 7.20: Estadísticas para prueba t de una muestra (pregunta 6)

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Ley Orgánica de Comunicación de Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet (Pregunta 6)	11	3.82	1.328	.400

Fuente: Cálculos de la autora

Esta Tabla indica que: existen 11 observaciones (número de expertos), el valor promedio de la muestra ($\bar{x}$) es de 3.82, la desviación estándar es de 1.328 y el error estándar del promedio es 0.400.

En la Tabla 7.21 se muestran los valores de la prueba estadística t de una muestra para los resultados obtenidos para la pregunta 6 en la segunda ronda, utilizando un intervalo de confianza del 95%, es decir que el nivel de significancia es de $\alpha = 0.05$. En vista de que la hipótesis nula es $H_{0:}\ \mu \leq 2$, el valor a probar es 2.

Tabla 7.21: Valores de la prueba t de una muestra con un valor a probar igual a 2 (pregunta 6)

One-Sample Test

	Test Value = 2					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Ley Orgánica de Comunicación de Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet (Pregunta 6)	4.541	10	.001	1.818	.93	2.71

Fuente: Cálculos de la autora

Esta tabla muestra que el valor observado de t es 4.541 con 10 grados de libertad (n – 1). El valor crítico de t se lo obtiene de la tabla estadística de valores críticos de t; en dicha tabla se puede determinar que para 10 grados de libertad y un nivel de significancia de $\alpha = 0.05$, el valor crítico de t es 1.812. Siendo el valor promedio de la muestra ($\bar{x}$=3.82) mayor que el valor a probar (μ=2), el valor de t es positivo, por lo tanto la región crítica para la prueba de una cola se encontrará en la región de la cola superior (ver Figura 2.1). En este sentido si el valor observado de t es mayor al valor t crítico se debe rechazar la hipótesis nula.

En el presente caso el valor observado de t es de 4.541 el cual es mayor que el valor crítico t de 1.812, por lo que se debe rechazar la hipótesis nula como ya se había establecido preliminarmente y aceptar la hipótesis alternativa.

Para confirmar aún más esta decisión se puede efectuar una prueba t de una muestra para un valor de prueba de 4, en vista de que H_1: $\mu \geq 4$.

Siendo el valor promedio de la muestra ($\bar{x}$=3.82) menor que el valor a probar (μ=4), el valor de t es negativo, por lo tanto la región crítica para la prueba de una cola se encontrará en la región de la cola inferior (ver Figura 2.1). En este sentido si el valor observado de t es menor al valor t crítico se debe rechazar la hipótesis alternativa.

En la Tabla 7.22 se muestran los valores de la "prueba t de una muestra" con el valor a probar igual a 4.

Tabla 7.22: Valores de la prueba t de una muestra con un valor a probar igual a 4 (pregunta 6)

One-Sample Test

	Test Value = 4					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Ley Orgánica de Comunicación de Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet (Pregunta 6)	-.454	10	.659	-.182	-1.07	.71

Fuente: Cálculos de la autora

Esta tabla indica que el valor observado de t es igual a -0.454 que es mayor al valor crítico t de -1.812, por lo que se confirma que se debe aceptar la hipótesis alternativa.

Se concluye que existe suficiente evidencia estadística para concluir que se debe rechazar la hipótesis nula (H_0) y aceptar hipótesis alternativa (H_1), esto es, que la Ley Orgánica de Comunicación del Ecuador constituirá una amenaza a la privacidad y protección de los usuarios de Internet. Cabe mencionar que a esta conclusión también se llegó preliminarmente en el análisis efectuado en la sección 7.2.

La utilización del método Delphi permitió confirmar conclusiones obtenidas previamente durante el desarrollo de la tesis.

La aplicación del método Delphi proporcionó interesantes experiencias que se estima oportuno compartirlas para poder ser utilizado en otras investigaciones. Su uso permitió reclutar expertos en temas especializados que por otros métodos hubiera sido casi imposible lograr en términos de disponibilidad de tiempo y ocupaciones. La característica de este método de que las respuestas individuales de los miembros del grupo se mantienen en forma confidencial, pues lo que se da a conocer en cada ronda es

la opinión del grupo, garantizó la libertad de opinión sobre los temas delicados y sensitivos consultados. Se apreció un involucramiento pleno de los expertos en el procedimiento establecido en el método Delphi manifestado por su disposición de contestar las preguntas en una segunda ronda y en algunos casos, inclusive, de reconsiderar sus respuestas iniciales, motivados quizás por recientes acontecimientos mundiales en que la privacidad de las personas, organizaciones y Estados se han visto afectadas.

Unas de las dificultades que se necesitó superar fue seleccionar los expertos y recibir su aceptación de participar en la investigación, y el inconveniente más serio presentado fue el tiempo de espera en recibir las respuestas del total de los miembros del grupo para no tener datos perdidos. Es necesario mencionar también que para evaluar estadísticamente las respuestas fue necesario conocer el manejo del software estadístico SPSS.

Conclusiones

1. Los Estados que deciden filtrar el Internet establecen una falange de leyes y medidas técnicas para bloquear a sus ciudadanos el acceso o la publicación de información en línea.
2. La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación.
3. Los levantamientos pro democráticos ocurridos en el medio oriente en el 2011 han demostrado que Internet se ha convertido en un medio crucial por el cual los ciudadanos pueden movilizar y defender reformas políticas, sociales y económicas.
4. "Reporteros sin Fronteras" ha establecido que existen "Enemigos de Internet" y "Países bajo Vigilancia". En la lista del año 2012 aparecen como enemigos de Internet: Bahréin y Bielorrusia, Arabia Saudita, Birmania, China, Corea del Norte, Cuba, Irán, Uzbekistán, Siria, Turkmenistán y Vietnam.
5. La arquitectura de Internet ha hecho más difícil la aplicación de los derechos de propiedad intelectual y esta situación ha apoyado la creación de redes abiertas (open) y entre pares (peer-to-peer) conocidas como P2P para compartir archivos.
6. En Ecuador se implementará el Centro de Respuesta a Incidentes Informáticos del Ecuador (CERT o CSIRT) para permitir que los usuarios ecuatorianos sean protegidos en su navegación por Internet.
7. En el Ecuador existe el marco legal para sancionar los delitos informáticos. en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del Ecuador, Ley 2002-67, publicada en el Registro Oficial No. 455 del 17 de Abril del 2002.

8. En la Constitución de la República del Ecuador está categóricamente garantizado el derecho de todos los ecuatorianos y ecuatorianas para gozar plenamente de la libertad de expresión, libertad de acceso a Internet, libertad de expresión en Internet, libertad de información, a la privacidad o intimidad y a la protección de datos personales. Después del análisis efectuado de los 3 casos de estudio propuestos, se establece que hasta la presente fecha en el Ecuador, no se han producido evidencias que amenacen la libertad de expresión en línea que gozan los ciudadanos ecuatorianos.
9. El artículo 29.9 del "Reglamento para los Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y Valor Agregado" del CONATEL, atenta contra la privacidad de los usuarios de Internet contraviniendo este derecho consagrado en la Constitución, pues el Estado puede identificar con facilidad y reprimir a cualquier usuario que desde su punto de vista atente contra la seguridad del país.
10. El criterio del grupo de expertos que participaron en la aplicación del método Delphi permitió validar la hipótesis de que la libertad de expresión en línea será un derecho de todas las personas.
11. El criterio del grupo de expertos permitió validar la hipótesis de que en los próximos años no habrá libertad de expresión en línea en todos los países del mundo.
12. El criterio del grupo de expertos permitió validar la hipótesis de que el Centro de Respuesta Global (CRG) brindará la protección y confianza necesarias contra las ciberamenazas que afectan a los usuarios de Internet.
13. El criterio del grupo de expertos permitió validar la hipótesis de que la Constitución de la República del Ecuador proveerá el marco legal que garantice la libertad de expresión en línea.
14. El criterio del grupo de expertos permitió validar la hipótesis de que el Reglamento de Abonados/Clientes-Usuarios de los Servicios de

Telecomunicaciones y Valor Agregado del Ecuador atentará contra la privacidad de los usuarios de Internet.

15. El criterio del grupo de expertos permitió validar la hipótesis de que la Ley Orgánica de Comunicación del Ecuador constituirá una amenaza a la privacidad y protección de datos de los usuarios de Internet.
16. El criterio del grupo de expertos permitió validar la hipótesis de que existirán amenazas de ciberataques a los usuarios de Internet en el país.
17. Existe una coincidencia entre las conclusiones obtenidas previamente en el análisis efectuado durante el desarrollo de la tesis y las conclusiones obtenidas a partir del criterio de los expertos que participaron en la aplicación del método Delphi en la presente investigación.

Recomendaciones

1. Se debe aprovechar las capacidades de las tecnologías de la información y la comunicación para poner en práctica el derecho a la información y fomentar un mayor pluralismo en la circulación de la información y el conocimiento.

2. Los gobiernos del mundo, en colaboración con el sector privado deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TICs.

3. Mejorar el acceso a las tecnologías de la información y la comunicación en el Ecuador para lograr un significativo progreso en la construcción de una Sociedad de la Información incluyente.

4. Implementar un observatorio que se encargue de mantener información actualizada de la situación de la libertad de expresión en línea en el entorno mundial y en el Ecuador y de implementar foros de discusión en línea y presencial.

5. Apoyar la iniciativa de la Superintendencia de Telecomunicaciones de creación del "Centro de Respuesta a Incidentes Informáticos" para fortalecer la ciberseguridad en el país.

6. Plantear por parte de los usuarios de Internet en el Ecuador o los organismos que los representen, una acción administrativa o una acción de protección tendente a lograr la eliminación del artículo 29.9 del "Reglamento para los Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y Valor

Agregado" del CONATEL, por vulnerar el derecho a la privacidad consagrado en la Constitución.

7. Estar pendientes sobre lo que resuelva la Corte Constitucional respecto a la demanda de inconstitucionalidad presentada contra la Ley Orgánica de Comunicación del Ecuador.

8. Incorporar un módulo en la Maestría de Comunicación Pública de Ciencia y Tecnología de la EDCOM sobre "La libertad de expresión en línea: oportunidades y amenazas".

Bibliografía

- Anderson, D, Sweeney D, & Williams T. 1999. *Método Cuantitativo para los Negocios*. México: International Thompson Editores.
- Argyrous, G. 2010. *Statistics for Research with a Guide to SPSS*. London, England: SAGE Publications Ltd.
- Asamblea General de la Organización de las Naciones Unidas 2000, *Resolución 55/2: La Declaración del Milenio. Documento A/RES/55/2*, New York: publicación de las Naciones Unidas.
- Asamblea General de la Organización de las Naciones Unidas 2011, *Promoción y protección del derecho a la libertad de opinión y de expresión*. Documento A/66/290, New York: publicación de las Naciones Unidas.
- Asamblea General de la Organización de las Naciones Unidas 2011, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. Documento A/HRC/17/27,* New York: Publicación de las Naciones Unidas.
- Astirraga, E. 2004, *Prospectiva*, San Sebastián, España: Publicación de la Universidad de Deusto, Facultad de CC.EE y Empresariales.
- Child Online Protection. 2009, *Guidelines for Policy Makers on Child Online Protection*, Ginebra: Publicación de UIT.
- Coakes, S. J., Steed, L. & Ong, C. (2010), *SPSS version 17.0 for Windows. Analysis without Anguish*, Milton, Queensland, Australia: John Wiley & Sons Australia, Ltd.
- Constitución de la República del Ecuador 2008, Quito: Registro Oficial No. 449 del 20 de octubre del 2008.
- Dalkey, N. 1969, *The Delphi Method: and Experimental Study of Group Opinion*, Santa Mónica, California: Rand Corporation.

- Domscheit-Berg, D. 2011. *Dentro de WikiLeaks: Mi etapa en la web más peligrosa del mundo*, Berlín: Econ Verlag.
- Dutton, W, Dopatka, A, Hills, M, Law, G, y Nash, N. 2011. *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology, Shaping the Internet*, Oxford - United Kingdom: Publicación de UNESCO.
- Faris, R & Villeneuve, N 2011, *Access Denied: Measuring Global Internet Filtering*, Cambridge, MA: The MIT Press.
- Freund, J, Miller, I y Miller, M. (2000). *Estadística Matemática con Aplicaciones*, Ney Jersey: Prentice Hall Inc.
- Global Internet Freedom Consortium 2008, *Inform, Connect, and Empower the People*. Visto en http://www.internetfreedom.org/ el 9 de febrero del 2013.
- Kaplan, A M & Haenlein, M 2010, *Users of the world, unite! The challenges and opportunities of social media*, Business Horizons, 53 (1), 59 – 68.
- Martin, B. 1996. *Technology Foresight: a review of recent government exercises*. Paris: OECD Publication.
- Mendel, T, Puddephatt, A, Wagner, B, Hawtin, D y Torres, N. 2012, *Global Survey on Internet Privacy and Freedom of Expression*, Paris: Publicación de la UNESCO.
- Moloney, P, Addis, C L y Lum, T. 2011, *U.S. Initiatives to Promote Global Internet*, Congressional Research Service.
- Neuman, W L 2006, *Social Research Method: Qualitative and Quantitative Approaches*, United States: PearsonEducation Inc.
- Nunnally, J. C. 1978. *Psychometric Theory*. New York: McGraw-Hill Book Company
- Pallant, J. 2011, *SPSS Survival Manual*, Crows Nest, NSW, Australia: Allen & Unwin.

- Reporteros sin Fronteras 2011, *Rebeliones Árabes: Los medios de comunicación, testigos clave de las revoluciones y de los retos del poder*, París: Publicación de Reporteros sin Fronteras.
- Reporters without Frontiers 2012, *Internet Enemies Report*, París: una publicación de Reporteros sin Fronteras.
- Resolución No. TEL-477-16-CONATEL 2012, *Reglamento para los Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y Valor Agregado* , Quito: Suplemento del Registro Oficial 750 del 20 de julio del 2012.
- Sanders, W B & Pinhey, T K 1983, *The conduct of social research*, New York: CBS College Publishing.
- Superintendencia de Telecomunicaciones 2012, *Revista SUPERTEL No. 13*.
- UIT 2003, CMSI-03/GENEVA/DOC/4-S, *Cumbre Mundial de la Sociedad de la Información. Declaración de Principios. Construir la Sociedad de la Información: un desafío global para el nuevo milenio*, Ginebra: Publicación de la UIT.
- UIT 2005, CMSI-05/GENEVA/DOC/5-S, *Cumbre Mundial de la Sociedad de la Información. Plan de Acción*, Ginebra: Publicación de la UIT.
- UIT 2005, CMSI-05/TUNIS/DOC/6-S, *Cumbre Mundial de la Sociedad de la Información. Agenda de Túnez para la Sociedad de la Información*, Ginebra: Publicación de la UIT.
- UIT-D 2010, Comisión de Estudio 1: *Garantía de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad*, Ginebra: Publicación de UIT.
- UIT 2012, *Medición de la Sociedad de la Información*, Ginebra: Publicación de UIT.
- UIT News 2010, *Incremento de las Redes Sociales*, Ginebra: Revista No. 6 de UIT.

- Villao, F 2012, *El Derecho de las Telecomunicaciones en el Ecuador, Segunda Edición*, Guayaquil: Serie Nuestros Valores de la ESPOL.
- Zittrain, J & Palfrey, J 2011, *Access Denied:Internet Filtering: The Politics and Mechanisms of Control*, Cambridge, MA: The MIT Press.

Anexo 1

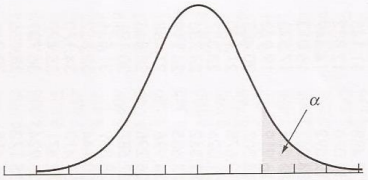
Abreviaturas

ACG	Agenda para la Ciberseguridad Mundial
ACTA	Tratado Comercial Anti-falsificación
BBC	British Broadcasting Corporation
CMSI	Cumbre Mundial de la Sociedad de la Información
CONATEL	Consejo Nacional de Telecomunicaciones
CRG	Centro de Respuesta Global
EDCOM	Escuela de Diseño y Comunicación Visual
CTMI	Conferencia Mundial de Telecomunicaciones Internacionales
FGI	Foro de la Gobernanza de Internet
GEANC	Grupo de Expertos de Alto Nivel sobre Ciberseguridad
IP	Protocolo Internet
ISP	Proveedores de Servicio Internet
LANIC	Registro de Direcciones de Internet para América Latina y el Caribe
NGN	Redes de Próxima Generación
OSCE	Organización para la Seguridad y la Cooperación en Europa
ONU	Organización de las Naciones Unidas
ONI	OpenNet Initiative
PIPA	Acta de prevención de la Propiedad Intelectual
SOPA	Acta para Detener la Piratería en Línea
SUPERTEL	Superintendencia de Telecomunicaciones
TIC	Tecnologías de la Información y Comunicación
UIT	Unión Internacional de Telecomunicaciones
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

Anexo 2

Tabla estadística de valores críticos de t

TABLE 1 *t* CRITICAL VALUES



	Upper tail probability (α)								
Degrees of freedom	**0.15**	**0.10**	**0.05**	**0.025**	**0.015**	**0.01**	**0.005**	**0.001**	**0.0005**
1	1.963	3.078	6.314	12.706	21.205	31.821	63.657	318.309	1273.155
2	1.386	1.886	2.920	4.303	5.643	6.965	9.925	22.327	44.703
3	1.250	1.638	2.353	3.182	3.896	4.541	5.841	10.215	16.326
4	1.190	1.533	2.132	2.776	3.298	3.747	4.604	7.173	10.305
5	1.156	1.476	2.015	2.571	3.003	3.365	4.032	5.893	7.976
6	1.134	1.440	1.943	2.447	2.829	3.143	3.707	5.208	6.788
7	1.119	1.415	1.895	2.365	2.715	2.998	3.499	4.785	6.082
8	1.108	1.397	1.860	2.306	2.634	2.896	3.355	4.501	5.617
9	1.100	1.383	1.833	2.262	2.574	2.821	3.250	4.297	5.291
10	1.093	1.372	1.812	2.228	2.527	2.764	3.169	4.144	5.049
11	1.088	1.363	1.796	2.201	2.491	2.718	3.106	4.025	4.863
12	1.083	1.356	1.782	2.179	2.461	2.681	3.055	3.930	4.717
13	1.079	1.350	1.771	2.160	2.436	2.650	3.012	3.852	4.597
14	1.076	1.345	1.761	2.145	2.415	2.625	2.977	3.787	4.499
15	1.074	1.341	1.753	2.131	2.397	2.602	2.947	3.733	4.417
16	1.071	1.337	1.746	2.120	2.382	2.583	2.921	3.686	4.346
17	1.069	1.333	1.740	2.110	2.368	2.567	2.898	3.646	4.286
18	1.067	1.330	1.734	2.101	2.356	2.552	2.878	3.611	4.233
19	1.066	1.328	1.729	2.093	2.346	2.539	2.861	3.579	4.187
20	1.064	1.325	1.725	2.086	2.336	2.528	2.845	3.552	4.146
21	1.063	1.323	1.721	2.080	2.328	2.518	2.831	3.527	4.109
22	1.061	1.321	1.717	2.074	2.320	2.508	2.819	3.505	4.077
23	1.060	1.319	1.714	2.069	2.313	2.500	2.807	3.485	4.047
24	1.059	1.318	1.711	2.064	2.307	2.492	2.797	3.467	4.021
25	1.058	1.316	1.708	2.060	2.301	2.485	2.787	3.450	3.997
26	1.058	1.315	1.706	2.056	2.296	2.479	2.779	3.435	3.974
27	1.057	1.314	1.703	2.052	2.291	2.473	2.771	3.421	3.954
28	1.056	1.313	1.701	2.048	2.286	2.467	2.763	3.408	3.935
29	1.055	1.311	1.699	2.045	2.282	2.462	2.756	3.396	3.918
30	1.055	1.310	1.697	2.042	2.278	2.457	2.750	3.385	3.902
40	1.050	1.303	1.684	2.021	2.250	2.423	2.704	3.307	3.788
50	1.047	1.299	1.676	2.009	2.234	2.403	2.678	3.261	3.723
60	1.045	1.296	1.671	2.000	2.223	2.390	2.660	3.232	3.681
120	1.041	1.289	1.658	1.980	2.196	2.358	2.617	3.160	3.578
Z critical value	1.036	1.282	1.645	1.960	2.170	2.326	2.576	3.090	3.290
Level of significance for a one-tailed test	**0.15**	**0.10**	**0.05**	**0.025**	**0.015**	**0.01**	**0.005**	**0.001**	**0.0005**
Level of significance for a two-tailed test	**0.30**	**0.20**	**0.10**	**0.05**	**0.03**	**0.02**	**0.01**	**0.002**	**0.001**