Universidad de Chile

Facultad de Derecho

Departamento de Derecho Internacional

ALCANCES DEL "CIBER-TERRORISMO" EN LA SOCIEDAD CONTEMPORÁNEA

Memoria para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales

AUTORA: ARLETTE BELÉN REYES BENZ
PROFESOR GUÍA: JOSÉ ZALAQUETT DAHER

Santiago, Chile

2014

TABLA DE CONTENIDOS

RESUMEN

El objetivo del presente trabajo consiste en analizar la problemática que se genera en torno al concepto emergente de ciber-terrorismo y la tendencia de explotar los medios de comunicación de masas, especialmente Internet, para causar gran impacto en la población.

El planteamiento del problema aborda el desarrollo histórico de los diferentes medios de comunicación de masas (libros, diarios, revistas, radio, cine y televisión) y un análisis particular del caso de Internet, que se presenta en la actualidad como un fenómeno en el cuál convergen todas las formas de comunicación de masas estudiadas.

Luego se analizan las escasas construcciones teóricas existentes sobre ciber-terrorismo, intentando distinguir este concepto de los delitos informáticos comunes, para establecer sus características particulares en base a lo que se ha definido tradicionalmente como terrorismo.

A continuación, se desarrolla un análisis de casos prácticos que se han asociado con el ciber-terrorismo para delimitar si éstos corresponden a una manifestación de este fenómeno propiamente tal.

Este trabajo finaliza con el planteamiento de las formas de regular Internet para controlar los efectos del uso del mismo en delitos informáticos, crímenes cibernéticos y en el ciber-terrorismo.

INTRODUCCIÓN

La masificación del uso de Internet y de las nuevas tecnologías de la información y las comunicaciones (TIC's) en las actividades cotidianas de la mayor parte de la población contemporánea es un hecho innegable y se manifiesta principalmente en la gran cobertura que las mismas han alcanzado en todo el mundo en un espacio reducido de tiempo.

El desarrollo de estas nuevas herramientas otorga posibilidades de innovación inimaginables en el pasado, pero a la vez nos hace vulnerables a raíz de la gran versatilidad de las mismas y de nuestra creciente dependencia de estas tecnologías.

Esto crea la necesidad de desarrollar con mayor precisión conceptual los alcances del llamado ciber-terrorismo, analizando el proceso por el cual los medios de comunicación de masas (MCM), cuyo representante paradigmático en la actualidad es Internet, se han convertido en una herramienta que los actores sub-estatales pueden utilizar para generar gran daño en la población.

Lo anterior se ve reflejado, por un lado, en el uso de medios cibernéticos por parte de grupos terroristas para cometer ataques contra la población civil y la aptitud del uso de

Internet como medio no-convencional de causar terror en la población, además de los alcances imprevisibles de estas acciones de terror informático en un grupo indeterminado de personas, como consecuencia de las características de ubicuidad e invisibilidad que las redes informáticas pueden brindar a este tipo de ataques. Y, por otro lado, en la actuación de los "*hackers*" y los "*crackers*", quienes no persiguen un fin político previamente definido, ni se atribuyen públicamente la comisión de sus actos.

Esto revela la importancia de hacer ciertas distinciones en torno al concepto de ciber-terrorismo, identificando los casos en que Internet es usado como un medio de comunicación y aquellos en que se le puede considerar un medio de ataque, además de las diferencias que existirían entre el ciber-terrorismo y los delitos informáticos en general, cuestión que también nos abre la puerta para identificar las relaciones existentes entre la resistencia civil y el activismo cibernético.

Adicionalmente, se puede realizar un análisis sobre el ciber-terrorismo, identificando sus características propias y sus semejanzas y diferencias con los elementos del terrorismo, tradicionalmente entendido, con especial énfasis en lo referente al uso o amenaza de uso de la fuerza y el objetivo político-ideológico perseguido.

Por último, hay que plantear el problema de seguridad que genera el ciber-terrorismo para los Estados que son víctimas y cuestionarnos sobre la posibilidad de abordar penalmente este problema desde una perspectiva de jurisdicción universal o extra-

territorial, dadas las dificultades que se presentan a la hora de determinar el lugar exacto de la comisión del delito y la incertidumbre en cuanto a la individualización de los afectados.

Lo anterior, a su vez, genera un problema adicional sobre las formas de persecución del terrorismo cibernético, atendiendo al conflicto que se crea entorno a las posibles limitaciones o regulaciones de uso a las que pudieran verse expuestas las redes de comunicación que forma Internet, que en principio deberían ser abiertas y descentralizadas.

Todas estas interrogantes justifican realizar una investigación sobre la materia, precisando conceptos y sistematizando la información existente, dada la necesidad de distinguir entre las distintas conductas que podrían calificarse como ciber-terrorismo frente a la existencia de conductas que pueden ser consideradas como delitos informáticos de carácter común.

CAPÍTULO I

DESDE “LA GUERRA DE LOS MUNDOS” HASTA EL CIBER-TERRORISMO

1. Generalidades.

La comunicación es la forma básica de interacción entre los seres humanos y es el modo en que una persona logra influir en el comportamiento de terceros, modificar su entorno y participar en el desarrollo de la sociedad en la que se desenvuelve.

Las formas de comunicación han evolucionado a lo largo de la historia, desde la comunicación directa, cara a cara, hasta la comunicación a través de ondas electromagnéticas o telecomunicación, que en la actualidad facilita la conexión con personas de todo el mundo mediante dispositivos tecnológicos en constante evolución (teléfonos, celulares, computadores, etc.), permitiendo acortar las distancias físicas y dando origen a una nueva forma de relacionarse, en el marco de un fenómeno que se conoce como globalización.

En esta evolución, los medios de comunicación de masas o medios de comunicación masivos (MCM), han desempeñado un papel fundamental, ya que, junto a los constantes avances tecnológicos, posibilitan influir sobre grandes audiencias, logrando que los

efectos de un mensaje o el potencial uso de las redes de comunicación tengan alcances nunca antes imaginados, dado que son nichos de innovación permanente.

La gran cobertura que han alcanzado las tecnologías de la información en la sociedad contemporánea y la creciente dependencia que se genera hacia ellas, no sólo es señal de que vivimos en una sociedad abierta, globalizada e interconectada, sino que también nos alerta sobre los posibles efectos no deseados del uso de estos mecanismos.

El presente capítulo muestra el desarrollo histórico de los MCM o *mass media* y algunos ejemplos de cómo se han usado para producir gran impacto en la población, analizando cualitativamente diferentes casos que van desde la transmisión por radio de "La Guerra de los Mundos" hasta los recientes casos de ciber-terrorismo.

2. Breve historia de los medios de comunicación de masas.

Usualmente se considera como medios de comunicación masivos los libros, los diarios, las revistas, las películas, la radio, la televisión y el Internet, todos los que pueden definirse como "una forma de comunicación usada para llegar a un gran número de personas"[1].

[1] FOLKERTS, Jean; LACY, Stephen y LARABEE, Ann. *The Media in your life. An Introduction to Mass Communication*. Pearson Education, Inc., Cuarta Edición, Estados Unidos, 2008, p. 4. Traducción libre. *'Mass media: a form of communication (radio, newspapers, television, etc.) used to reach a large number of people.'*

A pesar de que los seres humanos se han comunicado desde la prehistoria a través de diferentes métodos (señales de humo, gestos, el habla, diferentes tipos de escritura, etc.), los inicios de los *mass media* en el mundo occidental están ligados a la invención de la imprenta, que permitió por primera vez difundir un mensaje masivamente[2].

Sin perjuicio de lo anterior, la invención de la radio fue el hecho que logró masificar definitivamente la difusión de un mensaje, dado que los potenciales auditores no necesitaban saber leer para comprender lo que se les transmitía. Este medio no requería mantener una conexión física con la central de emisión, de manera que el mensaje podía llegar tan lejos como la tecnología inalámbrica lo permitiera. Adicionalmente, la radio agregó mayor instantaneidad a la comunicación, posibilitando la entrega de noticias casi en tiempo real.

Más tarde fue el turno de la televisión, que agregó imágenes al sonido, logrando una experiencia más cercana a la realidad en el público, lo que se ve acrecentado con las evoluciones progresivas de los televisores, desde la transmisión de imágenes en blanco y negro hasta la televisión a color y de imágenes de alta definición. Contemporáneamente, la tecnología permite que los espectadores puedan seleccionar programas de televisión entre un amplísimo rango de opciones.

[2] El mundo occidental se vio revolucionado por la invención de la imprenta moderna, no obstante existir precedentes históricos del mismo aparato implementados en China varios siglos antes.

El más reciente medio inventado es Internet, que se ha convertido en poco tiempo en el paradigma de los *mass media*, ya que ha alcanzado una amplia cobertura en el mundo, permitiendo comunicarse con diferentes personas desde cualquier parte del mundo, ver televisión en directo o escuchar música en vivo, utilizando únicamente un computador y una conexión a un servidor.

Sobra decir que la evolución histórica de los medios de comunicación de masas no puede ser analizada como un continuo en el que la invención de un nuevo medio acaba con el uso del medio anterior, sino que más bien "los viejos y los nuevos medios- el cine y la televisión, por ejemplo- coexisten y compiten hasta que termina por establecerse una cierta división del trabajo o de las funciones"[3].

2.1. Libros, diarios y revistas.

La imprenta o prensa para imprimir se inventó en Europa aproximadamente en 1450 y se le atribuye a Johann Gutenberg, aunque hay indicios de que métodos de impresión basados en el uso de tipos móviles habían sido descubiertos mucho antes en Asia, pero sin alcanzar el revuelo que causó en occidente durante el siglo XV. [4]

[3] BRIGGS, Asa y BURKE, Peter. *De Gutenberg a Internet. Una historia social de los medios de comunicación.* Editorial Taurus, Madrid, 2002, p. 58.
[4] Ibíd., p. 27.

A pesar del descontento de algunos grupos ilustrados como clérigos, escribas y las autoridades de la época, que opusieron una resistencia inicial hacia esta forma de comunicación, por razones que algunos autores relacionan con el menoscabo de su posición dentro de la sociedad[5] (ya que la invención de la imprenta socavó lo que se ha descrito como el monopolio de la información por parte de la Iglesia en el Medioevo[6]) la imprenta penetró rápidamente en los círculos de intelectuales de la época, transformándose en el principal medio de difusión masiva existente hasta esa fecha.

En un primer momento, el libro que se imprimió masivamente fue la Biblia (1456), para luego pasar a todo tipo de libros, en diferentes formatos, dependiendo de la manera en que evolucionaban las técnicas de impresión y los hábitos de lectura[7].

Rápidamente, el libro y el impreso penetraron en todas partes, primeramente por medio de librerías establecidas, sedentarias, especializadas y bien conocidas por las autoridades, pero también por medio de una multitud de revendedores regulares e irregulares[8], que ayudaron a aumentar el área de cobertura y en consecuencia el número de lectores y receptores del mensaje transmitido.

Por supuesto, en los primeros siglos posteriores a la invención de la imprenta, el uso de este medio de comunicación masiva dependía en gran medida de los medios de

[5] Ibíd., p. 30.
[6] Ibíd., p. 93.
[7] Ibíd., pp. 34 y 35.
[8] BARBIER, Frédéric y BERTO LAVENIR, Catherine. *Historia de los medios: de Diderot a Internet.* Ediciones Colihue, Buenos Aires 2007, p.42.

transporte físico que se requerían para hacer llegar los ejemplares impresos a diferentes lugares del mundo, traducidos en diversas lenguas[9]. Por ello, en los países de América sólo las elites tenían acceso a los libros escritos de la época, ya que el costo del transporte de los ejemplares desde Europa hacía incrementar significativamente su valor.

Junto con la creación de la imprenta y la popularización de su uso, la progresiva alfabetización de la población produjo un cambio en la vida cotidiana de las personas, con lo que se generó un aumento de la cantidad de empleos relacionados con la escritura, los que gozaban de un elevado status social[10], ya que "las vías de ascenso social pasaban igualmente por la educación y por la apropiación de una cultura letrada"[11]. Sin embargo, la importancia de la imprenta radicó en que ponía el conocimiento al alcance de un público más extenso, facilitando a las generaciones posteriores la posibilidad de construir sobre el trabajo intelectual de las generaciones anteriores.[12]

Con el pasar de los años, el periódico y el folletín, junto con la novela, se volvieron cada vez más importantes, destacándose como los principales medios de comunicación

[9] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 39.
[10] Ibíd., p. 46.
[11] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 128.
[12] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 31.

entre los años 1815-1870[13], ya que durante ese periodo se alcanzó en Occidente uno de los más altos niveles de cobertura y diversidad editorial desde los inicios de la imprenta.

Sin perjuicio de lo anterior, en un comienzo, para la mayoría de la población, leer era una habilidad muy difícil de adquirir, lo que propició el nacimiento de un mercado de imágenes impresas[14], que sentaron las bases de la impresión de revistas, "como una expresión intermedia entre los libros, de contenido trascendente, y los periódicos, de preponderante actualidad"[15], que se conocieron por primera vez en Bélgica en el año 1605.

Se ha sostenido que "una consecuencia importante de la invención de la imprenta fue la implicación más estrecha de los empresarios en el proceso de difusión de conocimientos"[16], ya que las utilidades eran crecientes y los mercados diversos. Además, el material impreso estimuló la conciencia política de las personas. A su vez, una conciencia política más aguda condujo al auge del consumo de material impreso[17], haciendo que la impresión de libros, diarios y revistas se transformara en un negocio muy rentable.

[13] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 132.
[14] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 50.
[15]CASERMEIRO, Alicia. *Surgimiento, desarrollo y adopción de los principales medios masivos de comunicación*. 1993.
[16] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 69.
[17] Ibíd., p. 120.

Desde la fecha de la invención de la imprenta hasta fines del siglo XVIII, el principal rol de los libros, diarios y revistas fue la información y la instrucción moral[18], ya que para el monarca, era útil que la población fuera alfabetizada y tuviera un mínimo de educación, aunque era inútil e incluso peligroso, que superara ese mínimo[19]. En cambio, desde los inicios del siglo XIX, esta forma de comunicación se orientó hacia el debate de ideas de carácter político, religioso y filosófico.

Es así como "[l]a revolución industrial y la revolución de las comunicaciones forman parte de un mismo proceso en el que la revolución del trasporte es la primera fase de una secuencia tecnológica que parece tener su propia lógica"[20] y que a largo plazo permitió incrementar el número de lectores de los libros, diarios y revistas impresos en grandes cantidades, principalmente en los países de Europa occidental, permitiendo la difusión de las ideas discutidas en los países desarrollados en los rincones más diversos del mundo.

Como consecuencia de este auge de las comunicaciones impresas de la época, "el nacimiento de la idea de propiedad intelectual fue una respuesta tanto al surgimiento de la sociedad de consumo como a la expansión de la imprenta"[21], ya que los autores de los diferentes libros reclamaron justamente sus derechos sobre las ganancias producidas a

[18] Ibíd., p. 81.
[19] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 49.
[20] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 126.
[21] Ibíd., p. 69.

partir de la impresión y reimpresión de sus obras, además de las utilidades generadas en los diferentes niveles de comercialización.

Una vez que se popularizó y masificó el consumo de libros, diarios y revistas, los precios bajaron y los contenidos se fueron adaptando a las necesidades de la mayoría de las personas que componían estos mercados. Se creó una especie de vulgarización del medio en comento, para formarse luego una especialización de los contenidos difundidos: cada libro, diario y revista enfocaba sus contenidos hacia un grupo determinado de la sociedad, fácilmente identificable respecto de otros grupos[22].

Con la llegada del siglo XX, la circulación de la prensa a precios moderados formó parte del funcionamiento de las democracias representativas modernas, y dio un contenido concreto a lo que es un derecho y un deber para el ciudadano convertido en elector: informarse[23].

Sin embargo, como consecuencia de la diversificación del mercado y de los gustos de los consumidores, el contenido editorial, incluso de la prensa, también se diversificó. Se crearon ofertas variadas respecto de la forma de abordar los mismos temas en debate, dependiendo de la tendencia política del medio en cuestión y de la preferencia de sus lectores.

[22] Por ejemplo, revistas dedicadas a las amas de casa, revistas dedicadas a los jóvenes, etc.
[23] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 151.

2.2. Radio.

La invención de la radio se le atribuye a Guglielmo Marconi, quien en 1897 creó una compañía dedicada a la venta y diseño de aparatos de radio a gran escala, que inicialmente fueron concebidos como telégrafos sin hilos, pero que gradualmente se fueron adaptando hacia la transmisión de sonidos, lo que sentó las bases de la invención del teléfono y de la radio. Este nuevo invento se ganó un espacio importante dentro de los medios de comunicación de la época, alcanzando gran éxito comercial y revolucionando las comunicaciones de principios del siglo XX[24].

La primera emisora con servicio regular del mundo fue KDKA, en Pittsburg, Estados Unidos, que en noviembre de 1920 comenzó a emitir sus transmisiones con el permiso respectivo[25], hasta que en 1927 se promulgó la *Radio-Act* norteamericana que puso fin a la lucha de interferencias y a la audición deficiente.[26]

En un comienzo, la radio era principalmente un medio de información, pero con el pasar de los años su función se fue diversificando. En Estados Unidos, por ejemplo, la NBC (*National Broadcasting Company*) y la CBS (*Columbia Broadcasting System*) surgieron como las grandes redes de radiofonía de ese país, apuntando hacia la oferta de entretenimiento y promoviendo el modelo de financiamiento a través de la publicidad.

[24] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 174 y ss.
[25] FAUS, Ángel. *La era audiovisual. Historia de los primeros cien años de la radio y la televisión*. Ediciones Internacionales Universitarias, Barcelona, 1995, p. 21.
[26] Ibíd., p. 25.

En el Reino Unido, en cambio, la BBC (*British Broadcasting Corporation*) apostó por los programas de educación, donde los espacios culturales tenían una relevancia significativa, adoptando un modelo de financiamiento basado en las regalías y las ventas de los aparatos de emisión, ya que desde el comienzo este medio se estableció como un monopolio otorgado por el Estado[27]. La radio inglesa rechazó la lógica comercial de la radio norteamericana, deseosa de proteger la democracia y de defender el interés público, llegando, por ello, a ser calificada como paternalista[28].

Se ha señalado que "[d]urante la Segunda Guerra Mundial, con su incesante demanda de noticias, la radio demostró su valor como instrumento político y como medio de información. El número de receptores aumentó considerablemente en todos los países de la Europa continental"[29], lo que hace que muchos autores consideren este periodo como la edad de oro de este medio.

La intención de los primeros experimentos radiofónicos era ser oídos desde la mayor distancia posible. Sin embargo, cuando se hizo evidente la potencia de penetración de la radio, el alcance pasó a convertirse en un mero problema técnico de potencia en la emisión[30]. Por ello, se comenzó a discutir más sobre el contenido de las emisiones que sobre su cobertura.

---

[27] BRIGGS, Asa y BURKE, Peter. Op. cit., pp. 183 y 184.
[28] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 261.
[29] HOBSBAWN, Eric. *Historia del siglo XX*. Traducción de Juan Faci, Jordi Ainaud y Carme Castells, Editorial CRÍTICA (Grijalbo Mondadori, S.A.), Buenos Aires, p. 199.
[30] FAUS, Ángel. Op. cit., p. 20.

Aun así, la evolución de la radio fue relativamente lenta. Hacia 1950, las programaciones se movieron desde las ficciones, los dramas radiofónicos, las comedias y los juegos, los cuales fueron desplazados hacia la televisión, hasta la música, que se transformó en el contenido central de las programaciones radiales. La radio se convirtió en un medio esencialmente regional, sostenido por anunciadores locales y con el pasar de los años se masificó el uso de los aparatos FM que ahora se vendían a precios más accesibles[31].

Se ha sostenido que la radio "ha desarrollado una ingente labor de promoción y mecenazgo del patrimonio cultural común, a la vez que ha influido de forma decisiva sobre la totalidad de los movimientos culturales y estéticos del siglo XX"[32]. Esto se debe a que, contrariamente a lo que sucedió con la televisión, que fue impuesta por la industria y por el marketing[33], la radio surgió como respuesta a las demandas de amplios sectores de la sociedad.

[31] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 374.
[32] FAUS, Ángel, Op. cit., p. 14.
[33] Ibíd., p. 20.

2.3. Cine y televisión.

La invención del cine se atribuye a Lois Lumière, quien en 1895 presentó su cinematógrafo a un pequeño grupo de personas en el Gran Café de París[34], paralelamente a los avances realizados por Thomas Edison en Estados Unidos[35].

La versatilidad que permitía esta nueva forma de expresión artística logró penetrar en las preferencias de consumo de la población de los países desarrollados de Occidente, generando fanatismos en torno a artistas, como Charlie Chaplin, que crecieron junto al *boom* del cine y su evolución desde el cine mudo hasta el cine sonoro durante las primeras décadas del siglo XX[36]. Adicionalmente, el cine pasó a convertirse en una fuente inagotable de ingresos y prontamente se empezaron a formar grandes conglomerados en la industria, cuya capital se estableció en Hollywood.

El crecimiento de la industria cinematográfica tuvo un auge durante la Gran Depresión, en 1929 en Estados Unidos, cuando se construyeron grandes salas de cine en diferentes ciudades donde reinaba el desempleo generalizado entre jóvenes y ancianos, lo que permitía pasar el tiempo libre viendo una película, en una época en que las entradas eran muy baratas[37].

[34] BRIGGS, Asa y BURKE, Peter Op. cit., p. 190.
[35] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 205.
[36] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 193.
[37] HOBSBAWN, Eric. Op. cit., p. 109.

A raíz del éxito de este descubrimiento, varios emprendedores de diferentes partes del mundo comenzaron a experimentar con la transmisión de imágenes en movimiento, hasta que finalmente en Gran Bretaña, John Logie Baird, obtuvo en 1929, un permiso de la BBC para lanzar un servicio de televisión experimental[38].

Sin embargo, los intereses creados por los conglomerados de comunicaciones entorno a la industria de la radio retrasaron la masificación de este invento hasta los años cincuenta, cuando las mismas instituciones que habían inaugurado la era de la radio fueron responsables de la era de la televisión[39].

Como consecuencia de lo anterior, fue recién en 1945 cuando la televisión comenzó a ofrecer programas regulares para un público relativamente importante[40], logrando que durante la década de los cincuenta el público masivo de los programas de televisión creciera exponencialmente y de manera explosiva mientras la asistencia al cine descendía[41]. Del mismo modo la televisión pasó, de forma más rápida que la radio, a ofrecer entretenimiento por sobre información y educación, lo que hace que se haya descrito la televisión comercial de los años 1960 como "el medio alienante por excelencia"[42]

[38] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 199.
[39] Ibíd., p. 243.
[40] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 281.
[41] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 263.
[42] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 410.

Después de un periodo de estancamiento, la industria del cine se reestructuró y pasó a difundir sus películas a través de la televisión, los videos domésticos y las redes de cable, uniéndose a la tendencia de formar grandes conglomerados que antes de la Segunda Guerra Mundial ya habían alcanzado notoriedad, como XXth Century Fox, Paramount, Universal y Columbia, entre otras[43]. Este desarrollo, marcó la primacía de la producción televisiva estadounidense en el mercado mundial[44].

Como bien se ha establecido, "[t]odo proceso técnico necesita de un periodo de experimentación al que sigue otro de expansión y, por fin, el necesario tiempo de interiorización, previo a un uso generalizado"[45]. Así, el desarrollo de la televisión en el mundo a lo largo del siglo XX, fue modernizándose en la búsqueda por prestar un mejor servicio a los usuarios, ya sea adoptando nuevas formas de transmisión vía satélite (1960) o aumentando la calidad de la imagen con la televisión a color (1966).

En este sentido, se ha dicho que "[l]a radiotelevisión no es una empresa como las demás: es una empresa de servicios y no de producción de bienes"[46], ya que el potencial de estos medios de comunicación tiene un valor para la comunidad que supera el valor del aparato de recepción en sí mismo.

[43] Ibíd, p. 376.
[44] FAUS, Ángel. Op. cit., p. 282.
[45] Ibíd, p. 248.
[46] Ibíd, p. 301.

2.4. Internet[47].

Todo comenzó con una red limitada llamada ARPANET que permitía compartir información entre universidades y centros de investigación, gracias al desarrollo de proyectos de investigación militar del Pentágono, a principios de los años setenta[48].

Entre 1993 y 1994, se convirtió en una red abierta a todo el mundo[49], utilizando lo que hoy conocemos como *World Wide Web*, que permite la interconexión global de una red de computadoras que pueden compartir información a través de un protocolo común denominado *Internet Protocol* o IP[50].

Su *boom* se vivió hacia fines del siglo XX, cuando numerosos empresarios invirtieron grandes sumas de dinero para potenciar el desarrollo de "páginas Web" con diferentes nombres de dominio, sobrevalorando la potencialidad comercial de los mismos, que se veían como una fuente de riqueza inagotable.

En el curso del presente siglo, la población aprendió a usar Internet como una herramienta para facilitar las tareas tradicionales, pero no como un fin en sí mismo, ampliando el mercado de oferentes de este servicio y de fabricantes de *software* y

[47] Un análisis más exhaustivo sobre la historia de Internet y sus características se realizará en el Capítulo II.
[48] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 395.
[49] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 343.
[50] OVALLE, José Ignacio. *Derecho de las Telecomunicaciones.* Santiago, 2010, p. 14.

computadores, lo que a su vez fue permitiendo un aumento de la cobertura y la cantidad de usuarios de la Web.

Internet es, sin duda, el medio de comunicación que ha causado más controversias en el último tiempo, ya que permite que se generen situaciones que no se pueden solucionar solamente a partir de su asimilación con los antiguos problemas que se planteaban en torno a las emisiones de la radio o de la televisión (como aspectos de propiedad intelectual, responsabilidad por los contenidos emitidos, etc.). Ello ha generado una serie de vacíos legales frente a la vorágine de descubrimientos de posibles usos de la red.

En suma, esta red, al ser un medio de comunicación de reciente existencia, ha planteado nuevos desafíos para el Derecho, en cuando a la forma en que se lo regula y el modo en que esto afecta a sus cientos de millones de usuarios alrededor del mundo.

3. Uso de los medios de comunicación de masas para producir gran impacto en la población.

Los autores concuerdan en que los medios de comunicación ejercen influencia sobre la población, ya que se ha notado que éstos “ayudan a definir una comunidad y una nación a través de los eventos que ellos cubren, las voces que nos traen y las historias

que nos cuentan"[51]. A partir de esta afirmación es posible identificar casos en que los medios de comunicación de masas han desempeñado un papel fundamental en la forma en que se comportan las personas y la reacción que manifiestan tanto de manera individual, como de manera colectiva, frente a ciertos estímulos predeterminados.

John Street[52], por ejemplo, enuncia algunos casos emblemáticos como el tiroteo en Columbine High School, en Ohio, en 1999 o el caso de Orson Welles y la dramatización de "La Guerra de los Mundos" en 1938. Otros[53], destacan la influencia de la publicidad de marcas reconocidas mundialmente o las reacciones de las personas frente a la cobertura televisiva de un evento mediático.

Adicionalmente, se ha observado que la influencia de los medios de comunicación masivos en la población es tan importante que muchos gobiernos quieren controlarlos a través de diferentes métodos como la censura de información[54], el secretismo, la propaganda y la regulación[55]. Incluso algunos autores[56] analizan el poder que han llegado a ejercer las diferentes agencias reguladoras en países como Estados Unidos, donde la FCC (*Federal Communications Commission*) desempeña un papel

[51] FOLKERTS, Jean; LACY, Stephen y LARABEE, Ann. Op. cit., p. 2.
[52] STREET, John. *Mass Media, Politics and Democracy*. PALGRAVE, Nueva York, 2001, pp. 80 y ss.
[53] FOLKERTS, Jean; LACY, Stephen y LARABEE, Ann. Op. cit., pp. 262 y ss.
[54] Que tiene antecedentes tan antiguos como la censura ejercida por la Iglesia católica con su Índice de libros prohibidos.
[55] STREET, John. Op. Cit., pp. 103 y ss.
[56] DIZARD, Wilson. *Old Media/ New Media: Mass communication in the information age*. Longman, Nueva York, 1994, p. 71.

significativo a la hora de decidir qué contenidos se difunden a través de los *mass media* de ese país.

Dentro de los diferentes estudios sobre los medios de comunicación y su influencia en la población, también se ha analizado la influencia que pueden tener los *mass media* en las decisiones políticas de los individuos, en el sentido de que la información que se transmite a través de los diferentes medios es la estructura a base de la cual los ciudadanos forman su opinión sobre el mundo y la justificación de sus actos[57].

En este sentido, también se ha incluido como un elemento del análisis el problema de quién o quiénes controlan los medios de comunicación de masas en un país determinado, dado que a partir de la identificación de estos grupos, se pueden deducir los intereses políticos y económicos que subyacen la línea editorial de un canal o de un periódico en particular, permitiendo a su vez identificar la visión de mundo que comparten, consciente o inconscientemente, las personas que consumen esos productos mediáticos regularmente.

Lo anterior se explica debido a que "[e]l poder sobre los medios es producto de decisiones políticas, valores y procesos. Entonces, al pensar sobre las consecuencias políticas de la propiedad de los medios necesitamos examinar los intereses comerciales

[57] STREET, John. Op. Cit., p. 7. '*In Western liberal democracies, the mass media have claimed the right to represent the people and to uphold democracy, and the consumers of newspapers and television have come to treat this media sources as the basis on which to think and act in the world'*.

de los conglomerados de medios, las prácticas de sus dueños y las políticas del gobierno"[58].

Tal es el poder que los medios de comunicación de masas pueden ejercer sobre la conducta de diversos sectores de la población que, ya en 1978, en la Vigésima Sesión General de la UNESCO, se estableció la "Declaración de Principios Fundamentales relativos a las Contribuciones de los Medios de Comunicación para el Fortalecimiento de la Paz y la Comprensión Internacional, la Promoción de los Derechos Humanos y la Oposición al Racismo, el Apartheid y la Iniciación a la Guerra", destacando el rol fundamental que tienen los medios de comunicación en la eliminación de las diferencias que dividen a los pueblos, la educación de los más jóvenes y en definitiva la representación de las opiniones de todos los sectores de la comunidad internacional como una forma de promoción y difusión de los derechos humanos.

En consecuencia, reconociendo la gran influencia que ejercen los medios de comunicación de masas en la sociedad contemporánea, a continuación vamos a analizar algunos casos en que se ha hecho uso de éstos para producir gran impacto en la población.

[58] SREET, John. Op. Cit., p. 144. '*Media power is product of political decisions values and processes. So in thinking about the political consequences of media ownership we need to examine the commercial interests of media conglomerates, the practices of owners and the policies of government'.*

3.1. "La Guerra de los Mundos".

Este hecho marcó un hito en la historia de la radiofonía y es citado por diferentes autores como prueba de la influencia y credibilidad que había alcanzado la radio en el mundo entero durante el periodo de entreguerras.

Básicamente, consistió en la transmisión, a través de la cadena de emisoras estadounidenses de la CBS, del radio teatro "Invasión desde Marte" (*Invasion from Mars*), una adaptación libre de la obra "La Guerra de los Mundos" (*The War of the Worlds*) de H.G. Wells, dentro del programa "Teatro Mercurio al Aire" (*Mercury Theatre on the Air*), realizada por Orson Welles durante el penúltimo día de octubre del año 1938.[59]

Esta transmisión, planeada como una estrategia para entretener a los oyentes en el marco de la celebración de *Halloween*[60], sembró el pánico colectivo entre sus oyentes, que se calculan en millones de personas a lo largo del país, quienes creyeron que verdaderamente había llegado el fin del mundo, mientras Orson Welles y un grupo de actores especialmente reclutados para la ocasión interpretaban meticulosamente las escenas de la supuesta invasión marciana al planeta Tierra.[61]

[59] FAUS, Ángel. Op. cit., p. 38.
[60] CANTRIL, Hadly. *The Invasion from Mars: A study in the psychology of panic*. Princeton University Press, Washington, 2009, p. 3.
[61] FAUS, Ángel. Op. cit., p. 38.

Las noticias sobre la supuesta invasión se emitieron durante la programación habitual de la emisora y con un ritmo cada vez más frecuente hasta que finalmente se dejó la línea libre al supuesto reportaje realizado en directo por un periodista de la radio con entrevistas a los testigos del pretendido aterrizaje marciano, gritos de la gente, efectos sonoros, opiniones de expertos, etc.[62]

"La Guerra de los Mundos" se convirtió en un símbolo de la radiodifusión de la época, como muestra de la radio-espectáculo o la radio-realidad, demostrando la extraordinaria aceptación de los servicios informativos de la radio, la extensión del medio a nivel de masas, la credibilidad que había alcanzado la radio hasta ese momento y el hecho de haber alcanzado el desarrollo técnico suficiente para hacer posible la "dramatización perfecta"[63].

La popularidad de este evento en el inconsciente colectivo americano se reflejó en una serie de publicaciones y emisiones radiales conmemorativas a lo largo de los años[64]. A pesar de lo irrisorio que puede resultarnos esta situación en la actualidad, esta transmisión, sin precedentes en aquella época, se transformó en una muestra del lado oscuro de los medios de comunicación de masas: la radio, que había mostrado que podía unir a un país haciendo llegar noticias e información a todos los rincones de la nación de

[62] FAUS, Ángel. Op. cit., p. 39.
[63] FAUS, Ángel. Op. cit., p. 39.
[64] KOCH, Howard. *La emisión del pánico*. Centro de Creación Experimental, Cuenca, 2002, p. 5.

manera simultánea, demostró que también podía destruirlo, sembrando el caos y la confusión con la misma velocidad. [65]

Junto con lo anterior, se ha señalado que este evento volvió evidente "el hecho de que la respuesta pública a la cobertura mediática de una catástrofe puede resultar infinitamente más peligrosa y destructiva que el desastre mismo"[66], poniendo sobre la mesa el debate acerca de los insospechados efectos que puede generar el uso de los medios de comunicación de masas en la población.

3.2. Propaganda Nazi durante la Segunda Guerra Mundial.

Si bien es cierto que la propaganda fue utilizada, entre otros, por regímenes comunistas y fascistas, diferentes autores han destacado la influencia de la propaganda nazi antes de y durante la Segunda Guerra Mundial sobre la población alemana e incluso más allá de las fronteras de ese país.

[65] WEINSTOCK, Jeffrey. *Mars attacks! Well, Welles, and radio panic: or, the story of the century.* En BROWNE, Ray y NEIL, Arthur. Ordinary Reactions to Extraordinary Events, Bowling Green State University Popular Press, 2001, p. 218. *'The dark underside of mass media, of the radio which had done so much to unify the United States, suddenly became apparent: not only could it bring the country together by disseminating news and information simultaneously to all corners of the nation, but it could also tear the country apart by communicating shock and panic just as readily'.*

[66] Ibídem. *'It immediately became evident that public response to media coverage of a catastrophe could be many orders of magnitude more dangerous and destructive than the disaster itself'.*

Hitler y Goebbels desempeñaron un rol fundamental en el diseño e implementación de esta propaganda[67] y en el hecho de que este término haya alcanzado una connotación tan negativa a partir de entonces.

La cultura escrita y los medios gozaron de un status reservado durante el régimen de la Alemania nazi. Desde la llegada al poder de Hitler, en 1933, la libertad de prensa fue suprimida. Goebbels organizó un ministerio de propaganda[68] que controlaba cada medio que circulaba en el país, donde uno de los diarios que alcanzó mayor protagonismo fue *Der Stürmer* (El atacante), que se caracterizó por el alto contenido antisemita de sus publicaciones.

Esta escalada comenzó a prepararse ya en 1930 cuando se creó una organización de la radio dentro del partido nazi, cuya finalidad era introducirse en todos los niveles del medio radiofónico (radioemisoras, radioaficionados, radioyentes, etc.). En 1932 la organización nazi de radio fue encomendada a Goebbels, quien posteriormente quedaría a la cabeza del Ministerio de Propaganda. Este Ministerio obligó a todas las radios del país a disponer de un tiempo de emisión reservado al gobierno[69]. Pronto estas emisiones se caracterizaron por tener un alto contenido propagandístico, que exaltaba el

[67] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 244.
[68] BARBIER, Frédéric y BERTO LAVENIR, Catherine. Op. cit., p. 201.
[69] FAUS, Ángel. Op. cit., p. 46.

nacionalismo, llegándose incluso a prohibir en 1935 la retrasmisión de música jazz en todas las emisoras, mientras aumentaba la emisión de música clásica alemana.[70]

La influencia propagandística no sólo se manifestó en la prensa y en la radio, sino que se introdujo en todo el espectro de los medios de comunicación masiva de la época, es decir, cine, teatro, libros e incluso en materiales educativos[71], exaltando mensajes que preparaban a la población para aceptar las medidas legislativas impuestas por el gobierno.

Algunos ejemplos que se citan comúnmente como propaganda nazi en el cine son la película "El triunfo de la voluntad" (1935) y "El judío eterno" (1940), mientras que los libros que alcanzaron mayor popularidad en la época fueron "La revolución nacional-socialista" (1934), "Hitler, El salvador de Alemania" (1935) y, por cierto, "*Mein Kampf*", entre otros.

De esta forma, la propaganda durante el régimen nazi penetró cada aspecto de la sociedad, exaltando las bondades del régimen y las supuestas características casi sobrehumanas de su líder, mediante campañas mediáticas que se intensificaban cada vez que se iba a implementar alguna medida controvertida.

[70] FAUS, Ángel. Op. cit., p. 47.
[71] Artículo publicado en el United States Holocaust Memorial Museum, Washington D.C. Fuente: < http://www.ushmm.org/wlc/es/article.php?ModuleId=10007439> [consultado: 02.12.2012].

3.3. Transmisión televisiva de la Guerra de Vietnam.

La guerra de Vietnam, uno de los conflictos característicos de la Guerra Fría, se produjo entre los años 1964 y 1975, enfrentando a Vietnam del Sur, apoyado por Estados Unidos, contra Vietnam del Norte, apoyado por la Unión Soviética.

Durante este periodo la televisión ya había alcanzado un gran desarrollo en términos de cobertura y calidad de las transmisiones, por lo que la posibilidad de ser testigos a larga distancia de los desastres de la guerra planteó cuestiones básicas tanto acerca de la dependencia de los medios respecto de las fuentes oficiales, como de la influencia de la prensa y la televisión sobre la política norteamericana.[72]

La reacción más destacada frente a esta primera transmisión televisada de una guerra, que cada día se tornaba más impopular, fue el movimiento antibelicista de los jóvenes norteamericanos que se opusieron a ser reclutados para participar en la guerra de Vietnam[73], quitándole respaldo al gobierno de la época mediante el cuestionamiento permanente de los motivos para participar de aquel conflicto sin sentido.

La transmisión televisiva de la guerra de Vietnam generó un impacto importante en la población civil de Estados Unidos, ya que la hizo tomar consciencia de las consecuencias nefastas que podían generar las decisiones de política exterior de ese

[72] BRIGGS, Asa y BURKE, Peter. Op. cit., p. 281.
[73] HOBSBAWN, Eric. Op. cit., p. 241.

país, junto con llevarla a cuestionar las versiones oficiales de las autoridades que se difundían ampliamente en la prensa, como un intento desesperado por conseguir el apoyo de la ciudadanía.

En este sentido, se señala que después de la guerra de Vietnam la forma en que se abordan los conflictos armados no sólo tiene que ver con la estrategia militar, sino que también con el aspecto mediático[74], dada la importancia que los medios pueden alcanzar en la población y la popularidad de una guerra.

3.4. Publicidad de marcas reconocidas mundialmente.

Hacia fines del siglo XX, después del término de la Guerra Fría y junto con la globalización y el auge del modelo económico neoliberal se formó en el inconsciente colectivo de los países subdesarrollados, o en vías de desarrollo, el deseo de imitar las creaciones culturales de los países desarrollados de Occidente, liderados por Estados Unidos.

Bajo este paradigma se formó una suerte de cultura común de los países más o menos urbanizados, que gira en torno a la industria del entretenimiento de masas[75]. Un

[74] RENIZ, Doris. *La información en tiempos de guerra y terrorismo*. En: Revista Javeriana (Ago. 2002). p. 39-55. [en línea] < http://hdl.handle.net/10720/524> [consultado: 25.12.2012].
[75] HOBSBAWN, Eric. Op. cit., p. 504.

rasgo de pertenencia o identidad de los adeptos a este tipo de entretención es el consumo de productos de determinadas marcas (Adidas, Nike, Coca-Cola, etc.).

En este proceso de internacionalización de los mercados y de la homogeneización de las preferencias de los consumidores, la publicidad ha jugado un rol trascendental. Las tendencias de consumo de las grandes masas se orientan al uso de técnicas cada vez más sofisticadas para llegar a la mayor cantidad de personas posible, haciendo uso de los *mass media* en todos sus niveles.

Desde mediados de la década de 1970, se ha debatido extensamente sobre el desequilibrio en el flujo comunicacional entre el primer mundo y el tercero, a menudo con referencia a los conceptos de imperialismo cultural y dependencia cultural[76]. Pareciera ser más fácil que los países en vías de desarrollo adopten costumbres y tendencias de consumo extranjeras en lugar de cultivar sus tradiciones o posicionar sus productos propios en el exterior.

Como una forma de dar cuenta de la situación anterior, el *pop art*, liderado por Andy Warhol, se dedicó a reproducir con la mayor objetividad los íconos visuales del comercialismo estadounidense: latas de sopa, banderas, botellas de Coca-Cola, Marilyn Monroe, etc.[77].

[76] MCQUAIL, Denis. *La acción de los medios.* Amorrortu Editores, Buenos Aires, 1998, p. 420.
[77] HOBSBAWN, Eric. Op. cit., p. 508.

En este sentido, la influencia que se ejerce a través de los medios de comunicación va posicionando de manera casi imperceptible a ciertas marcas como portadoras de un valor en sí mismas, asociado a la juventud, la belleza, el éxito y la felicidad. Esto conduce a las personas a querer poseer estos productos casi sin consideraciones sobre su precio o calidad.

El efecto que ejerce la publicidad sobre la población, a través de los medios, ha sido tan exitoso en conseguir la preferencia de los consumidores sobre determinados productos, que las compañías multinacionales invierten millones de dólares al año sólo por este concepto[78]. Se demuestra así, que "[la] publicidad desempeña un papel decisivo en el comercio mundial y en la forma en que experimentamos y vivimos nuestras vidas. Es parte de nuestro lenguaje y de nuestra cultura. Refleja nuestra manera de pensar acerca de las cosas y la forma en que nos vemos a nosotros mismos"[79].

3.5. Cobertura periodística de los eventos mediáticos generados por catástrofes naturales.

Como muy bien se ha observado, "los medios masivos pueden contribuir a que los individuos se sientan apegados a la comunidad y a la sociedad en general y participen

[78] O'GUINN, Thomas, ALLEN, Chris y SEMENIK, Richard. *Publicidad y comunicación integral de marca*. Thompson Editores, 4ª Edición, México, 2006, p., 7.
[79] Ibíd., p. 8.

en su vida colectiva sobre la base de un sentimiento de simpatía, en especial hacia los que se encuentran en dificultades de diversos tipos"[80].

En este sentido, durante los últimos años, los reportajes y entrevistas en directo de las víctimas de una catástrofe natural como el huracán Katrina en Estados Unidos o el terremoto que afectó a nuestro país en febrero de 2010, son una clara muestra de la influencia que tiene este tipo de cobertura mediática en la población. La principal reacción se relaciona con las cadenas de ayuda material y económica a las víctimas, además de los voluntariados para trabajar en la remoción de escombros y reubicación de los damnificados.

Como consecuencia de lo anterior, cada vez que ocurre una catástrofe natural de proporciones se inicia una serie de actividades en las principales cadenas de prensa, radio y televisión, tanto a nivel nacional como internacional, para intentar cubrir de la manera más completa posible la noticia de la cual todo el mundo quiere enterarse.

Dentro de esta lógica, se producen transmisiones que pueden durar varios días seguidos y que alteran la programación habitual de los canales de televisión, reuniendo a las personas en grupos para contemplar a larga distancia cada detalle de la noticia en secuencias repetidas una y otra vez.

[80]MCQUAIL, Denis. Op. cit., p. 387.

En las personas se desarrolla un alto grado de empatía por la situación de las víctimas de estas catástrofes naturales, lo que los lleva a intentar ayudarlos monetariamente o a cuestionar la acción del gobierno frente a este tipo de fenómenos.

3.6. Ciber-terrorismo.

Es preocupante que el uso que se está dando a Internet y los medios informáticos en la sociedad contemporánea esté afectando, a través de medios intangibles, esferas de la vida de las personas que antes creíamos inviolables.

En este escenario, dentro de los casos más conocidos se destacan los ataques cibernéticos, que tienen por objeto irrumpir en un sistema informático con el objeto de destruir la información contenida en él; los delitos informáticos, que se relacionan con el sabotaje y el robo de información privada; y el ciber-terrorismo, concepto que no ha sido empleado de modo claro o unívoco, sino que se utiliza para definir una amplia gama de hechos en los que se emplea el Internet y diferentes herramientas computacionales para causar impacto en la población.

La característica que comparten todas estas formas de ejercer influencia sobre la población, es el uso de Internet y el hecho de que las personas se sienten particularmente vulnerables frente a estos ataques, toda vez que ellos mismos desconocen muchas veces si existe una forma efectiva de protegerse, dado que hoy en

día el Internet forma parte de la mayor parte de las cosas que hacemos en la cotidianeidad.

El ciber-terrorismo es una nueva forma de causar terror en la población y es una tendencia que aún no ha sido del todo explotada para generar gran destrucción a través de medios fáciles de conseguir (computadores conectados a Internet), que permiten a sus perpetradores mantenerse en el anonimato, garantizar la impunidad y aumentar la sensación de inseguridad de la sociedad civil en general.

4. Importancia de los medios de comunicación de masas en la sociedad del siglo XXI.

A partir de lo anterior, no es difícil entender las razones por las cuales se ha definido a los medios masivos de comunicación como objetos de interés público[81], en el sentido de que la comunicación a nivel de masas es fundamental para el funcionamiento de un Estado, por lo que las tecnologías de las telecomunicaciones no pueden funcionar sin la participación de éste en el proceso de regulación e implementación de las redes de telecomunicación porque se reconoce el beneficio que ellas aportan a toda la comunidad.

[81] MCQUAIL, Denis. Op. cit., p. 27.

Sin perjuicio de la importancia de las telecomunicaciones y de los medios de comunicación de masas para el desarrollo de un país, la orientación sensacionalista a menudo tomada por la prensa periódica masiva y popular, produjo una general pérdida de confianza (del público informado) en los medios como el único o el mejor representante del interés público en la comunicación[82], debido a la persecución de intereses privados por parte de los conglomerados de empresas dedicadas al rubro de las comunicaciones.

Esta desconfianza ha incentivado un cambio de paradigma en los medios de comunicación, que ha evolucionado desde una oferta limitada de contenidos homogéneos a una audiencia masiva- pasiva con efectos indiferenciados, a un modelo en el cual hay muchas fuentes diferentes de contenidos diversificados dirigidos a una audiencia fragmentada y muy activa, cuyos efectos son variados e impredecibles.[83]

El mejor ejemplo de lo anterior es lo que ha sucedido con Internet y las redes sociales (como Facebook y Twitter), que permiten a todas las personas ser emisores y editores de contenidos que se difunden en la red de manera instantánea entre otros usuarios de los mismos servicios, lo que permite crear una comunidad de ciudadanos más críticos y activos.

[82] MCQUAIL, Denis. Op. cit., p. 33.
[83] MCQUAIL, Denis. Op. cit., pp. 448 y ss.

En definitiva, más allá de los cambios de paradigma que se han observado, los nuevos medios de comunicación llegaron para quedarse y lo lógico es que sigan apareciendo nuevas tecnologías que perfeccionen los descubrimientos precedentes, por lo que debemos aprender a vivir con ellos y adaptarnos a sus nuevos usos, procurando que el Derecho les siga el paso un poco más de cerca.

CAPÍTULO II

USO DE INTERNET PARA CAUSAR GRAN IMPACTO EN LA POBLACIÓN

1. Generalidades.

La masificación del uso de Internet a nivel mundial ha sido un fenómeno inmensamente acelerado. Gracias al creciente acceso de las personas a la adquisición de computadores y a la contratación de planes de navegación que se adaptan a todas las necesidades y bolsillos, no es sorprendente que en la mayoría de los países industrializados exista al menos un equipo conectado a Internet por cada grupo familiar.

Adicionalmente, los organismos estatales, a veces con la ayuda de iniciativas privadas, han procurado satisfacer la necesidad de conexión a Internet de los sectores económicamente más vulnerables, con el objeto de no dejar relegados a estos grupos del desarrollo de la sociedad en la era de la información.

Lo anterior ha permitido formar una comunidad de usuarios de Internet bastante heterogénea, compuesta por personas de todas las edades, clases sociales y nacionalidades. Esta comunidad de cibernautas recurre a la red con fines académicos, de información, de difusión, de comunicación, de entretención, etc. Esto es posible gracias

a la gran capacidad de Internet para reinventarse a sí mismo, ofreciendo nuevas aplicaciones y siendo fuente de permanente innovación.

Entendiendo que los medios de comunicación de masas pueden generar, y de hecho han generado, gran impacto en la población, a continuación analizaremos la forma en que Internet en particular ha sido usado como un medio para lograr este objetivo.

Este ejercicio supone ahondar en el desarrollo histórico de este medio para identificar las características que lo diferencian de otros medios de comunicación masiva y las razones en que se basan los principios que rigen su uso alrededor del mundo, además de analizar algunos casos en que el uso de Internet ha desempeñado un rol fundamental en un acto que genere gran impacto en la población.

2. Breve historia de Internet.

2.1. Antecedentes.

Los comienzos de Internet están ligados a la investigación militar en Estados Unidos, durante la Guerra Fría, sobre la forma de interconectar un grupo de computadores de la

manera más efectiva posible permitiendo a los órganos de inteligencia militar no perder la comunicación frente a un posible ataque nuclear. [84]

En octubre de 1957 se lanzó al espacio el *Sputnik*, el primer satélite soviético. Hecho que marcó un hito en la competencia entre Estados Unidos y la Unión Soviética por demostrar su poder científico y militar frente al mundo. Esto incentivó a que en 1958, el Departamento de Defensa de Estados Unidos fundara ARPA (*Advanced Research Projects Agency*) con el objeto de potenciar la investigación científica en ese país.[85]

Sucesivamente, debido esta iniciativa y a la investigación desarrollada en diferentes universidades estadounidenses, se fueron creando redes que interconectaban pequeños grupos de ordenadores a través de protocolos y tecnologías compartidas entre ellos, pero diferentes entre sí, que permitían comunicarse de manera alternativa a los métodos tradicionales de la época, tales como la telefonía y la radiofonía.

En 1969 se creó ARPANET, un modelo primitivo de Internet, que conectaba un grupo de computadores en la Universidad de California (UCLA).

Progresivamente, diferentes universidades norteamericanas se fueron sumando a la iniciativa, pero notaron que la conversión de los diferentes protocolos para adaptarse al

[84] CANEDO ANDALIA, Rubén. *Aproximaciones para una historia de Internet*. *ACIMED*. 2004, vol.12, n.1 [en línea] http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000100005&lng=es&nrm=iso [consultado: 18.02.2013].
[85] GARCÍA, Pablo. *Principios de Derecho de Internet*. Tirant Lo Blanch, Segunda Edición, Valencia, 2005, p. 30.

protocolo usado por cada una de las universidades hacía muy costosa la interconexión de sus bases de datos.

Lo anterior, fomentó la búsqueda de una red más amplia y abierta a la que todos pudieran conectarse, independientemente de la tecnología utilizada. Con esto surge Internet (*Interconnected Networks*), la red de redes, que en base a la utilización de un protocolo de transmisión de datos conjunto TCP/IP (*Transmission Control Protocol/ Internet Protocol*) posibilitó "la interoperabilidad entre sistemas heterogéneos, la comunicación entre terminales mediante una multitud de redes diversas y el manejo automático de los fallos en la transmisión de datos"[86].

Junto con lo anterior, la dirección IP es lo que identifica al servidor o al usuario de Internet y va dejando "huellas" de su uso de la red, asociando el ingreso de su computador a ciertas páginas Web. Esto permite rastrear la fuente de contenidos ilícitos o nocivos que se reproduzcan en Internet.

2.2. Masificación del uso de Internet

En 1983 ARPANET se desvinculó de la red militar que le dio origen, dejando abierto el paso a todas las universidades, empresas y demás instituciones para el uso de la red, con el nuevo protocolo de Internet. Desde este momento Internet se transformó en una

[86] CANEDO ANDALIA, Rubén. Op. Cit.

red de libre acceso para todos aquellos usuarios que tuvieran un computador conectado a un servidor y fueron creándose nuevas aplicaciones, como por ejemplo el *chat*, que dotó a la transmisión de datos de mayor interactividad.

El momento en que el uso de Internet se volvió masivo fue cuando surgió, durante los años noventa, el *World Wide Web* como *browser* que permitió acceder a esta nueva plataforma multimedia fácilmente desde cualquier computador que estuviera conectado a la red. Este nuevo formato se creó con el objeto de combatir la saturación de la cual estaba siendo víctima Internet desde su apertura global. Junto con lo anterior, Tim Berners-Lee, su inventor, creó las bases del protocolo de transmisión HTTP[87], el lenguaje de documentos HTML[88] y el concepto de los URL.

Esta innovación, junto con la caída de los precios de los computadores, permitió que, a partir de 1994, la mayoría de la población pudiera tener acceso a Internet. Inicialmente se hacía necesaria una conexión telefónica desde los hogares u oficinas[89], pero hoy en día es posible conectarse desde cualquier lugar del mundo, de manera inalámbrica, gracias a la incorporación del *Wifi* y del Internet móvil, de la mano del WAP (*Wireless Application Protocol*).

[87] *Hyper Text Transfer Protocol* (Protocolo de Transferencia de HiperTexto), mecanismo de intercambio de información que constituye la base funcional de la *World Wide Web*.
[88] *Hyper Text Markup Language* (Lenguaje de Marcado de HiperTextos), lenguaje que es la base estructural en la que están diseñadas las páginas de la *World Wide Web*.
[89] Lo que marca el nacimiento del Internet comercial.

2.3. Aplicaciones de Internet más usadas.

Una vez que Internet fue inventado, los especialistas en la materia procuraron crear e implementar diferentes aplicaciones de la red para que su uso se mantuviera vigente. Inicialmente, existía el correo electrónico, la transferencia de archivos y el acceso remoto, pero estas aplicaciones, a pesar de la revolución en las comunicaciones que supuso la creación de los *e-mails*, no terminaban de transformarse en una competencia real frente a los medios de comunicación tradicionales. De hecho, el fenómeno de Internet se mantuvo por mucho tiempo circunscrito a los círculos de científicos y académicos.

El momento en el que Internet se volvió masivo fue cuando se crearon nuevas aplicaciones, que complementadas y superpuestas a las antiguas formaron un conjunto de diversas alternativas disponibles en la red para ser de utilidad a las personas en diferentes situaciones.

2.3.1. World Wide Web

Esta aplicación permite a los usuarios ver documentos que contienen gráficas y textos, además de seguir un *link* desde un documento a otro.[90] La mayor parte del uso

[90] COMER, Douglas. *Internetworking with TCP/IP. Principles, protocols and architectures.* Cuarta Edición, Prentice Hall, New Jersey, 2000, p. 4.

que se le da a Internet hoy en día se basa en esta aplicación[91], lo que se relaciona con la facilidad con que se puede acceder a los sitios web y con la gran variedad de información disponible en la red.

Cada sitio de la *Web* adquiere un nombre identificable por los usuarios en base al Sistema de Nombres de Dominio (*Domain Name System*) que distingue un sitio de Internet de otro a través de un conjunto de letras y/o números determinado, como por ejemplo "www.uchile.cl", que en este caso identifica a su vez el lugar geográfico en que se realizó la inscripción del nombre de dominio (.cl= Chile). [92]

Algunos de los sitios más visitados en el mundo hoy en día son Google, Facebook, Youtube y Twitter[93], los que reflejan el comportamiento de la sociedad contemporánea respecto a los medios de comunicación y la forma en que éstos interactúan entre sí en el marco de la globalización.

a) Google:

Los buscadores de Internet fueron creados para solucionar el problema de falta de sistematización de la información contenida en la Web.

[91] Se estima que el "WWW" utiliza el 80% del tráfico en Internet.
[92] Para mayor información: www.nic.cl o www.icann.org
[93] Estos sitios a su vez representan nuevas aplicaciones de Internet.

Si bien es cierto que Internet puso a disposición de los usuarios un sin número de contenidos, en un comienzo la tarea de encontrar el documento que se estaba buscando en la red era agotadora y quitaba demasiado tiempo. Esto se producía porque, a diferencia de una biblioteca en el "mundo real", Internet no poseía un catálogo de todos los contenidos disponibles en el "mundo virtual" que permitiera a los usuarios hacer más eficiente su búsqueda.

Frente a este problema que amenazaba con frenar el crecimiento de la red de redes se inventaron los buscadores de Internet. AltaVista, creado en 1995, fue uno de los motores de búsqueda más utilizados de la época, pero a partir de su creación en 1998, Google se ha transformado en el líder de la industria, innovando permanentemente en su oferta de productos y servicios.

Google representa, en la actualidad, una herramienta de gran utilidad para tener una referencia sobre la información que se está buscando en Internet. Hoy en día casi no tiene competidores y es blanco habitual de críticas por sus prácticas en contra de la libre competencia. [94]

[94] ALANDETE, David. Coto al poder de Google. El País. 25.06.2009. [en línea] <http://elpais.com/diario/2009/06/25/sociedad/1245880801_850215.html> [consultado: 31.03.2013].

b) Facebook:

Esta es una aplicación que fue creada en 2004 por Mark Zuckerberg, un estudiante de Harvard. El sitio pretendía transformarse en una red social donde un grupo determinado y acotado de personas pudieran compartir videos y fotos, comunicarse por chat, enviar y recibir archivos, etc.

A la fecha Facebook cuenta con más de mil millones de usuarios alrededor del mundo[95] y muchos lo califican como un fenómeno social que ha revolucionado la forma de relación entre las personas, ya que permite establecer, mantener o recuperar relaciones con personas que se transforman en un "capital social" siempre disponible para cada usuario.[96]

c) Youtube:

Esta aplicación fue creada en el año 2005 y fue adquirida por Google un año más tarde. En términos simples Youtube presta un servicio de almacenamiento que permite subir y compartir videos en la web.

---

[95] El número de usuarios calculado al 02.02.20013 es de 1.06 billones de usuarios. Fuente: <http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/> [consultado: 10.03.2013].

[96] ELLISON, Nicole, STEINFIELD, Charles y LAMPE, Cliff. *The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites.* Journal of Computer-Mediated Communication, Volumen 12, Tema 4, Julio 2007, pp. 1143-1168. [en línea] <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00367.x/full> [consultado: 10.03.2013].

Gracias a esta plataforma millones de personas alrededor del mundo se han convertido en editores y productores de sus propios contenidos, exhibiendo videos de música, denunciando el actuar de las autoridades u opinando sobre temas de interés, entre otras.

De esta forma, Youtube se ha transformado en un medio alternativo a la televisión, que permite que cualquier persona pueda ofrecer al público contenidos que antes se encontraban exclusivamente vinculados a aquella. Esto diversifica la oferta de contenidos y disminuye el poder de los conglomerados de medios masivos de comunicación a nivel mundial.

Tal es la popularidad que ha alcanzado este sitio, que desde hace un par de años, varias compañías dedicadas a la publicidad han fijado su interés en él para promocionar sus productos y ofrecer sus servicios. Además, la confiabilidad que ha alcanzado este sitio se demuestra en que incluso se ha llegado a medir el éxito de una banda o un cantante en base a las visitas que reciben sus videos en Youtube[97], ya que se piensa que existe relación entre lo que los cibernautas ven en Internet y lo que compran o consumen en el "mundo real".

[97] Como ejemplo de este fenómeno puede considerarse el caso del coreano PSY con su canción GANGNAM STYLE, que ha causado furor en la web, con cerca de un 1500 millones de visitas. [en línea] <http://www.youtube.com/watch?v=9bZkp7q19f0> [consultado: 21.03.2013].

d) Twitter:

Esta aplicación, creada en marzo de 2006, permite a los usuarios registrados enviar y leer mensajes de texto acotados a 140 caracteres (*tweets*). A diferencia de los mensajes de texto tradicionales (SMS en los celulares), este servicio proporciona una plataforma gratuita para los que prefieren este tipo de comunicación.

Twitter es una de las redes sociales que gozan de gran popularidad y el año 2012 registró más de 200 millones de usuarios con más de 340 millones de *tweets* publicados diariamente.[98] Hoy en día este servicio es utilizado principalmente a través de dispositivos móviles (Smartphone, BlackBerry, IPhone, etc.) y está reemplazado progresivamente a los servicios de mensajería tradicionales de los celulares y las compañías telefónicas.[99]

[98] Twitter. *Twitter turn six*. 21.03.2012. [en línea] <https://blog.twitter.com/2012/twitter-turns-six> [consultado: 23.09.2013].

[99] The guardian. *Twitter heads for stock market debut by filing for IPO*. 13.09.2013. [en línea] < http://www.theguardian.com/technology/2013/sep/12/twitter-ipo-stock-market-launch?CMP=EMCNEWEML6619I2&et_cid=48826&et_rid=7107573&Linkid=http%3a%2f%2fwww.theguardian.com%2ftechnology%2f2013%2fsep%2f12%2ftwitter-ipo-stock-market-launch> [consultado: 23.09.2013].

2.3.2. Correo electrónico (*e-mail*)

El correo electrónico, creado en 1972 por Ray Tomlinson[100], permite a sus usuarios enviar un mensaje a uno o a un grupo de individuos, además de ofrecer la posibilidad de adjuntar archivos, en todo tipo de formato, en cada mensaje.

Esta aplicación fue y sigue siendo una de las más exitosas de Internet, lo que se demuestra en el hecho de que el uso de *e-mails* ha ido reemplazando velozmente a las formas tradicionales de correspondencia.

Algunos autores[101] justifican lo anterior en base a que el correo electrónico ha sido diseñado de tal manera que hace confiable el envío y la recepción instantánea de comunicaciones por parte de los usuarios. A ello se suma a la seguridad que aporta el hecho de que para establecer una comunicación por este medio se requiera crear una cuenta para obtener una clave de acceso al sitio de Internet que ofrece ese servicio.

El uso masivo del correo electrónico en la actualidad da cuenta de la tendencia de la población a preferir mecanismos de comunicación más rápida por medio de las nuevas tecnologías.

[100] GARCÍA, Pablo. Op.cit., p. 36.
[101] COMER, Douglas. Op. cit., p. 4.

2.3.3. Transferencia de archivos

Esta aplicación permite enviar y recibir archivos de mayor tamaño que aquellos que se pueden adjuntar en un correo electrónico, otorgando las mayores garantías de que el archivo no será copiado o modificado al ser compartido.

La transferencia de archivos puede darse de dos formas: transferencia anónima y transferencia autentificada.

La transferencia anónima permite que cualquier persona pueda entrar y transferir información, con el único requisito de poseer una cuenta de correo electrónico. [102] Este sistema es utilizado para trasferir documentos que quieren hacerse públicos en la red, como es el caso de *software* de libre distribución o actualizaciones de programas.

El mecanismo de seguridad que se utiliza en la trasferencia autentificada, al igual que el *e-mail*, es el otorgamiento de usuarios y contraseñas para acceder a la plataforma que permite la transferencia y el hecho de que al ser transferido un archivo desde un computador a otro no se interrumpa la trayectoria de la comunicación por terceros. [103]

El uso de esta aplicación refleja el aumento que ha tenido el cambio del soporte papel al soporte digital en las diferentes áreas de la vida cotidiana. Desde un tiempo a

[102] GARCÍA, Pablo. Op. cit., p. 58.
[103] COMER, Douglas. Op. cit., p. 4.

esta parte los usuarios de la red han demostrado una marcada preferencia por mantener sus archivos o documentos en una versión digital debido a las ventajas prácticas que esto supone en la sociedad de la información, donde se privilegia la velocidad en el acceso a la información y a su vez la posibilidad de difundirla fácilmente.

2.3.4. Acceso remoto o terminal virtual

Esta aplicación permite al usuario de un computador situado en un lugar determinado acceder al escritorio de un computador situado en un lugar diferente, estableciendo una sesión interactiva en el equipo terminal. [104]

El acceso remoto ha sido muy utilizado por las empresas para mejorar la operatividad del trabajo realizado por sus empleados, ya que esto les permite acceder a su escritorio virtual de la oficina desde sus hogares o desde cualquier otro lugar donde exista una conexión a Internet.

Además, esta aplicación es segura para los dueños del equipo terminal, toda vez que requiere de una autenticación del usuario remoto a través de una clave y una cuenta de acceso (*login*) que es proveída por el dueño del equipo terminal.

[104] COMER, Douglas. Op. cit., p. 4.

La creciente popularidad en el uso del terminal virtual por las empresas y otros tipos de organizaciones da cuenta de la tendencia actual a usar las herramientas que ofrece Internet para hacer más eficiente el trabajo de oficina y para aminorar los costos de tener a las personas trabajando físicamente en un lugar determinado. Además, ello permite al trabajador administrar de mejor forma su tiempo y disminuir las horas que pasa en una oficina, aumentando la productividad.

3. Internet como medio de comunicación de masas

En términos simples, Internet puede definirse como "una red que une ordenadores de todo el mundo que permite el acceso a cualquiera de ellos, con la posibilidad de obtener e intercambiar información de manera muy sencilla". [105]

Algunos autores discrepan a la hora de calificar Internet como un medio de comunicación de masas, ya que las nuevas tecnologías de la información no cumplen con las características tradicionales de los *mass media*, a saber, que la información y los productos de entretenimiento sean generados de manera centralizada[106].

[105] GARCÍA, Pablo. Op. cit., p. 29.
[106] DIZARD, Wilson. Op. cit., p. 2. '*Mass media historically has meant centrally produced standardized information and Entertainment products, distributed to large audiences through separate channels'*.

Una de las principales características de la red es que permite que cada uno de sus usuarios pueda ser editor y creador de sus propios contenidos, por lo que sería un medio descentralizado por definición.

Sin embargo, la mayoría de los autores[107] discrepan de lo anterior, pues definen a los *mass media* en base al receptor del mensaje, y dado que los contenidos que se difunden en la *Web* pueden ser recibidos por una gran cantidad de personas al mismo tiempo, esta circunstancia convertiría a Internet en el medio de comunicación masiva por excelencia.

Si a lo anterior le sumamos el fenómeno de la convergencia de los medios de comunicación, que en la actualidad nos permite, por ejemplo, ver videos de Internet a través de nuestro celular o descargar una película o un libro en nuestro computador portátil u otro dispositivo, no hay duda de que Internet ha revolucionado nuestra aproximación a los *mass media* en general, a la vez que ha propiciado que tengamos la necesidad de estar conectados a la red permanentemente.

El futuro de las comunicaciones está intrínsecamente ligado a la innovación tecnológica[108] e Internet, con su constante adaptación y creación de nuevas aplicaciones, es el medio de comunicación de masas que pareciera indicarnos de manera más clara el

[107] Ver Capítulo I.
[108] STREET, John. Op. cit., p. 165.

camino que seguirán las comunicaciones en los años venideros en el contexto de la globalización[109].

4. Características de Internet

4.1. Red pública y abierta

Internet es una red pública y abierta que tiene escasas barreras de ingreso.[110]

A diferencia de otros medios de comunicación, en que se requieren permisos para operar dentro de la industria como emisor de contenidos (v.gr. radio y televisión), en este caso sólo se requiere de un computador conectado a la red. En este sentido, el uso de Internet como medio de comunicación es barato y menos exclusivo que el resto de los *mass media*.

En nuestro país el uso de Internet se rige por la Ley General de Telecomunicaciones (Ley N° 18.168), que entiende por telecomunicación "toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos e informaciones de cualquier

[109] STREET, John. Op. cit., p. 170. (165, Tomlinson, 1999) '*Globalization refers to the rapidly developing process of complex interconnections between societies, cultures, institutions and individuals world-wide. It is a social process which involves a compression of time and space, shrinking distances through a dramatic reduction in the time taken – either physically or representationally – to cross them, so making the world seem smaller and in a certain sense bringing human beings "closer" to one another*'.
[110] OVALLE, José Ignacio. Op. cit., p. 13.

naturaleza, por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos" [111].

En esta ley se establece que Internet es un servicio complementario de los servicios públicos de telecomunicaciones, ya que existe un interés público comprometido en garantizar el acceso por parte de la mayoría de la población a este servicio[112], cuestión que se demuestra en la permanente revisión de las políticas públicas focalizadas en aumentar los niveles de cobertura y acceso de la población a Internet. [113]

Además de lo anterior, Internet es una red abierta. Esto se refleja en nuestro país en la legislación, pues cualquiera puede ser prestador de servicios de Internet, mientras cumpla con los requisitos técnicos y normativos de la prestación del servicio. Por otro lado, todas las personas pueden acceder a la red como usuarios del servicio, sin más limitaciones que las técnicas.

En consecuencia, Internet es una red pública y abierta en un doble sentido, tanto desde el punto de vista del prestador del servicio de Internet, como desde el punto de vista del usuario o cliente del mismo.

---

[111] Artículo 1º, Ley General de Telecomunicaciones.
[112] El artículo 3º, letra b) de la LGT señala que los servicios públicos de telecomunicaciones son aquellos "destinados a satisfacer las necesidades de telecomunicaciones de la comunidad en general".
[113] Según el último estudio de la Subtel, la penetración de Internet en Chile alcanzó en el 2012 un 41% por cada 100 habitantes. Fuente: <http://www.subtel.gob.cl/index.php?option=com_content&view=article&id=3186%3Asubtel-acceso-a-internet-por-cada-100-habitantes-llega-a-41-y-banda-ancha-movil-se-acerca-a-los-5-millones-de-conexiones&catid=95%3Aservicios-telecomunicaciones&lang=es> [consultado: 19.03.2013].

4.2. Red ininterrumpida y grande

Internet está conformado por un conjunto de servidores y redes de computadores, interconectados a nivel mundial a través de proveedores de acceso, que operan bajo un protocolo común[114]. En este sentido, esta red se extiende como una telaraña invisible alrededor de todo el planeta permitiendo la conexión de un punto a otro con gran facilidad.

Además de lo anterior, la red es grande debido a que "la digitalización de la información y la capacidad de transmitirla por la red telefónica, hacen que Internet tenga una capacidad ilimitada de almacenamiento de información" [115].

4.3. Red descentralizada y no gobernada

Internet no tiene dueño ni nadie que lo represente. La red está conformada por un conjunto de servidores conectados entre sí, sin una estructura jerarquizada ni bajo un sistema de control o vigilancia superior.[116]

La única excepción a esta característica son organismos como el ICANN, en Estados Unidos, o NIC Chile, en nuestro país, que se encargan de gestionar la adjudicación y el

[114] OVALLE, José Ignacio. Op. cit., p. 13.
[115] MOYA GARCÍA, Rodrigo. *La Libertad de Expresión en la Red de Internet.* Separata para el curso de Derecho Informático, Primer Semestre, 2005, pp. 6 y 7.
[116] OVALLE, José Ignacio. Op. cit., p. 13.

uso de los nombres de dominio en cada uno de estos países. Sin embargo, estos organismos sólo representan una autoridad en esa materia en particular y en ningún caso pueden involucrarse en la regulación de otras áreas del uso de Internet.

En base a lo anterior, algunos autores plantean que Internet posee en realidad un gobierno autogestionado que se regula a sí mismo por los propios usuarios de la red. Esto se debe a que, en la práctica, la red no depende de la infraestructura, es decir, "Internet no está ligado a ninguna infraestructura, aparte del sistema telefónico, fijo o móviles, antenas y satélites, por tanto lejos de un control gubernamental efectivo"[117].

4.4. Red anónima y controlada por el usuario

Internet permite enviar información y acceder a ella sin identificación del respectivo usuario[118], lo que facilita la expresión de ideas de todo tipo, a la vez que se ha prestado para evadir la persecución frente a la comisión de un delito.

El anonimato en la red se ha formulado como un derecho de los usuarios de Internet que dice relación con "el derecho que tiene el usuario de Internet para que su identidad permanezca oculta o en forma reservada ante la mirada de otros actores que se desenvuelven en la Red. El contenido del Derecho al Anonimato incluye la confidencialidad de las comunicaciones en Internet, la confidencialidad de los datos de

[117] MOYA, Rodrigo. Op. cit.
[118] OVALLE, José Ignacio. Op. cit., p. 13.

tráfico y de todos aquellos datos e informaciones que permitirán desenvolverse con la mayor libertad en la Red"[119].

Como un intento de limitar los posibles abusos que se pueden generar a partir del anonimato, se han incorporado en Internet mecanismos de autenticación en algunos sitios web para controlar su uso ilícito, limitando en algún grado el acceso en beneficio de la seguridad del uso de los sitios.

Sin perjuicio de lo anterior, Internet es básicamente controlada por el usuario, ya que éste "es libre para escoger los contenidos a los que quiere tener acceso y aquellos que quiere incorporar a la Red"[120]. Esto supone la existencia de un espacio de libertad envidiable teniendo en consideración la historia de los medios de comunicación y las discusiones que se han generado en torno a la libertad de expresión en la red.

4.5. Red interactiva

La web está diseñada para establecer comunicaciones bidireccionales.[121]

[119] CABEZAS Logan, P. y MOYA Muñoz, F. (2008).*El Derecho al anonimato del usuario de internet*. Disponible en: <http://tesis.uchile.cl/handle/2250/107854> [consultado: 19.03.2013].
[120] MOYA, Rodrigo. Op. cit.
[121] OVALLE, José Ignacio. Op. cit., p. 13.

Si comparamos Internet con cualquier otro medio, podemos llegar fácilmente a la conclusión de que la interactividad es una de las características que lo distingue de los demás medios donde prima la comunicación unidireccional (v.gr. radio y televisión).

Lo anterior se debe a que cada mensaje que se trasmite a través de la red en los diferentes formatos que las nuevas aplicaciones de Internet permiten en la actualidad (v. gr. un video en Youtube o un estado en Facebook), recibe una respuesta instantánea de algún otro usuario de Internet.

Esto permite mantener una serie de comunicaciones simultáneas entre los usuarios en tiempo real, haciendo uso de diversas plataformas multimedia, que a diferencia de la comunicación de los *mass media* tradicionales, permite una retroalimentación permanente a gran velocidad. [122]

4.6. Red global

Se ha dicho sobre Internet que, no obstante ser una sola red, se encuentran incorporados a ella todos los países y personas de nuestro planeta, sin otras limitaciones que las que imponga la tecnología. [123]

[122] En un minuto en Internet se realizan 2 millones de búsquedas en Google, 277 mil usuarios se conectan a sus cuentas de Facebook y 1,3 millones de usuarios ven videos en Youtube. Fuente: <http://www.24horas.cl/tendencias/mundodigital/las-increibles-cifras-de-lo-que-sucede-en-internet-en-un-minuto-568982> [consultado: 21.03.2013].
[123] OVALLE, José Ignacio. Op. cit., p. 13.

Esto se debe principalmente a las características examinadas anteriormente, en especial a la inexistencia de mayores barreras o controles en el acceso. Ello se suma al hecho de que se trata de una red ininterrumpida cuyos mensajes se transmiten por todo el mundo, a diferencia de la televisión o la radio, cuyas señales sólo alcanzan un área de emisión limitada que requiere de tecnología adicional para lograr un alcance global (como es el caso de la televisión satelital o las señales de radio online en Internet).

5. Casos en que Internet ha sido usado para causar gran impacto en la población

5.1. Virales en la Web

A nivel social, el fenómeno de los virales en Internet no deja de sorprender.

Debido a la convergencia de los medios y los avances tecnológicos, la mayoría de la información que antes se comunicaba exclusivamente por los medios de comunicación de masas tradicionales hoy, además, se difunde en la Web.

En este sentido, la publicidad, por ejemplo, se ha trasladado en un porcentaje de creciente importancia a Internet, ya que la difusión de información es más rápida y llega a un público masivo.

Los virales en Internet se caracterizan por la rápida multiplicación del número de quienes reciben y, a la vez, retrasmiten un determinado contenido en la red a través del envío de correos electrónicos, mensajería instantánea o páginas web, entre otros medios. Generalmente, se trata de videos o imágenes con contenido humorístico[124] o bien de un mensaje relativo a un hecho que provoca un alto impacto en la población.

La difusión masiva de estos videos o imágenes en la red provoca un efecto inmediato en las acciones de gran número de usuarios de Internet. En un corto periodo de tiempo lo más buscado en Google o los *trending topics* (temas del momento) de las redes sociales, como Twitter o Facebook, se enfocan en la imagen o el video viral, como una gran reacción en cadena multidireccional.

5.2. *Wikileaks*[125]

Wikileaks es una organización sin fines de lucro formada en el año 2007, cuyo principal objetivo es poner en conocimiento público información y noticias importantes para la comunidad. [126] Para lograr su objetivo, *Wikileaks* ha desarrollado un moderno sistema que se vale de las diferentes aplicaciones de Internet para proteger la identidad de sus informantes anónimos, quienes filtran todo tipo de documentos confidenciales, tanto del gobierno, como de conocidas empresas multinacionales.

[124]El video de Harlem Shake es un ejemplo de virales a nivel mundial. Millones de personas graban y comparten sus videos en la red, representando su propia versión del video original. Ver: <http://www.youtube.com/watch?v=4hpEnLtqUDg> [consultado: 27.03.2013].
[125] Retomaremos el análisis de este caso en el Capítulo IV del presente trabajo.
[126] Para mayor información: <http://wikileaks.org/About.html> [consultado: 31.03.2013].

Los archivos filtrados a través de *Wikileaks* contienen información sobre gastos militares millonarios de Estados Unidos, revelaciones impactantes sobre las cifras de soldados fallecidos durante la guerra en Afganistán, comunicaciones secretas entre las embajadas de Estados Unidos alrededor del mundo que muestran la inconsistencia entre su discurso público en materia de relaciones exteriores y sus verdaderas prácticas (p.ej. información sobre las reales condiciones en que se mantiene a los prisioneros en Guantánamo, entre otras).

Sin perjuicio de que la mayor parte de las filtraciones de *Wikileaks* corresponden a información clasificada del gobierno de Estados Unidos, existen también archivos sobre países de Europa, como Inglaterra o Alemania, y de Latinoamérica, como Colombia.

Durante el año 2012 el gobierno de Estados Unidos inició una investigación para descubrir la fuente que filtró documentos secretos que revelaban información confidencial durante el año 2010. Bradley Manning, un analista de sistemas del ejército norteamericano, resultó ser el principal sospechoso de filtrar más de 250.000 cables entre las embajadas de Estados Unidos alrededor el mundo y una serie de archivos confidenciales. [127]

Durante ese mismo año, Julian Assange, el fundador de *Wikileaks*, fue acusado por delitos sexuales cometidos en Suecia y logró conseguir asilo en la embajada de Ecuador

[127] BBC News. *Bradley Manning supporters stage UK events.* 23.02.2013. [en línea] <http://www.bbc.co.uk/news/uk-21556107 > [consultado: 31.03.2013].

en Londres antes de que lo extraditaran a ese país. Assange aún permanece viviendo en la embajada de Ecuador en Londres e insiste en que estas acusaciones no son fundadas y en que obedecen a una persecución política en su contra por las repercusiones que han tenido las reveladoras informaciones filtradas en *Wikileaks* durante los últimos años. [128]

5.3. Virus informáticos

El anglicismo *hacking* "alude al simple acceso sin autorización a sistemas informáticos ajenos utilizando las redes públicas de telefonía o transmisión de datos" [129]. Los sujetos que recurren a esta técnica son llamados *hackers* y su conducta calza con la descripción que en el mundo hispano se le ha dado al intrusismo informático.

Una de las herramientas de las que se valen los hackers para perpetrar sus intrusiones sin autorización en los sistemas computacionales de millones de personas son los virus informáticos.

Los virus informáticos son "los más temidos y frecuentes procedimientos informáticos de destrucción de elementos lógicos" [130], cuya función es replicarse de un sistema informático a otro y situarse en los computadores de forma que puedan "destruir

[128] BBC News. *Julian Assange: Wikileaks to release 'million more files in 2013'*. 20.12.2012. [en línea] <http://www.bbc.co.uk/news/uk-20806355> [consultado: 31.03.2013].
[129] GONZÁLEZ RUS, Juan José. *"Los ilícitos en la red (I): hackers, crackers cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes"*. En ROMEO CASABONA, Carlos María y Otros. *El Cibercrimen: Nuevos retos jurídico-penales. Nuevos desafíos político-criminales.* Editorial Comares, Granada, 2006., p. 243.
[130] Ibíd., p. 265.

o modificar programas y ficheros de datos, presentar un determinado mensaje, provocar fallos en el sistema operativo o interferir los procesos normales del sistema operativo"[131]. Los virus más comunes son los "troyanos" y los "gusanos".

Los virus troyanos se presentan enmascarados dentro de un programa aparentemente útil o con una apariencia inocua, con el fin eludir los mecanismos de seguridad de que disponga el computador[132].

Los gusanos, en cambio, se transmiten generalmente a través del correo electrónico y se auto-ejecutan sin necesidad de que el receptor realice acción alguna para ello[133].

En la práctica se tiende a utilizar una combinación de ambos elementos para intervenir el funcionamiento normal de un computador en particular o de numerosos computadores en general.

Uno de los gusanos que han causado mayor impacto alrededor del mundo es el "*ILOVEYOU Worm*" o "*Love Bug Worm*" que infectó a millones de computadores en el año 2000. Este gusano se envió masivamente a los *e-mails* de contacto de su creador[134] y estaba diseñado para reenviarse a su vez a cada contacto de los receptores del correo

[131]Ibídem.
[132]Ibídem.
[133]Ibíd., p. 266.
[134] Onel de Guzmán, un estudiante de informática filipino que desarrolló el virus como parte de su proyecto de tesis de pregrado. Fuente: WARD, Mark. *A decade on from the ILOVEYOU bug*. BBC News. 2010 <http://www.bbc.co.uk/news/10095957> [consultado: 27.03.2013].

electrónico inicial, de manera que se expandió exponencialmente colapsando los servidores de *e-mail* en todo el mundo y forzando a grandes compañías a cerrar sus correos por un día. Se calcula que las pérdidas fueron de miles de millones de dólares.[135]

Otro caso que impactó a la opinión pública fue el del virus "*Stuxnet*" [136] que en el año 2010 fue utilizado para atacar una central nuclear en Irán mediante la manipulación del sistema operativo que controlaba las turbinas que mantenían funcionando el generador de energía. [137] Este caso es el primer intento conocido del diseño y uso de un virus informático para dañar infraestructura del "mundo real". [138]

El problema que se genera con los virus informáticos, es que existen anti-virus y *firewalls* para combatir la intrusión de éstos en nuestros computadores, pero cada vez que se crea un nuevo gusano o troyano, el anti-virus queda obsoleto y los usuarios son vulnerables hasta que se incorpore la nueva forma del virus a la base de datos del mecanismo de seguridad implementado en ese computador. [139]

---

[135] MARSHALL, John. *Method and system for file blocking in an electronic messaging system.* 2000. [en línea] <http://www.google.com/patents?hl=es&lr=&vid=USPAT7017187&id=lzN4AAAAEBAJ&oi=fnd&dq=i+love+you+worm&printsec=abstract#v=onepage&q=i%20love%20you%20worm&f=false> [consultado: 27.03.2013].

[136] Retomaremos el análisis de este caso en el Capítulo IV del presente trabajo.

[137] Para mayor información ver: <http://www.slashgear.com/stuxnet-virus-existed-2-years-prior-to-attacks-26271641/> [consultado: 27.03.2013].

[138] COX, Simon. *Anonymous, hacktivism and the rise of cyber protesters*. BBC News. 26.11.2012. [en línea] <http://www.bbc.co.uk/news/technology-20446048> [consultado: 31.03.2013].

[139] MARSHALL, John. Op. cit.

Lo anterior, es fuente de gran temor en la población frente a la incertidumbre que genera el descubrimiento de nuevas formas de virus informáticos y el hecho de que su rápida propagación puede generar daños incalculables.

5.4. *Anonymous*

Anonymous es una organización de activistas de Internet, que a través de la utilización del *hacking* han creado una nueva forma de protestar en la red. Sus miembros se mantienen en el anonimato y ha sido muy difícil condenarlos por algunos delitos informáticos que se les atribuyen, especialmente a los ataques de sitios web del gobierno de Estados Unidos.

En base a los ataques que se han atribuido a este grupo, se dice que *Anonymous* defiende la libertad en Internet y se opone a cualquier forma de censura en la red. Además, se opone a la cientología, a la corrupción en el gobierno, a la pedofilia y a la homofobia. [140]

Uno de los ataques de *Anonymous* que causó mayor impacto en la población ocurrió en enero del año 2012. El Departamento de Justicia de Estados Unidos y el FBI habían cerrado el sitio Megaupload, destinado a compartir archivos de música, películas, series, libros, etc. gratuitamente en Internet.

[140] FILDES, Johnathan. *Stuxnet virus target and spread revealed*. BBC News. 2011. [en línea] <http://www.bbc.co.uk/news/technology-12465688 > [consultado: 27.03.2013].

Como una forma de protestar frente a este acto que afectaba a los usuarios que compartían archivos de manera libre y gratuita en la red, *Anonymous* atacó los sitios de Internet de esos organismos y de las empresas involucradas en las demandas por piratería e infracciones a la ley de *copyright* que contribuyeron con el cierre del sitio.

Desde sus primeros ataques en 2008, *Anonymous* se ha convertido en un grupo de activismo cibernético poderoso que se percibe por la opinión pública como un justiciero de los débiles en la web. Hoy en día, incluso se realizan manifestaciones de personas que respaldan el actuar de esta organización, pues ven representados en ella sus convicciones respecto de la vulneración de los derechos de la ciudadanía por parte de grupos más poderosos. El símbolo característico de esta organización y de sus partidarios es la máscara de Guy Fawkes usada en el cómic y la película "V de Vendetta", que otorga más poder a su mensaje.

5.5. Ciber-terrorismo[141]

El ciber-terrorismo se ha transformado en un tema de interés en el mundo. Sobre todo porque aún se desconoce el verdadero impacto que puede generar en las personas.

[141]Nos remitimos a lo expuesto en el Capítulo I sobre el uso de los medios de comunicación para causar gran impacto en la población.

Sin perjuicio de lo anterior, se han creado leyes para defenderse contra posibles ataques que se generen debido al mal uso de la web[142] y se ha hablado del concepto de ciber-seguridad tanto por organizaciones públicas como privadas.

El problema que surge a partir de los hechos que la prensa ha calificado como ciber-terrorismo, es que, más allá del impacto que provocan en la opinión pública una vez que se descubren, los estudios en la materia no han logrado desarrollar un concepto acabado o delimitar las características del mismo.

En conjunto con lo anterior, las autoridades de países como Estados Unidos, han reconocido la creciente masificación del uso de Internet como medio de ataque por organizaciones terroristas o sujetos independientes, poniendo énfasis en la necesidad de realizar una ataque pre-emptivo frente al nivel de devastación que pueden llegar a causar los ciber-ataques en el mundo físico[143].

Frente a esto, se hace necesario realizar un análisis más acabado de los conceptos utilizados respecto de este nuevo tipo de amenaza en el ciber-espacio, ya que calificar como ciber-terrorismo un hecho que en realidad corresponde a un delito informático ya tipificado puede tener consecuencias manifiestamente injustas desde el punto de vista normativo.

[142] En Estados Unidos el Presidente Obama impulsó un avance en esta materia con el decreto ley de ciber-seguridad. Ver: [en línea] <http://www.fayerwayer.com/2013/02/obama-firma-decreto-ley-de-ciberseguridad-para-enfrentar-los-ciberataques-a-estados-unidos/> [consultado: 31.03.2013].

[143] BBC News. *US prepares first-strike cyber-forces.* 12.10.2012 [en línea] <http://www.bbc.co.uk/news/technology-19922421 > [consultado: 31.03.2013].

CAPÍTULO III

¿QUÉ ES EL CIBER-TERRORISMO?

1. Generalidades.

Tal como se señala en los capítulos anteriores, los medios de comunicación de masas (MCM) y en especial Internet se han posicionado como herramientas muy poderosas para influir en la población. Si a esto se agrega el amplio desarrollo que han experimentado las tecnologías de la información y las comunicaciones (TIC's) en los últimos años y el fenómeno llamado convergencia, que permite tener acceso a diferentes aplicaciones utilizando sólo un dispositivo tecnológico, podemos entender las razones del auge del ciber-terrorismo en la sociedad contemporánea.

Pero, ¿qué se entiende por ciber-terrorismo?

Es relevante hacerse esta pregunta porque el tratamiento que se le dé a este fenómeno y las políticas que los gobiernos adopten para combatirlo dependerá de la forma en que se delimite el concepto, cuestión que a su vez sentará las bases de la manera de abordar las repercusiones jurídicas que los actos de ciber-terrorismo traen aparejados.

A su vez, la claridad conceptual sobre esta materia permite abordar sobre una base sólida los dilemas que se puedan plantear en el futuro, considerando que la realidad es intrínsecamente dinámica y exige una constante adaptación a sus cambios y exigencias.

En el presente capítulo se analizarán los conceptos de ciber-terrorismo propuestos por diversos autores, identificando sus características propias y distinguiéndolo de otros fenómenos con los que suele confundírselo.

2. Nociones básicas sobre el terrorismo.

Antes de tratar el concepto de ciber-terrorismo, es preciso determinar qué se entiende por terrorismo.

Existen 14 tratados internacionales[144] y diferentes tratados regionales[145] que tipifican conductas que se califican como terroristas para el derecho internacional. No obstante, "no se ha logrado un consenso respecto de la definición jurídica internacional del

[144] Algunos de estos tratados son: Convenio para la represión del apoderamiento ilícito de aeronaves (1970), Convención internacional contra la toma de rehenes (1979), Convención sobre la protección física de materiales nucleares (1980), Convenio Internacional para la represión de actos terroristas cometidos con bombas (1997), Convenio Internacional para la represión de la financiación del terrorismo (1999), Convenio Internacional para la represión de los actos de terrorismo nuclear (2005), entre otros. Fuente: <http://www.un.org/spanish/terrorism/instruments.shtml> [consultado: 20.08.2012].

[145] De diferentes organizaciones regionales en África, América, Asía, Europa y en el mundo árabe. Fuente: <https://www.unodc.org/tldb/es/regional_instruments.html> [consultado: 20.08.2012].

terrorismo"[146]. Ello se debe a que resulta más fácil lograr acuerdo en calificar determinadas conductas como terroristas que definir el terrorismo, dada la diversidad de posiciones entre los Estados sobre la legitimidad del uso de la fuerza.

A nivel doctrinario, sin embargo, los autores concurren en que el terrorismo supone ciertos elementos mínimos. Alex Bellamy[147] define el terrorismo como "un ataque deliberado a no combatientes con fines políticos", que "puede ser practicado tanto por actores estatales como no estatales".

Para este autor, lo realmente condenable del terrorismo consiste en "dar muerte de manera deliberada a aquellos a quienes está prohibido matar"[148], ya que esto constituiría una violación de los principios del *jus in bello* (en particular al principio de distinción que establece la inmunidad de los no combatientes), cuestión que es abiertamente condenada por el derecho internacional.

También se ha definido terrorismo como "actos de violencia extrema injustificada llevados a cabo con fines políticos por opositores a la autoridad establecida para ejercer una influencia directa sobre las autoridades o una influencia indirecta al crear un clima de temor y conmoción públicos, que a menudo alcanza a víctimas inocentes"[149]

---

[146] Comisión Interamericana de Derechos Humanos. Informe sobre terrorismo y Derechos Humanos. 2002. [en línea] < http://www.cidh.org/Terrorism/Span/resumen.htm> [consultado: 13.09.2012].
[147] BELLAMY, Alex. *Guerras Justas. De Cicerón a Irak*. Fondo de Cultura Económica, Buenos Aires, 2009, pp. 211 y ss.
[148] Ibíd., p. 215.
[149] MCQUAIL, Denis. Op. cit., p. 359.

Además, se sostiene que el acto terrorista busca aterrorizar a la población[150]. En este sentido, se ha señalado que "los actos de terrorismo no son sólo comportamientos con devastadores efectos violentos, sino que también son comportamientos cuya distinción de otros actos de violencia es que ellos están constituidos comunicativamente. Esto es, las acciones pretenden enviar un mensaje de miedo a una audiencia e indicar que si las políticas y los comportamientos en contra de los terroristas (o aquellos a quienes dicen representar) no cambian, más acciones terroristas como esa se cometerán"[151], lo que otorga una especial importancia a los medios de comunicación a la hora de transmitir estos mensajes a la población y la forma en que abordan este tipo de noticias.

En suma, a pesar de la inexistencia de un criterio único para definir un acto terrorista, los autores[152] identifican elementos característicos del terrorismo, como son: el uso o amenaza de uso de la fuerza, en contra de no combatientes o de manera indiscriminada, con motivación política, por parte de actores no estatales y con la intención de "sembrar el terror" en la sociedad (lo que se vincula con la publicidad del acto en la mayor medida posible) y conseguir una reacción por parte de las autoridades que se espera que favorezca los fines de quienes recurren a este tipo de violencia.

---

[150] LAQUEUR, Walter. *Una historia del terrorismo.* Editorial Paidós, Buenos Aires, 2003, p. 42.

[151] STOHL, Michael. *Old myths, new fantasies and the enduring realities of terrorism*. Critical Studies of Terrorism, Vol. 1, No. 1, April, 2008, p. 7. Traducción libre. *'Acts of terrorism are not only behaviours with devastating violent effects, but are also behaviours whose distinction from others acts of violence is that they are communicatively constituted. That is, the actions are intended to send an audience a message of fear and to indicate that if policy and behaviours towards the terrorist (or those they purport to represent) do not change, more such terrorist actions will follow.'*

[152] ZALAQUETT, José. *Chile ratifica la Convención Interamericana contra el Terrorismo*. En No. 2 (2006): Anuario de Derechos Humanos, 2006, p. 181. [en línea] <http://www.anuariocdh.uchile.cl/>

Adicionalmente, a partir de los ataques ocurridos el 11 de septiembre de 2001, se han identificado en la doctrina[153] como características del "nuevo terrorismo" el hecho de que se encuentre insertado dentro de los Estados, que se constituya a partir de redes internacionales con gran capacidad de devastación, la voluntad de auto-inmolación de muchos de sus participantes y el hecho de ser ubicuo y relativamente invisible.

Estas características convierten al terrorismo en una amenaza grave y permanente para la comunidad internacional en su conjunto, debido a la creciente interdependencia que existe entre los diferentes países y el hecho de que las fronteras nacionales ya no sean un obstáculo, principalmente como consecuencia del grado de desarrollo que ha alcanzado Internet y las redes computacionales en términos de acceso y cobertura en todo el mundo.

Lo anterior, además de dar cuenta del fenómeno conocido como globalización, revela la aptitud de Internet de convertirse en un nuevo vehículo o instrumento de ataque o un nuevo tipo de arma en la medida que potencia de manera estratégica los alcances de los métodos terroristas tradicionales, aumentando a su vez la inseguridad de los países frente a este fenómeno emergente.

[153] ZALAQUETT, José. Op. Cit., p. 180.

3. Evolución del terrorismo

En tiempos modernos, se pueden distinguir tres fases principales de la evolución del terrorismo.

3.1. Antes de 1970

Inicialmente el terrorismo se ve vinculado con el derecho de rebelión y con el tiranicidio, ya que se consideraba una respuesta válida de los ciudadanos frente a los abusos del poder del Estado.

Durante este periodo los ataques terroristas se caracterizaban por el uso de la fuerza de modo indiscriminado en contra de civiles, utilizando métodos de guerra tradicional (principalmente bombas).

Además, esta etapa se caracteriza por la inexistencia de convenios internacionales específicos en contra de los ataques terroristas, debido a que se pensaba que estas conductas ya eran objeto de reproche jurídico por la aplicación de los convenios internacionales sobre el derecho humanitario y los derechos humanos.

3.2. Entre 1970 y el ataque a las Torres Gemelas

Este periodo se caracteriza por la aparición de nuevas formas de ataque, como el secuestro de aeronaves o el uso de auto-bombas, facilitadas por los desarrollos de la vida moderna, ciertas ideologías, la vulnerabilidad de la vida urbana y mayores oportunidades de gran difusión comunicacional.

Como respuesta a esta tendencia, durante este periodo se dictaron numerosas convenciones internacionales, como lo son, el Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (1970), la Convención Internacional contra la Toma de Rehenes (1979), la Convención sobre la Protección Física de Materiales Nucleares (1980) y el Convenio Internacional para la Represión de Actos Terroristas Cometidos con Bombas (1997), entre otras.

3.3. Post 11/9/2001

Después del ataque terrorista contra las Torres Gemelas tendió a redefinir el concepto de seguridad y de amenazas a la seguridad de los Estados, junto con propugnarse la implementación temporal de restricciones adicionales a ciertos derechos humanos para facilitar la represión del terrorismo.

Durante este periodo entró en vigencia la Convención Interamericana contra el Terrorismo (2003), que buscaba promover la dictación de leyes antiterroristas en los Estados americanos para reprimir el terrorismo, por ejemplo, en materia de financiación del terrorismo.

4. Conceptos de ciber-terrorismo.

Dado que el fenómeno de Internet es relativamente reciente[154], su uso asociado al terrorismo tampoco tiene larga data, por lo que existen opiniones diversas sobre el uso del concepto de ciber-terrorismo, su alcance y aplicaciones prácticas.

4.1. Uso de Internet para facilitar o expandir los efectos del terrorismo tradicional

Dorothy Denning define ciber-terrorismo como: "la convergencia entre ciberespacio y terrorismo. Se refiere a los ataques ilegales y amenazas de ataques en contra de computadores, redes y la información almacenada en ellos cuando son realizados para intimidar o coaccionar un gobierno o su población en la persecución de objetivos políticos o sociales. También, para calificarlo como ciber-terrorismo, en opinión de esta autora, un ataque debe resultar en violencia en contra de personas o propiedad, o al menos causar un daño suficiente para generar miedo en la población, como por ejemplo, los ataques que llevan a la muerte o lesiones corporales, explosiones o una severa

[154] Los primeros avances en la configuración de lo que hoy conocemos como Internet con su sistema de World Wide Web (WWW) se produjeron durante la década de 1980.

pérdida económica. Adicionalmente, pueden ser actos de ciber-terrorismo graves ataques en contra de infraestructura fundamental de un Estado, dependiendo de su impacto. En cambio, no lo serían aquellos ataques que interrumpen servicios no-esenciales o que involucran mayormente una costosa molestia."[155]

En este sentido, se estaría describiendo el ciber-terrorismo en base a la definición tradicional de terrorismo, esto es, como una forma de facilitar o expandir los efectos de un ataque violento en contra de no-combatientes mediante el uso de Internet y las nuevas tecnologías.

En esta misma línea, se ha sostenido que "[e]l objetivo de un ataque ciber-terrorista no es sólo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general. […]. Un ataque ciber-terrorista, por tanto, debe analizarse en términos del objetivo que persigue y de su impacto, y no solamente por el modo de ataque."[156], lo que nos alerta sobre el potencial peligro que significaría la combinación

[155] DENNING, Dorothy E. Declaración hecha el 23 de Mayo de 2000 en una audiencia frente al Congreso de EE.UU. en el marco de la discusión de un panel de expertos sobre las Amenazas Terroristas para los Estados Unidos. [en línea] <http://www.fas.org/irp/congress/2000_hr/00-05-23denning.htm> [consultado: 28.08.2012] Traducción libre. *'Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.'*

[156] VERTON, Dan. *Black Ice: La amenaza invisible del ciberterrorismo*. Editorial Mc Graw- Hill/ Interamericana de España, Madrid, 2004, p. xxvii.

de armas físicas y cibernéticas en la comisión de un ataque terrorista, además de la importancia de la motivación del perpetrador en la calificación conceptual del acto.

4.2. Uso de Internet por parte de grupos terroristas para fines organizacionales

Por otra parte, existen autores que han desarrollado un concepto de ciber- terrorismo de manera aún más amplia definiéndolo simplemente como "el uso de tecnología y medios de información por grupos y agentes terroristas"[157], destacando como ejemplos de este tipo de acto el uso de la tecnología de la información para organizar y llevar a cabo ataques, apoyar actividades de los grupos y realizar campañas de promoción ideológica en Internet.

Usar una definición de este tipo conduciría a aumentar la cantidad de actos que pueden ser considerados como ciber-terroristas, ya que el uso de Internet por parte de grupos y agentes terroristas se ha generalizado para, por ejemplo, buscar financiamiento de sus actividades o para comunicarse entre las células de la organización.

[157] KRASAVIN, Serge. *What is Cyber-terrorism?*. Computer Crime Reseasrch Center (CCRC). [en línea] <http://www.crime-research.org/library/Cyber-terrorism.htm>. [consultado: 28.08.2012]. Traducción libre. *'Use of information technology and means by terrorist groups and agents'*.

4.3. Ataques contra sistemas esenciales que dependen de tecnología cibernética.

El enfoque hacia el ataque de infraestructuras fundamentales (o infraestructura crítica) de un país para calificar un acto como ciber-terrorismo ha sido adoptado por James Lewis, quien define este fenómeno como "el uso de herramientas de las redes computacionales para cerrar infraestructura nacional fundamental (como energía, transporte, operaciones gubernamentales) o coaccionar o intimidar a un gobierno o a la población civil"[158]. Este autor hace la prevención de que tal infraestructura se ha vuelto sólo aparentemente vulnerable como consecuencia de su mayor dependencia de las redes computacionales y que la amenaza del ciber-terrorismo no es tan real como se ha creído ver hasta la fecha.

A mayor abundamiento Dan Verton sostiene que "[e]n términos generales, el ciber-terrorismo es la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista extranjero sub-nacional, con objetivo político, utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos"[159].

---

[158] LEWIS, James. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. En Center for Strategic and International Studies (CSIS), December 2002, p. 1. Traducción libre. *'Cyber-terrorism is the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.'*

[159] VERTON, Dan. Loc. cit.

La conceptualización del ciber-terrorismo en base al ataque perpetrado en contra infraestructura crítica ha cautivado a numerosos autores estadounidenses, debido a que los casos de estudio propuestos, en su mayoría, se han concentrado en este tipo de ataque, además del hecho de que existe un temor comprensible respecto del efecto dominó que podría generarse en todo el país si uno de estos ataques resultara exitoso.

5. Dos tendencias: uso restringido y uso amplio del concepto.

Dentro de la discusión sobre el concepto de ciber-terrorismo se distinguen dos tendencias, dependiendo de si el término se utiliza de manera restringida o de manera amplia. La primera tendencia (uso restringido) es representada por autores que asocian el concepto con los elementos del terrorismo en sentido tradicional, apuntando a la aptitud del ataque de producir un daño efectivo en la población civil. Mientras que la segunda tendencia (uso amplio) relaciona el concepto de ciber-terrorismo con el uso de la tecnología asociada a Internet y las redes informáticas como medio para llevar a cabo actos de terrorismo.

Huelga decir que ambas tendencias aparecen muchas veces integradas en las definiciones que se han ido elaborando a lo largo de los últimos años para explicar este fenómeno, aunque existe una marcada preferencia de los autores por definir el ciber-terrorismo sobre la base del uso de las redes informáticas para perpetrar los ataques.

a) Uso restringido

La definición de ciber-terrorismo en base al uso de Internet para facilitar o expandir los efectos del terrorismo, entendido como ataque violento en contra de no-combatientes, corresponde al uso restringido del concepto, ya que da cuenta de la importancia de que el ataque cause un daño físico considerable a la población civil para poder calificarlo como tal.

También, la definición de ciber-terrorismo como ataques en contra de sistemas esenciales que dependen de tecnología cibernética sería considerada como un uso restringido del concepto, ya que se refiere a formas de terrorismo tradicionalmente entendidas que causan daño desmedido a la población civil (v.gr. terrorismo nuclear).

El uso restringido del concepto de ciber-terrorismo limita drásticamente el número de casos que se pueden calificar como tal, ya que el énfasis se encuentra en los efectos que produce el ataque. En este tipo de definiciones la atención se centra en el acto terrorista que persigue la conducta de forma directa o indirecta.

b) Uso amplio

La otra tendencia sobre el concepto de ciber-terrorismo, lo define de manera amplia como “cualquier acto de terrorismo que utilice sistemas de información o tecnología

digital (computadores o redes computacionales) ya sea como un instrumento o como objeto del ataque"[160]. Esta es la tendencia mayoritaria en la actualidad y se presenta en mayor o menor medida en la construcción de los conceptos de ciber- terrorismo por parte de los estudiosos de la materia.

En este caso se pone énfasis en el uso de Internet y las redes computacionales como un instrumento que ayuda a perseguir los fines del terrorismo de manera directa o indirecta, ampliando la cantidad de casos que podrían considerarse como ciber-terrorismo.

Una connotación tan amplia de ciber-terrorismo que incluye el uso de Internet y los sistemas computacionales con fines que se relacionan sólo indirectamente con un ataque terrorista (comunicación, propaganda política, financiamiento, reclutamiento, etc.) puede ser cuestionable.

6. Tecnologías cibernéticas: medio de ataque y blanco del ataque

Adicionalmente, es posible hacer una distinción según si Internet y las redes computacionales empleadas por los grupos o agentes terroristas se usan como medio de ataque o como blanco del ataque.

[160] FLEMMING, Peter y STOHL, Michael. *Myths and Realities of Cyberterrorism.* Paper preparado para la International Conference on Countering Terrorism Through Enhanced International Cooperation, 22-24 de Septiembre de 2000, Courmayeur, Italia, p. 31. Traducción libre.'*We have chosen to define cyber terrorism as any act of terrorism that uses information systems or digital technology (computers or computers networks) as either an instrument or target'*.

Ignacio Subijana[161] distingue entre una perspectiva medial y una final. La primera "se estructura en torno a dos elementos: la presencia de un grupo terrorista y el empleo de una infraestructura tecnológica para lograr la ampliación de su capacidad operativa", mientras que la perspectiva final "toma como referente la destrucción de información sensible contenida en los sistemas telemáticos o informáticos".

En este sentido en el uso de Internet y las redes computacionales para facilitar o expandir los efectos del terrorismo tradicional se estarían utilizando las tecnologías cibernéticas como medio de ataque, mientras que en el caso de los ataques en contra de infraestructuras esenciales que dependen de tecnología cibernética, la misma se convertiría en el blanco del ataque.

Finalmente, este autor plantea una perspectiva holística para entender el concepto de ciber-terrorismo, donde se incorporan ambas perspectivas (medial y final), definiéndolo como "cualquier acto realizado a través de tecnologías de información que pueda lograr directa o indirectamente causar terror o generar daños significativos a un grupo social o político a través de la destrucción del soporte tecnológico de cualquiera de sus infraestructuras fundamentales" [162]. Este concepto mezcla el uso de las tecnologías cibernéticas en el acto terrorista con el objeto de destruir el soporte tecnológico que una infraestructura fundamental.

[161] SUBIJANA, Ignacio. *El ciberterrorismo: Una perspectiva legal y judicial*. Revista ENGUZKILORE, Número 22, San Sebastián, Diciembre 2008, p. 172 y ss.
[162] Ibídem., p. 173.

7. Elementos característicos del ciber-terrorismo.

Sin perjuicio de las diferentes posiciones antes expuestas en relación con el concepto de ciber-terrorismo, la mayoría de los autores[163] coinciden en que Internet y las redes de información computacional brindan muchas ventajas a los grupos terroristas, ya que facilitan la comunicación entre las células de los diferentes grupos, son fáciles de obtener y operar (fácil acceso), son económicas y más baratas que los métodos de terrorismo tradicional, les brindan invisibilidad a los actores (anonimato) y potencian la ubicuidad de sus ataques, aumentando el miedo que se genera entre la población que desconoce el potencial de devastación que se puede causar con el uso de la nuevas tecnologías de la información y tiende a sobredimensionar sus posibles alcances.

Frente a la disparidad de criterios para definir este fenómeno y la existencia de una gama de combinaciones posibles entre los elementos que caracterizan las tendencias que pueden identificarse al respecto, algunos autores prefieren combinar los conceptos utilizados por los expertos entorno a la intención y los efectos del ataque, definiendo ciber-terrorismo como "el uso de computadores como armas de ataque u objeto del ataque, por grupos internacionales o sub-estatales, o agentes clandestinos, políticamente motivados, que hacen uso o amenazan con hacer uso de la fuerza y el miedo con el

[163] Ver por ejemplo, SÁNCHEZ, Gema. *Ciberterrorismo. La guerra del siglo XXI*. Revista El Viejo Topo, N º 242, 2008, p. 23. [en línea] <http://dialnet.unirioja.es/servlet/articulo?codigo=2542384> [consultado: 28.08.2012]; WEIMANN, Gabriel. *Cyberterrorism. How real is the threat?* United States Institute of Peace (USIP), Special Report Nº 119, 2004, p. 6.

objeto de influenciar a una audiencia o provocar que un gobierno cambie sus políticas".[164]

En conjunto con lo anterior, también se pone énfasis en la motivación política que debe estar presente en la comisión de los ataques, definiendo ciber- terrorismo como "violencia premeditada y políticamente motivada perpetrada en contra de blancos no combatientes por grupos sub-nacionales o agentes clandestinos, a través de medios de programas computacionales y mecanismos de transmisión de datos como el Internet"[165], dando cuenta de la necesidad de que la definición de ciber-terrorismo contenga los elementos característicos del terrorismo.

En definitiva, lo que caracteriza al ciber-terrorismo y lo que lo diferencia del terrorismo en sentido estricto es el uso de Internet y las tecnologías computacionales como una herramienta para perpetrar ataques en contra de infraestructura fundamental o crítica de un país (energía eléctrica, combustibles, transporte, sistemas de suministro de agua potable, etc.) o en contra de bases de información de alta importancia para el desarrollo del mismo (lo que podría llegar a producir daños en la población civil),

[164] WILSON, Clay. *Computer Attack and Cyberterrorism: Vulnerabilities and Policy issues for Congress.* En LINDEN, Edward L. Focus on Terrorism, Vol 9, Nova Science Publishers, Inc., 2007, p. 6. Traducción libre. *'Cyberterrorism may be defined as the use of computers as weapons, or as targets, by politically motivated international, or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies'.*

[165] JAIN, Gaurav. *Cyber Terrorism: A Clear and Present Danger to Civilized Society?* Information Systems Education Journal, Volume 3, Number 44, August 12, 2005, p. 3. [en línea] <http://isedj.org/3/44/> [consultado: 31.08.2012]. Traducción libre. *'Cyber terrorism can be defines as premeditated, politically motivated violence perpetuated against non-combatant targets by sub-national groups or clandestine agents, through means of computer programs and data transfer mechanism such as the Internet.'*

además de la motivación política que existe en el grupo o agente subestatal para cometer ese acto, causando terror generalizado en la población.

De esta forma, se delimita el significado de ciber-terrorismo, permitiendo diferenciar este fenómeno de aquellos con los cuales se le tiende a confundir y a su vez comprender los alcances del mismo dependiendo de la definición que se utilice y la perspectiva que se adopte para describirlo.

8. El ciber-terrorismo vs. el ciber-crimen.

En la literatura especializada se ha entendido por ciber-crimen "el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual"[166].

El elemento en común, que suele confundir a las personas en el uso de los conceptos de ciber-terrorismo y el ciber-crimen, para calificar una situación en particular, es el hecho de que ambos fenómenos se desarrollan a través de Internet utilizando muchas

[166] ROMEO CASABONA, Carlos María. *"De los delitos informáticos al cibercrimen. Una aproximación conceptual y político- criminal."* En ROMEO CASABONA, Carlos María y Otros. *El Cibercrimen: Nuevos retos jurídico-penales. Nuevos desafíos político-criminales.* Editorial Comares, Granada, 2006, p. 9.

veces mecanismos de operación similares, como en el caso de la acción de los llamados *hackers*. Esto genera la peligrosa tendencia de calificar todas las conductas en que se utilice Internet como medio para cometer un acto ilícito como ciber-terrorismo, atendiendo a la connotación negativa que otorga la palabra "terrorismo" en la descripción de cualquier acto, dado que, "[e]n el uso común actual, 'terrorismo' es un rótulo que aplicamos a determinados actos de violencia política para quitarles legitimidad"[167].

Sin perjuicio de lo anterior, el ciber-terrorismo y el ciber-crimen se diferencian principalmente en que en el primer caso se puede identificar una motivación política de la conducta, mientras que en el segundo caso el acto obedece a una agenda personal o al intento de obtener un beneficio económico por parte del sujeto que lo comete. En este sentido, el intrusismo y el sabotaje informático que favorecen la comisión de delitos relacionados con pornografía infantil, correos electrónicos *spam* o el robo de información de tarjetas de crédito no podrían considerarse como ciber-terrorismo[168], sino que sólo configurarían un delito en la medida que estén tipificados estos actos en la ley del país respectivo.

En nuestro país, por ejemplo, la ley 19.223 de 1993 tipificó figuras penales relativas a la informática, condenando principalmente la destrucción maliciosa de sistemas de

[167] BELLAMY, Alex. Op. Cit., p. 213.
[168] JAIN, Gaurav. Op. Cit., p. 3.

tratamiento de información[169] y la información contenida en ellos[170], además del acceso a sistemas de información para conocer la información contenida en ellos[171] y la difusión de los datos contenidos en los sistemas de tratamiento de información[172]. En consecuencia, la actual normativa en Chile, a través de esta ley, condena las conductas de intrusismo y sabotaje informático en general (incluyendo lo que conocemos como *hacking*), siguiendo el ejemplo de otros países[173] y acogiendo las sugerencias de organismos internacionales sobre la forma de tratar estos ilícitos.

Como han observado algunos autores[174], en la formulación de esta ley se adoptó un modelo fenomenológico para tratar estos nuevos delitos, poniendo énfasis en el medio comisivo para la formulación del tipo, mientras que, en la actualidad, existe un proyecto de reforma de esta ley, que no tiene urgencia en el Congreso, que intenta formular la tipología de los delitos informáticos como se hace generalmente con los demás delitos en la dogmática penal, es decir, relacionándolo con la afectación a un bien jurídico protegido y sólo en segundo término con el medio comisivo.

[169] "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo." (Artículo 1º, Ley 19.223).
[170] "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio." (Artículo 3°, Ley 19.223).
[171] "El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio." (Artículo 2°, Ley 19.223).
[172] "El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado." (Artículo 4°, Ley 19.223).
[173] En la historia de la ley se mencionan como ejemplos en la materia Estados Unidos, Francia, Alemania, Austria y Suiza.
[174] LORDOÑO MARTÍNEZ, Fernando. *Los delitos informáticos en el proyecto de reforma en actual trámite legislativo*. No. 4 (2004): Revista de Derecho Informático, 2004, p. 172-174. [en línea] <http://www.boletinfilologia.uchile.cl/index.php/RCHDI/article/viewPDFInterstitial/10679/10959> [consultado: 20.09.2012].

La discusión que se está planteando doctrinariamente a nivel nacional sobre la forma de abordar legislativamente el nuevo fenómeno criminológico que se presenta en la sociedad globalizada entorno al uso de Internet y las nuevas tecnologías de la información tiene especial relevancia también a nivel internacional, puesto que en el futuro, el resultado de la posición que se adopte frente a este tipo de problemática también tendrá repercusiones en la posición que se adopte a la hora de abordar el fenómeno del ciber-terrorismo desde una perspectiva penal internacional.

Esto es así, debido a que se podría optar por tipificar una nueva conducta antijurídica con características propias y crear una nueva convención sobre la materia o bien, se podría realizar una aplicación integral de las normas existentes en función del bien jurídico protegido, lo que en este caso conduciría a la aplicación de los diferentes instrumentos de carácter internacional que condenan aquellas conductas calificadas como terroristas.

Independientemente de la posición que se adopte en el futuro sobre la forma de penalizar las conductas de ciber-terrorismo, lo cierto es que existe una diferencia entre este fenómeno y el ciber-crimen en general, o los delitos informáticos en particular[175]. Ello no puede ser obviado, ya que una falta de claridad conceptual a este respecto podría

[175] Donde, a diferencia del ciber-crimen, la red utilizada tiene una relevancia limitada o secundaria para las características de la conducta delictiva, puesto que se trata de redes cerradas o de acceso restringido (como por ejemplo, el *hacking*). Esto ha generado una tendencia a la utilización del concepto de ciber-crimen o ciber-delito para la calificación de los nuevos delitos que se cometen en todo tipo de redes (abiertas o cerradas), donde el uso de los sistemas informáticos cobra real importancia (como por ejemplo, en el caso del *phishing*). (ROMEO CASABONA, Op. Cit., pp.6-10).

conducir a elevar la cantidad de casos que se califican como ciber-terrorismo, lo que a su vez aumentaría la influencia que pueden ejercer algunos países sobre la forma de regular o limitar el uso de Internet en nombre de la seguridad nacional y la guerra contra el ciber-terrorismo, cuestión que se abordará más adelante.

9. El ciber-terrorismo vs. el *hacktivism*.

9.1. Ciber-activismo

El activismo cibernético o ciber-activismo se ha posicionado como una nueva forma de expresión de la ciudadanía a través de las redes de Internet, donde las personas de diferentes partes del mundo pueden ponerse en contacto y organizar manifestaciones de diversa índole[176]. Esta nueva forma de expresión puede definirse como "el uso normal y no problemático de Internet en apoyo de una agenda o una causa"[177], de manera tal que la creación de sitios web para subir material en ellos o el uso de la red para discutir asuntos podrían considerarse como ejemplos de este tipo de activismo.

[176] Los ejemplos prácticos serán tratados exhaustivamente en el siguiente capítulo.
[177] DENNING, Dorothy. Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. En ARQUILLA, John y RONFELDT, David. Networks and Netwars: The Future of Terror, Crime, and Militancy. Editorial RAND, Estados Unidos, 2001, p. 241. [en línea] <http://books.google.cl/books?hl=es&lr=&id=VKFMTDnapl4C&oi=fnd&pg=PA239&dq=activism,+hacktivism+and+cyberterrorism&ots=jEeGN5QkHe&sig=l8uRBWbpwhMsWC1LbFesgVlZ28&redir_esc=y#v=onepage&q=activism%2C%20hacktivism%20and%20cyberterrorism&f=false> [consultado: 22.09.2012].

Las plataformas de Internet que hoy en día se configuran como el lugar paradigmático de encuentro de los activistas en el ciberespacio son las redes sociales, como *Facebook* o *Twitter,* que se caracterizan por ser de naturaleza estructural anárquica y horizontal, cuestión que "posibilita una gran robustez del flujo de comunicaciones, lo que deriva en un mayor acceso a la información y una menor capacidad para limitar dicho acceso"[178]. Lo anterior potencia el desarrollo de diferentes movimientos en la red con alcances inesperados y una gran capacidad para influenciar el cambio en las políticas públicas de un país o de una región.

Este tipo de activismo no plantearía problemas a la hora de diferenciarlo del ciber-terrorismo, debido a que en rigor se trataría de una legítima forma de ejercer la libertad de expresión y la libertad de asociación por parte de aquellos que deciden manifestarse y organizarse a través de los medios que brindan hoy en día el Internet y las redes computacionales. Desde luego, tal como sucede con las manifestaciones en el mundo físico, algunas de estas acciones en el mundo virtual pueden degenerar en un ilícito.

[178] SUAZO VEJARES, Sótero ; MARTÍNEZ ORTIZ, Javier ; ELGUETA RUIZ, Álvaro Patricio. *Redes sociales como herramientas de ciberactivismo: el caso de los grupos de Facebook en Chile y el Gran Concepción (2009)*. En Ecos de la Comunicación, Año 4, Nº 4, 2011, p. 155. [en línea] <http://bibliotecadigital.uca.edu.ar/repositorio/revistas/redes-sociales-como-herramientas-ciberactivismo.pdf > [consultado: 24.09.2012].

9.2. *Hacktivism*

Dando un paso más allá del mero ciber-activismo, se distingue el llamado *hacktivism*[179] que se relaciona con grupos que no necesariamente obedecen órdenes ni tienen un objetivo político definido y que actúan en el límite de la legalidad utilizando ataques como la "denegación de servicio" (*Denial of Service* o DoS), que afecta la disponibilidad de un sitio de Internet en un momento determinado, o el *hacking*, para acceder a información confidencial que manejan los gobiernos y las compañías multinacionales, para luego difundirla en la red[180].

También algunos autores[181] consideran el método de "bloqueo" *(virtual sit-in* o *blockade)* como una forma de *hacktivism*, aunque otros consideran que esta acción constituye sólo una expresión más del activismo cibernético, toda vez que no abusa del sistema en sentido técnico, ya que se sus efectos sólo pueden generarse cuando un gran grupo de personas previamente concertadas al respecto sobrecarga una página web específica entorpeciendo su funcionamiento.[182]

---

[179] Concepto creado a partir de la combinación de *hacking* y *activism* como forma de describir el uso del intrusismo informático como una herramienta de activismo cibernético.
[180] SLOBBE, J. y VERBERKT, S.L.C. *Hacktivists: Cyberterrorists or Online Activists?* An Exploration of the Digital Right to Assembly. 2012, p. 5. [en línea] <http://arxiv.org/abs/1208.4568> [consultado: 02.09.2012].
[181] YAR, Majir. *Cybercrime and Society*. SAGE Publications Ltd, Londres, 2006, p. 48. [en línea] <http://books.google.cl/books?id=LyNEk9y9GOUC&pg=PA48&lpg=PA48&dq=virtual+sitin&source=bl&ots=J1WCpktPp&sig=mNtF7rXEDAnNVfYKtSAEH4innSE&hl=es&sa=X&ei=kW1gUJ3pGqu_0QG1goHgBA&ved=0CEEQ6AEwAw#v=onepage&q=virtual%20sit-in&f=false> [consultado: 24.09.2012].
[182] SLOBBE, J. y VERBERKT, S.L.C. Op. Cit., p. 4.

Los ataques que son perpetrados por grupos como “Anonymous” o “Lulzsec” se suelen confundir con ataques ciber-terroristas debido a que el elemento del uso de Internet y las tecnologías computacionales es compartido por ambos, pero lo que diferencia los ataques de los llamados *hacktivists* de los ataques de un ciber-terrorista es el hecho de que el primero no tiene una motivación política que fundamente su actuar (con excepción del ideal de libertad absoluta de Internet) y no busca provocar daño o aterrorizar a la población civil, sino que busca liberar información en la red; mientras que en el caso del ciber-terrorista la existencia de una motivación política es manifiesta y aunque no siempre se genere un daño grave contra la población civil, el objetivo es causar un gran impacto, aterrorizando a la población.

Sin perjuicio de que algunas prácticas de *hacktivism* pueden ser constitutivas de ilícitos, en la medida en que se cometan ciber-crímenes o delitos informáticos en la persecución de sus objetivos, es evidente que de no cumplir con las características que anteriormente se analizaron en torno al ciber-terrorismo sería inapropiado calificarlo como tal, debido a que, a pesar de que pueda recurrir a los mismos métodos de *hacking* u otras formas de sabotaje e intrusismo informático[183], no se persigue el mismo objetivo ni se genera el mismo efecto en la población civil.

[183] Tales como *cracking*, *sniffing* o denegación de servicio.

CAPÍTULO IV

ANÁLISIS DE ATAQUES CONSIDERADOS COMO CIBER-TERRORISTAS

1. Generalidades

Durante los últimos años se ha desarrollado una marcada tendencia de la prensa internacional de calificar ciertos hechos como ciber-terrorismo, sin realizar un mayor análisis sobre las características que presentan dichos ataques para determinar si cabe o no dentro del concepto.

En esta sección analizaremos algunos casos que la prensa ha calificado como ciber-terrorismo, poniendo énfasis en las características del hecho para tratar de enmarcarlo dentro de alguno de los conceptos analizados en el capítulo anterior (activismo cibernético, delitos informáticos, etc.).

Este estudio se hará a partir de algunos casos escogidos que han causado mayor o menor revuelo mediático en los últimos 10 años y que aún siguen siendo discutidos y citados entre los círculos de especialistas, dada la escasa o nula existencia de casos comprobables de ataques ciber-terroristas propiamente tales.

2. Organizaciones mediáticas asociadas con ataques cibernéticos

Existe una serie de organizaciones que se suelen identificar con ataques cibernéticos y comúnmente se asocian con el ciber-terrorismo. A continuación analizaremos los casos de Anonymous, LulzSec y Wikileaks, como los grupos emblemáticos que usualmente se vinculan con el terrorismo en la web.

2.1. *Anonymous*[184]

2.1.1. Inicios

Los inicios de "*Anonymous*" se asocian a la página web "4chan.org", creada el 1 de octubre de 2003, que fue diseñada para compartir fotos, videos e información de todo tipo, clasificada en diferentes categorías propuestas, sin ningún tipo de restricción en cuanto a su contenido.

Junto con lo anterior, ese sitio permitía el completo anonimato de los usuarios, ya que si éstos no querían identificarse con sus nombres, se les daba la posibilidad de subir contenidos a la web bajo la denominación de "*Anonymous*" (Anónimo en inglés).

[184] PRABHJEET, Kaptaan (27.02.2013) *How Hackers Changed the World - BBC documentary 2013*. [en línea] <http://www.youtube.com/watch?v=Rj35GguOAGE> [consultado: 05.06.2013].

Las condiciones que ofrecía esta página web fomentaron una explosión de creatividad por parte de los usuarios, que buscaban llamar la atención de los demás visitantes de la página publicando contenidos llenos de humor y sarcasmo, que muchas veces llegaban a ser grotescos, pero que sin duda causaban un gran impacto en su audiencia.

Dentro de los variados contenidos que aún se pueden encontrar en "4chan.com" se destacan los llamados "memes"[185] (que en la actualidad son ampliamente difundidos en las redes sociales), discusiones sobre comics o animé y enlaces para descargar películas gratis de todo tipo.

El formato único que implementó esta página web y su creciente popularidad, hizo que en la práctica la mayoría de los usuarios compartieran contenidos de manera anónima, de forma tal que parecía, desde el punto de vista de un observador externo, que un solo sujeto, llamado "*Anonymous*", compartía y comentaba los contenidos subidos a la página.

Esta situación creaba la sensación de que todos los usuarios de internet eran uno solo y de que en este estado de anonimato virtual que les brindaba la red residía su poder como conjunto. Eran todos y ninguno al mismo tiempo.

[185] Idea que se transmite a través de una imagen.

Luego de alcanzar esta autoconciencia, los diferentes "*Anonymous*" se coordinaron en grupos para realizar "bromas" en otros sitios de internet, utilizando técnicas de *hacking*[186] o simplemente abusando de las potencialidades de determinadas páginas web[187]. El éxito de estos experimentos creó en los involucrados una sensación de pertenencia, ya que se descubrió el poder de la comunidad de internautas organizados, que manejaba códigos propios y era capaz de influir en otros mediante la creación de una cultura común.

2.1.2. Ataques

El primer ataque conocido de "*Anonymous*" fue en contra de la página web de Harold Turner, un hombre estadounidense que transmitía un programa de radio a través de Internet. Las opiniones vertidas en este sitio eran abiertamente racistas y para mostrar su repudio hacia este personaje, un grupo de individuos que se identificó como *Anonymous* comenzó a realizar diferentes intervenciones en esta página web entre los meses de diciembre del año 2006 y enero del año 2007, que lograron sacarlo del aire.[188] Turner respondió demandando a "4chan.org" por infracción a la ley de derechos de autor.[189]

---

[186] Como DDoS (denegación de servicio).
[187] Caso de HABBO, en que un grupo organizado de internautas crearon cientos de personajes en la plataforma mencionada para burlarse de los demás usuarios.
[188] OLSZEWSKI, Anthony. *Internet War waged against Hal Turner, Hudson County hate monger and FBI informant.* 07.04.2010. En Hudson County Facts. [en línea] < http://hudsoncountyfacts.com/hudsoncounty/?p=1165> [consultado: 06.08.2013].
[189] Resumen del juicio disponible en Internet <http://dockets.justia.com/docket/new-jersey/njdce/2:2007cv00306/198438/> [consultado: 06.08.2013].

En el año 2008 *Anonymous* se vio involucrado en el llamado "Proyecto Chanología" (*Project Chanology*) que tenía como blanco de burlas a la Iglesia de Cienciología. Inicialmente, se difundió masivamente en internet un video de Tom Cruise describiendo las bases de su fe[190]. Ante esto, la Iglesia envió una carta de cese y desistimiento por infracción a los derechos de autor de dicho video. Frente a esto *Anonymous* respondió con una serie de ataques de denegación de servicio a los sitios web de la organización y con manifestaciones en las afueras de las iglesias alrededor del mundo, usando la máscara característica de la novela gráfica de Guy Fawkes, "*V for Vendetta*".

Durante ese mismo año, *Anonymous* subió a Internet un video con una declaración de guerra en contra de esa religión y las ideas que enarbola[191]. Además, se hizo circular un video en la red con el código de conducta que debería observarse durante las manifestaciones públicas realizadas en representación del grupo[192].

La Iglesia de Cienciología reaccionó denunciando a los manifestantes e iniciando acciones legales ante tribunales. Frente a esto las manifestaciones en su contra fueron decreciendo en cuanto a la convocatoria y los ataques de denegación de servicio se hicieron menos frecuentes.

---

[190] Aleteuk. (17/01/2008). *Tom Cruise Scientology Video - (Original UNCUT)*. [en línea] <http://www.youtube.com/watch?v=UFBZ_uAbxS0> [consultado: 05.06.2013].

[191] Church0fScientology. (21/01/2008). *Message to Scientology*. [en línea] <http://www.youtube.com/watch?v=JCbKv9yiLiQ> [consultado: 05.06.2013].

[192] Church0fScientology. (01/02/2008). *Code of Conduct*. [en línea] Disponible en <http://www.youtube.com/watch?v=-063clxiB8I> [consultado: 05.06.2013].

El 2010 se gestó la llamada “Operación Venganza” (*Operation Payback*).

Algunas organizaciones como PayPal, MasterCard y Visa congelaron las donaciones a *Wikileaks* mediante estos medios debido a presiones políticas en el marco de la polémica que se generó a nivel mundial respecto de los cargos que enfrentaba Julian Assange. [193] Frente a esto, *Anonymous* respondió con una serie de ataques de denegación de servicio a los sitios web de estas organizaciones durante el mes de diciembre de 2010, causando más que una simple molestia. Con la caída de estos sitios el número de transacciones realizadas a través de Internet disminuyó, lo que socavó la confianza de la población en el sistema de comercio electrónico.[194]

En los últimos años, los ataques de este grupo se han enfocado en sitios web de todo tipo de organizaciones a nivel internacional, justificándose en la defensa de causas sociales. Lo anterior es posible gracias a la formación de células de *Anonymous* alrededor del mundo. Incluso en Chile se produjo una manifestación de este grupo en contra de la construcción del proyecto Alto Maipo, la que se tradujo en un video en que se exigía la renuncia del Subsecretario de Energía Sergio del Campo y cierres de sitios web de menor importancia.[195]

---

[193] BBC News. *Inside PayPal’s high-tech control room*. 18.12.2010. [en línea] <http://www.bbc.co.uk/news/technology-12018487> [consultado: 06.08.2013].
[194] BBC News. *Pro-Wikileaks activist abandon Amazon cyber attack*. 09.12.2010. [en línea] <http://www.bbc.co.uk/news/technology-11957367> [consultado: 06.08.2013].
[195] La Tercera. *Día de la Tierra: Anonymous ataca sitios web en protesta por el proyecto Alto Maipo*. 22.04.2013. [en línea] <http://www.latercera.com/noticia/tendencias/2013/04/659-519968-9-dia-de-la-tierra-anonymous-ataca-sitios-web-en-protesta-por-el-proyecto-alto.shtml> [consultado: 05.08.2013].

Resumiendo, la forma en que actúa *Anonymous* se puede catalogar como activismo cibernético o *hacktivism* (según las definiciones utilizadas en el capítulo anterior), donde predominan ataques de denegación de servicio que hacen caer determinados sitios web como una forma de manifestarse en contra de una situación particular.

Los ataques de este grupo no buscan generar terror en la población, sino que, más bien, su motivación es manifestar su descontento ante una situación que ellos creen que es errónea en base a los principios que regulan internet y la cosmovisión que comparten los internautas en la web[196]. En este sentido, sus ataques buscan provocar una reacción de las autoridades y de los involucrados en los conflictos específicos, pero este impacto no se enmarca dentro de los elementos característicos del terrorismo, ni del ciber-terrorismo.

En definitiva, estos ataques utilizando las técnicas del *hacking*, como la denegación de servicio, pueden ser catalogados como delitos informáticos y son castigados según las medidas que se prevean en la legislación de cada país.

2.2. *LulzSec*

Este grupo se creó con el único fin de burlarse de la seguridad de los sitios de internet de compañías reconocidas mundialmente y de organizaciones gubernamentales.

[196] A saber, libertad de expresión, no-discriminación, etc.

De ahí su nombre ("*LulzSecurity*"[197]) y su lema ("Riéndose de su seguridad desde 2011")[198].

LulzSec se formó el 2011 por un grupo de hackers, como una alternativa a lo que había demostrado Anonymous los años anteriores. Su primer ataque registrado fue en mayo de ese mismo año, en contra de FOX. Este grupo ingresó a la base de datos del programa "Factor X" (*X-Factor*) y filtró información personal de los participantes del programa.[199]

Luego atacaron a PBS entrando a su sistema de noticias por internet y publicando una información falsa sobre un cantante de hip-hop. Ese medio publicó que Tupac Shakur, fallecido en 1996, había sido encontrado vivo en Nueva Zelanda.[200]

A principios de junio de ese mismo año Sony fue víctima de una nueva intervención en sus bases de datos. *LulzSec* reveló información sobre las cuentas de sus clientes, incluyendo información personal y sus claves de acceso.[201]

---

[197] *Lulz*, en el lenguaje coloquial americano, es una degeneración de la expresión LOL (*Laughting Out Loud*) que significa diversión o risa provocada a expensas de un tercero.
[198] *Laughing at your security since 2011.*
[199] Fox News. A Brief History of the LulzSec Hackers. 21.06.2011. [en línea] < http://www.foxnews.com/tech/2011/06/21/brief-history-lulzsec-hackers/> [consultado: 06.08.2013].
[200] The Washington Post. *Name and faces: PBS website hacked.* 30.05.2011. [en línea] <http://www.washingtonpost.com/blogs/reliable-source/post/names-and-faces-pbs-website-hacked-christopher-knight-and-adrianne-curry-separate/2011/05/30/AGoVlwEH_blog.html> [consultado: 06.08.2013].
[201] The Washington Post. *LulzSec to release Sony data this afternoon.* 02.06.2011. [en línea] <http://www.washingtonpost.com/blogs/post-tech/post/lulzsec-to-release-sony-data-this-afternoon/2011/06/02/AGOD1JHH_blog.html> [consultado: 06.08.2013].

En esta misma línea, se le atribuyó a *LulzSec* el ataque a la página web de *The Sun*, periódico de prensa amarilla británico, robando información sobre sus suscriptores (nombres, direcciones, números de teléfonos y correos electrónicos).[202]

Todos estos ataques iniciales buscaban mostrar las debilidades de los medios de seguridad a nivel informático y fueron calificados por la prensa como "vandalismo cibernético", aunque la mayoría estaba ligado a una manifestación en contra de algún hecho (en esa época reventaba el escándalo de *Wikileaks* y muchos actos se cometieron en favor de Julian Assange, por ejemplo).

En una fase posterior, *LulzSec* se atribuyó una serie de ataques a páginas del gobierno de Estados Unidos (como la CIA, el FBI y el Senado)[203], del Reino Unido (SOCA, una agencia que persigue al crimen organizado)[204] y de Brasil[205], entre otros. En todos estos ataques lo que se buscaba era hacer caer las páginas de las instituciones asociadas y hacer pública la vulnerabilidad que existía frente a este tipo de acciones.

---

[202] BBC News. *Data of Sun website users stolen.* 02.08.2011. [en línea] <http://www.bbc.co.uk/news/technology-14371738> [consultado: 06.08.2013].

[203] The Washington Post. *CIA Web site hacked; group LulzSec takes credit.* 16.06.2011. [en línea] <http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html> [consultado: 06.08.2013].

[204] BBC News. *Soca website taken down after LulzSec 'DDoS attack'*. 20.06.2011. [en línea] <http://www.bbc.co.uk/news/technology-13848510> [consultado: 06.08.2013].

[205] Noticias Montreal. *Una nueva víctima de los hackers: el gobierno de Brasil.* 22.06.2011. [en línea] <http://noticiasmontreal.com/4789/una-nueva-victima-de-los-hackers-el-gobierno-de-brasil/> [consultado: 06.08.2013].

Después de casi dos meses de funcionamiento y una seguidilla de ataques, *LulzSec* anunció el fin de sus operaciones.[206] Habían demostrado un punto: la seguridad en Internet era una cuestión ilusoria, ya que no existía ningún sitio web infranqueable.

Todos los ataques atribuidos a este grupo fueron realizados a través de técnicas del *hacking* que, al igual que en el caso de *Anonymous*, pueden calificarse como delitos informáticos comunes y pueden ser castigados dependiendo de la normativa existente en cada país.

Entre el año 2012 y 2013 varios de los integrantes de *LulzSec* fueron condenados a un tiempo de prisión (entre 24 y 36 meses) y trabajo comunitario (entre 500 y 1000 horas) por los delitos de los que se les encontró culpables (principalmente *hacking*), en el Tribunal de la Corona de Southwark (*Southwark Crown Court*).[207]

[206] Noticias Montreal. *Grupo de hackers LulzSec anuncia el fin de sus operaciones*. 26.06.2011. [en línea] <http://noticiasmontreal.com/4795/grupo-de-hackers-lulzsec-anuncia-el-fin-de-sus-operaciones/> [consultado: 06.08.2013].

[207] BBC News. *LulzSec hacker group handed jail sentences*. 16.05.2013. [en línea] < http://www.bbc.co.uk/news/technology-22552753> [consultado: 06.08.2013].

2.3. *Wikileaks*[208]

2.3.1. Inicios y primeras polémicas

Esta organización y su respectiva página web, se creó el 2006 con el objeto de permitir a los usuarios filtrar de manera anónima información confidencial sobre diferentes organizaciones, que pudiera ser de interés público.

Inicialmente este proyecto fue visto con desconfianza por parte de algunos sectores de la prensa que sospechaban de los motivos ocultos que pudieran tener sus impulsores (quienes, en un primer momento, se mantuvieron en el anonimato) y los mismos usuarios al divulgar este tipo de documentos en Internet.[209]

A partir de enero de 2007, Julian Assange asumió el liderazgo público de la organización y el reconocimiento mediático como el fundador de *Wikileaks.* Junto a él trabajaba un grupo de ingenieros, matemáticos y profesionales de los cinco continentes.

En febrero de 2008 el Tribunal del Distrito Norte de California, Estados Unidos (*United States District Court for the Northern District of California*), ordenó cerrar el sitio temporalmente debido a la demanda de un banco suizo, basada en que se había

[208] Ver: www.wikileaks.org
[209] BBC News. *Who stands to gain from Wikileaks?* 13.03.2007. [en línea] <http://news.bbc.co.uk/2/hi/technology/6443437.stm> [consultado: 08.08.2013].

publicado en esa página web documentos que involucraban al banco con lavado de dinero y evasión de impuestos.[210] Este incidente indujo a los representantes de *Wikileaks* a preferir los *hostings* de Suecia o de otras localidades donde las respectivas Constituciones resguardan la libertad de prensa sin censura previa.

Durante el mes de septiembre de ese mismo año, *Wikileaks* se vio involucrado en otro escándalo, debido a la publicación en su sitio una serie de correos electrónicos e información personal de Sarah Palin[211], que fue obtenida a través del *hacking* de su cuenta en "www.yahoo.es" por parte de *Anonymous*.[212]

Durante el 2009 Wikileaks se puso nuevamente en la palestra al cuestionarse la veracidad de una información que se había filtrado en ese sitio el año anterior. En este caso, un listado de los miembros del Partido Nacional Británico y una serie de datos personales de los mismos.[213]

---

[210] BBC News. *Whistle-blower site taken offline*. 18.02.2008. [en línea] <http://news.bbc.co.uk/2/hi/technology/7250916.stm> [consultado: 09.08.2013].

[211] Gobernadora de Alaska entre diciembre de 2006 y julio de 2009. En esa época disputaba una reñida campaña en contra de John McCain por representar la candidatura del Partido Republicano a la vice-presidencia de Estados Unidos.

[212] BBC News. *Palin's e-mail account plundered.* 18.09.2008. [en línea] <http://news.bbc.co.uk/2/hi/technology/7622724.stm> [consultado: 09.08.2013].

[213] BBC News. *Griffin says leaked BNP list fake*. 20.10.2009. [en línea] <http://news.bbc.co.uk/2/hi/uk_news/politics/8315928.stm> [consultado: 10.08.2013].

2.3.2. Reconocimiento internacional

Wikileaks comenzó a ser mundialmente reconocido a partir de noviembre del año 2010, debido a la polémica que se generó entorno a la publicación en ese sitio de 250.000 mensajes emitidos por diplomáticos de Estados Unidos de embajadas y consulados alrededor del mundo entre los años 1966 y 2010.[214]

Durante el mes de julio de ese mismo año se filtraron 77.000 documentos del gobierno estadounidense relativos al conflicto en Afganistán y durante el mes de octubre habían sido subidos a la web 400.000 documentos sobre la guerra de Irak.

Los documentos filtrados contenían información clasificada o confidencial que dejaba vulnerable al gobierno de Estados Unidos, en tanto exponía su estrategia en materia de política exterior, cuestión que lo convirtió en blanco de las críticas y en motivo de vergüenza para la clase política de ese país.[215]

Estos documentos revelaban comunicaciones con información como la preocupación de ese gobierno sobre la tenencia de armas nucleares en Pakistán[216] y las políticas

[214] BBC News. *US embassy cables: The background*. 29.11.2010. [en línea] <http://www.bbc.co.uk/news/world-us-canada-11862320> [consultado: 10.08.2013].
[215] BBC News. *Diplomatic leaks 'more embarrassment than damage'*. 29.11.2010. [en línea] <http://news.bbc.co.uk/today/hi/today/newsid_9237000/9237029.stm> [consultado: 10.08.2013].
[216] BBC News. *Leaks expose UK and US fears over Pakistan nuclear arms*. 30.11.2010. [en línea] <http://www.bbc.co.uk/news/world-us-canada-11883230> [consultado: 10.08.2013].

armamentistas de países de Medio Oriente en general o las relaciones entre los líderes de Rusia e Italia, por ejemplo.[217]

La responsabilidad de haber filtrado estos documentos fue atribuida a un joven analista militar, Bradley Manning, que trabajaba en el área informática de inteligencia del Ejército de Estados Unidos, a quien se le imputaron una serie de cargos como espionaje, ayudar al enemigo (traición a la patria), fraude computacional y robo de información del gobierno. Durante el mes de agosto de 2013, Manning fue condenado a 35 años de prisión por la mayoría de los cargos formulados en su contra.[218]

De manera paralela, el año 2010 Julian Assange fue acusado de violación y abuso sexual por la policía sueca, por hechos que habrían ocurrido en ese país en agosto de ese mismo año.[219] El fundador de *Wikileaks* negó los cargos desde un primer momento y atribuyó el acto a una persecución política en su contra debido al impacto que habían causado los contenidos filtrados a través de su página web durante ese año.

La policía sueca emitió una orden de captura internacional en contra de Assange mientras éste se encontraba en Londres. La justicia británica falló a favor de la extradición en reiteradas oportunidades ante las apelaciones de la defensa de Assange,

[217] BBC News. *Wikileaks release of embassy cables reveals US concerns.* 28.11.2010. [en línea] <http://www.bbc.co.uk/news/world-us-canada-11858895> [consultado: 10.08.2013].
[218] BBC News. *Bradley Manning sentenced to 35 years in Wikileaks case.* 21.08.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-23784288> [consultado: 25.08.2013].
[219] BBC News. *Timeline: sexual allegations against Assange in Sweden*. 16.08.2012. [en línea] <http://www.bbc.co.uk/news/world-europe-11949341> [consultado: 10.08.2013].

hasta que finalmente en agosto del 2012 la Corte Suprema del Reino Unido dictó sentencia a favor de la extradición.

Frente a lo anterior Assange consiguió asilo político en la embajada de Ecuador en Inglaterra, para evitar el cumplimiento del fallo y ante una real o supuesta amenaza de violación de sus derechos fundamentales en caso de ser extraditado.

2.3.3. Polémicas recientes

El caso de Edward Snowden volvió a poner a *Wikileaks* en la palestra el año 2013.[220]

Snowden, quien trabajaba en la CIA como asistente técnico, filtró información sobre la vigilancia de los datos transmitidos a través de Internet y las grabaciones de las comunicaciones telefónicas que realizaba el gobierno estadounidense de manera ilegal a sus ciudadanos mediante la NSA (*National Security Agency*).

La información se filtró al diario británico *The Guardian*, que posteriormente confirmó la fuente y realizó una entrevista a pedido del propio Snowden para explicar los motivos que tuvo para revelar esa información.[221]

[220] BBC News. *Snowden affair puts Wikileaks back into spotlight.* 28.06.2013. [en línea] <http://www.bbc.co.uk/news/world-latin-america-23077279> [consultado: 11.08.2013].
[221] BBC News. *Edward Snowden says he is NSA Prism leak source in interview*. 09.06.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-22836419> [consultado: 11.08.2013].

Julian Assange y el equipo jurídico de *Wikileaks* prestaron apoyo a Snowden, quien se convirtió en fugitivo de la justicia estadounidense, la que presentó cargos de espionaje y robo de información en su contra.

Snowden pidió asilo en diferentes países mientras escapaba de Estados Unidos y tuvo que volar de Hong Kong a Moscú, debido a la existencia de un tratado de extradición entre Estados Unidos y el país donde se encontraba.

Aunque su intención original era buscar asilo en Ecuador, una vez en Rusia, pasó más de un mes en el aeropuerto debido a que sus documentos de viaje fueron revocados por sus persecutores. Recién en el mes de agosto le permitieron entrar a territorio ruso con la oferta de asilo por el periodo de un año.[222]

En resumen, si bien se tiende a asociar a *Wikileaks* con delitos informáticos, en realidad lo que hace esta organización es servir de plataforma para que se publiquen documentos confidenciales de cara al interés público involucrado en transparentar el contenido de los mismos, por lo que en ningún caso pueden ser condenados jurídicamente, dada la aplicación de los principios de libre expresión y libertad en general que operan en Internet.

[222] BBC News. *Profile: Edward Snowden*. 07.08.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-22837100> [consultado: 11.08.2013].

Esto supone la libertad de publicar cualquier contenido en la web sin censura previa, mientras no afecte los derechos y reputación de los demás, la seguridad nacional, el orden público o la salud y moral públicas. De todas formas, sólo un tribunal podrá ordenar que se elimine el contenido publicado para restablecer el imperio del Derecho en aquellos casos en que un tercero se sienta afectado por la información publicada.

Adicionalmente, existe una división de responsabilidad entre el ente que proporciona la plataforma para publicar la información y aquellos que la publican, donde el primero no tiene ningún control sobre el origen de los contenidos, lo cual hace posible que la página de esta organización siga funcionando de la misma forma desde su creación.

Sin perjuicio de lo anterior, se puede decir que la mayoría de las personas que aportan contenidos a este sitio pueden llegar a incurrir en delitos como *hacking* (*Anonymous*), espionaje (Manning) y robo de información (Manning y Snowden), entre otros; dado que se trata de información confidencial que se filtra a la red aprovechándose de la posición que desempeñan en determinadas organizaciones. Lo anterior hace que sea más fácil acceder a la información y divulgarla de manera ilícita.

3. Ataques perpetrados con el uso de medios informáticos

En este apartado analizaremos algunos casos en que se utilizaron medios informáticos para perpetrar delitos que en algún momento fueron calificados como

ciber-.terrorismo. La mayoría de los casos involucra elementos que fueron analizados en el capítulo anterior, a saber, ataques en contra de infraestructura fundamental, ataque en contra de computadores y uso de los mismos para perpetrar los ataques.

3.1. Planta de tratamiento de aguas de Maroochy

Vitek Boden, un ex trabajador de la planta de tratamiento de aguas servidas de Maroochy Shire, en Queensland, Australia, decidió vengarse de la empresa que la operaba, Hunter Watertech, y del municipio frente a la negativa de contratarlo nuevamente, en al año 2000.

Utilizando un computador portátil y un transmisor de radio, Boden consiguió manipular el funcionamiento de la planta de tratamiento de aguas servidas en 46 oportunidades. Durante dos meses se derramaron 800.000 litros de aguas servidas en los parques aledaños y en un río cercano. Los daños fueron cuantificados en más de 1 millón de dólares australianos.

Boden fue condenado a 2 años de prisión por infringir leyes ambientales y por cometer delitos informáticos.[223]

[223] ABRAMS, Marshall y WEISS, Joe. *Malicious Control System Cyber Security Attack Case Study-Maroochy Water Services, Autralia*. 23.07.2008. [en línea] < http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf> [consultado: 12.08.2013].

Lo que facilitó el ataque fue el hecho de que la planta funcionaba con una red inalámbrica insegura, lo que permitió a Boden operar el funcionamiento de la misma mediante un programa instalado en su computador portátil que le permitía manejar el funcionamiento de las válvulas y cambiar su configuración.[224]

Este caso muestra que un ataque utilizando medios cibernéticos en contra de infraestructuras esenciales, como lo es una planta de tratamiento de aguas servidas, es posible y puede llegar a tener consecuencias terribles en el mundo real. Sin embargo, difícilmente podríamos calificar este caso en particular como ciber-terrorismo, dado que no existió una motivación política en el acto y a pesar del grave daño causado al medio ambiente, no se afectó ninguna vida humana.

3.2. Titan Rain

Este fue el nombre que le dio el FBI a una serie de ataques perpetrados en contra de la red de computadores del gobierno de Estados Unidos y empresas relacionadas durante el año 2003. Un grupo de hackers, presumiblemente chinos, lograron penetrar el sistema informático de Lockheed Martin[225] y de la NASA en búsqueda de información confidencial sobre inteligencia militar.[226]

---

[224] DAVEL. *Harbor to Harbour.* 04.09.2012. [en línea] <http://harbor2harbour.com/?p=144> [consultado: 12.08.2013].

[225] Una empresa dedicada al desarrollo de tecnologías avanzadas en materias de defensa y seguridad, que fabrica armamento para el gobierno de Estados Unidos.

[226] HALL, Kevin. *The 7 worst cyberattacks in history (that we know about)*. 22.07.2010. [en línea] <http://www.dvice.com/archives/2010/09/7_of_the_most_d.php> [consultado: 14.08.2013].

Este episodio fue considerado como el mayor ataque cibernético de la historia, ya que recién el año 2004, un empleado de una de las empresas comprometidas se percató de que el sistema de seguridad había sido vulnerado.

A pesar de que es un caso conocido entre los expertos en ciber-seguridad, no existe registro del mismo en la prensa tradicional de la época y los datos disponibles son escasos. Nunca se pudo condenar a nadie por el hecho, ni se confirmó con exactitud qué información lograron extraer durante las intervenciones, ya que utilizaron un sofisticado sistema para borrar sus huellas y hacer imposible rastrearlos.

No obstante lo anterior, esta serie de ataques difícilmente podría ser calificada como ciber-terrorismo, ya que más bien corresponde a un caso de espionaje informático.

3.3. Stuxnet

Este es uno de los casos más conocidos de ataques en contra de la infraestructura fundamental de un país. Stuxnet, descubierto en junio del año 2010, es un “gusano” (*worm*) que atacó una planta nuclear iraní desde el año 2009 sin ser detectado por los operadores de seguridad informática hasta un año más tarde.

Durante el año 2010, la planta nuclear afectada quedó temporalmente fuera de funcionamiento mientras se realizaban las gestiones necesarias para que pudiera operar

de manera segura. La manipulación externa de la planta a través de este virus logró desactivar las turbinas que le permitían purificar el uranio[227] y alteró el funcionamiento de los computadores de sus trabajadores.[228]

El método utilizado fue el de implantar el virus en los mecanismos de funcionamiento de la planta a través del control de la configuración de los mismos haciendo uso de un programa malicioso que afectaba a Siemens (empresa que crea los *software* de casi la totalidad de los sistemas industriales alrededor del mundo) y se aprovechaba de una falla de Windows para expandirse silenciosamente por los sistemas afectados.

Desde un comienzo, estos ataques fueron atribuidos a un Estado, ya que la complejidad del gusano utilizado y la duración del ataque involucraban necesariamente una costosa inversión de dinero.[229] En particular se acusó a Estados Unidos y a Israel de patrocinar estos ataques como una forma de prevenir la fabricación de armas nucleares en Irán.

Un tiempo después lo anterior fue confirmado gracias a la filtración a la prensa de información confidencial sobre seguridad militar estadounidense, que confirmaba la

[227] BBC News. *Iran Stuxnet leak probe: US Gen James Cartwright 'target'*. 28.06.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-23094353> [consultado: 20.08.2013].
[228] BBC News. *Stuxnet worm hits Iran nuclear plant staff omputers*. 26.07.2010. [en línea] <http://www.bbc.co.uk/news/world-middle-east-11414483> [consultado: 20.08.2013].
[229] BBC News. *Stuxnet worm 'targeted high-value Iranian assets'*. 23.07.2010. [en línea] <http://www.bbc.co.uk/news/technology-11388018> [consultado: 20.08.2013].

participación de ese país en la creación de Stuxnet y su posterior utilización en contra de Irán, en el marco de lo que se denominó "Operación Juegos Olímpicos" (*Olympic Games Operation*). [230]

El desarrollo de este gusano comenzó durante el año 2006, como una forma de implementar nuevas armas de ataque en contra de la amenaza que representan para Estados Unidos la real o supuesta carrera armamentista desarrollada por países como Irán, Corea del Norte y China. En su momento Stuxnet fue promovido por el ex presidente Bush, pero más recientemente el presidente Obama instó a implementar este tipo de ataques en el marco de la "guerra cibernética" o *cyberwarfare*.[231]

A pesar de que el uso de Stuxnet y la manipulación del funcionamiento de una planta nuclear en Irán pueden involucrar diferentes delitos informáticos y penas a quienes resulten responsables, el gobierno de Estados Unidos, por razones obvias, parece estar más preocupado de perseguir a los responsables de divulgar la información que los vinculaba con este caso que buscar las verdaderas responsabilidades involucradas en los hechos ocurridos.

[230] The Washington Post. *FBI is increasing pressure on suspects in Stuxnet inquiry*. 26.01.2013. [en línea] <http://www.washingtonpost.com/world/national-security/fbi-is-increasing-pressure-on-suspects-in-stuxnet-inquiry/2013/01/26/f475095e-6733-11e2-93e1-475791032daf_story.html> [consultado: 20.08.2013].

[231] The New York Times. *Obama Ordered Sped up Wave of cyberattacks against Iran*. 01.06.2012. [en línea] <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0> [consultado: 20.08.2013].

Sin embargo, este caso no corresponde a un evento de ciber-terrorismo puesto que, no obstante tratarse de un ataque a infraestructura fundamental de un país que pudo haber causado daños irreparables en términos de pérdida de vidas humanas, no obedece a una acción políticamente motivada que busque generar impacto en la población con el uso o amenaza de uso de la fuerza en contra de no-combatientes.

3.4. Ataques cibernéticos a Estonia

Durante el año 2007 se produjeron una serie de ataques de denegación de servicio a diferentes sitios web de Estonia.[232] En este episodio se vieron afectadas páginas del gobierno, de bancos, de colegios y otras organizaciones, causando grandes pérdidas y la alerta de los especialistas en materia de seguridad en la red.

Los hechos ocurrieron después de que el gobierno de ese país decidiera reubicar una estatua de bronce de un soldado ruso que recordaba la época de la Unión Soviética durante la Segunda Guerra Mundial. Miles de descendientes rusos se manifestaron en las calles y luego comenzaron los ataques. El gobierno ruso descartó su participación en el hecho y en el año 2008 un estudiante estonio fue condenado por delitos informáticos que involucraban técnicas de *hacking*.[233]

[232] The Washington Post. *Estonia recovers from massive denial-of-service attacks.* 17.05.2007. [en línea] <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/17/AR2007051701049.html> [consultado: 22.08.2013].
[233] The Washington Post. *Student fined for attack against Estonian Web site.* 25.01.2008. [en línea] <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012500064.html> [consultado: 23.08.2013].

Estos ataques se enmarcaron dentro de una protesta por un acto que tenía especial significación para un sector de la población estonia. Aun cuando puedan haber tenido una motivación política, no pueden asociarse con el ciber-terrorismo toda vez que no se amenazó con usar la fuerza ni se usó la misma en contra de la población civil mediante el uso de medios cibernéticos. La motivación del acto más bien apuntaba a una venganza a través de la comisión de delitos informáticos comunes.

3.5. Corea del Norte en contra de Corea del Sur

Durante el mes de marzo del año 2013 se produjeron una serie de ciber-ataques en contra de sitios surcoreanos que se atribuyeron a Corea del Norte.[234] Los hechos afectaron a 48.000 computadores y servidores, provocando el cierre de canales de televisión (KBC, MBC y YTM) y la caída de sistemas de algunos bancos (Shinhan, NongHyup y Jeju).

La responsabilidad fue atribuida a los norcoreanos debido a que varios de los programas utilizados en estos ataques se asociaban a programas utilizados anteriormente en contra de los sistemas computacionales surcoreanos. A pesar de que no hubo personas afectadas, este hecho contribuyó a aumentar la creciente tensión que se vive en la península coreana.

[234] BBC News. *South Korea blames North Korea for bank and TV cyber-attacks.* 10.04.2013. [en línea] <http://www.bbc.co.uk/news/technology-22092051> [consultado.23.08.2013].

En años anteriores Corea del Sur había sido víctima de ciber-ataques por parte de su vecino del norte. Desde el año 2009 en adelante diversos ataques cibernéticos se produjeron en contra de sistemas surcoreanos. Utilizando técnicas del *hacking*, como la denegación de servicio, se gestó el año 2010 un ataque en contra del banco NongHyup, que derivó en la imposibilidad de sus clientes de acceder a su dinero durante un periodo de tiempo.[235]

Los ataques cibernéticos de hackers norcoreanos en contra de sitios web surcoreanos corresponden a una política sostenida en el tiempo, ya que las direcciones IP utilizadas son las mismas. Sin embargo, no ha sido posible vincular al gobierno norcoreano con estas iniciativas, ni menos encontrar a los responsables de dichos ataques.

Estos casos difícilmente pueden ser considerados como ciber-terrorismo, dado que más bien corresponden a delitos informáticos comunes, como el *hacking*. Y aun cuando pudieran tener una motivación política, no existe amenaza a vidas humanas, ni tampoco se busca causar terror en la población para conseguir un cambio en las acciones de las autoridades u otros propósitos políticos o ideológicos.

[235] BBC News. *North Korea 'behind South Korean bank cyber hack'*. 03.05.2011. [en línea] <http://www.bbc.co.uk/news/world-asia-pacific-13263888> [consultado: 28.08.2013].

3.6. El curioso caso de Gary McKinnon

Gary McKinnon es un reconocido hacker británico que, durante los años 2001 y 2002, perpetró una serie de ataques en contra de los sistemas computacionales del ejército de Estados Unidos y de la NASA. Desde un comienzo McKinnon reconoció ser el autor de la intromisión en 97 computadores norteamericanos en búsqueda de información confidencial sobre los fenómenos OVNI, que él creía que había sido ocultada por las autoridades de ese país.[236]

Lo distintivo de este caso es que en rigor, McKinnon no cometió *hacking* al acceder a estos sistemas del gobierno, ya que se trataba de computadores que funcionaban con "contraseñas en blanco", es decir, no tenían contraseñas de acceso ni un sistema de seguridad muy sofisticado.[237]

El gobierno estadounidense calificó los hechos como ciber-terrorismo y buscó extraditar a McKinnon para juzgarlo por cargos que significaban al menos 60 años de presidio en una cárcel de máxima seguridad, por la aplicación de la Ley Antiterrorista.

[236] BBC News. *Clock ticking for hacker McKinnon*. 15.01.2009. [en línea] <http://news.bbc.co.uk/2/hi/uk_news/7831481.stm> [consultado: 28.08.2013].
[237] Gastón Ocampos. 10.12.2010. *1-Gary McKinnon DOCUMENTAL COMPLETO-sistemas de la NASA_1_PARTE.wmv.* [en línea]<http://www.youtube.com/watch?v=Cyq5Pn7mEC8&list=PL71349476460F64DD&index=2> [consultado: 29.08.2013].

Este hecho fue considerado como uno de los ataques de hackers más grandes de todos los tiempos y el delito fue perseguido incluso durante el gobierno de Obama.[238]

La extradición fue autorizada el año 2006 y se apeló esa decisión ante la Cámara de los Lores en el Reino Unido sin obtener resultados positivos.[239] El equipo jurídico de McKinnon llevó al caso a la Corte Europea de Derechos Humanos, puesto que los tratados de extradición entre Estados Unidos e Inglaterra lo dejaban indefenso y a merced de penas desproporcionadas en relación al daño que causó el delito imputado.

A pesar del retraso que generaron los recursos en contra de la extradición de McKinnon, no fue sino hasta el 2012 que este hombre quedó a salvo. En ese año, la Home Secretary (Ministra del Interior), Theresa May, dijo que la extradición no iba a hacerse efectiva debido a que significaba un riesgo para la vida de McKinnon en consideración a la enfermedad de Asperger que le diagnosticaron y la posibilidad cierta de que cometiera suicidio en caso de ser condenado por mucho tiempo.[240]

[238] BBC News. *Gary McKinnon: Mother urges President Obama to pardon son*. 14.12.2012. [en línea] <http://www.bbc.co.uk/news/uk-20732801> [consultado: 30.08.2013].
[239] En esa época aún no existía una Corte Suprema en el Reino Unido, que si bien fue creada en 2005, comenzó a operar en 2009.
[240] The Washington Post. *Britain deals blow to U.S. extradition treaty, blocks handover of hacker*. 16.10.2012. [en línea] <http://www.washingtonpost.com/world/europe/britain-deals-blow-to-us-extradition-treaty/2012/10/16/39c123b8-1792-11e2-a346-f24efc680b8d_story_1.html> [consultado: 28.08.2013].

Adicionalmente, el Fiscal a cargo del caso confirmó que, al menos en el Reino Unido, no se presentarían cargos en su contra por la baja probabilidad de lograr una condena.[241]

En nuestra opinión, este caso difícilmente puede ser calificado como un ataque ciber-terrorista, dado que no cumple con ninguno de los elementos del terrorismo. No existe motivación política, no busca aterrorizar a la población, ni pretende amenazar con el uso o usar la fuerza en contra de no-combatientes. A lo sumo podría calificarse como *hacking* el haber ingresado a los sistemas computacionales de agencias del gobierno y haber filtrado parte de la información.

4. ¿Y los casos de ciber-terrorismo?

Si entendemos el ciber-terrorismo como "el uso de computadores como armas de ataque u objeto del ataque, por grupos internacionales o sub-estatales, o agentes clandestinos, políticamente motivados, que hacen uso o amenazan con hacer uso de la fuerza y el miedo con el objeto de influenciar a una audiencia o provocar que un gobierno cambie sus políticas"[242], es decir, vinculando el uso de las nuevas tecnologías de información con los elementos tradicionales del terrorismo; podemos afirmar que hasta el momento no ha existido ningún ataque conocido con tales características.

[241] BBC News. *Hacker Gary McKinnon will not face UK charges.* 14.12.2012. [en línea] <http://www.bbc.co.uk/news/uk-20732804> [consultado: 28.08.2013].
[242] WILSON, Clay. Op. cit.

No obstante, los casos analizados demuestran que existe una creciente utilización de estos mecanismos con objetivos diversos (venganza, protesta, etc.), que causa daños en el "mundo real" y que sin duda es objeto de preocupación por parte de las autoridades y la comunidad internacional.

Lo anterior perfila al ciber-terrorismo como el futuro de los ataques terroristas a nivel internacional y como una suerte de potencial siguiente etapa que superaría las formas de terrorismo empleadas post 11 de septiembre de 2001 y hasta la fecha. Sin embargo, hasta que no ocurra un hecho que pueda ser calificado como ciber-terrorista sin objeciones teóricas al respecto, el periodo que estamos viviendo sólo podría calificarse como preliminar al desarrollo de estos métodos por grupos terroristas en actos terroristas propiamente tales.

En definitiva, lo que nos demuestran los casos prácticos analizados, es que la prensa ha abusado del concepto de ciber-terrorismo para generar mayor interés en determinadas noticias y que Estados Unidos tiende a referirse al tema para condenar hechos que involucran delitos informáticos que son particularmente dañinos para sus intereses políticos y económicos.

Por otra parte, los casos analizados confirman la posibilidad cierta de que pueda existir un ataque ciber-terrorista, dado que existen los medios para ello y probablemente el terrorismo esté apuntando en esa dirección. Junto con lo anterior, se pone sobre la

mesa el tema de la ciber-seguridad y la guerra cibernética, como mecanismos de resguardar los sistemas computacionales de carácter estratégico para una nación.

CAPÍTULO V

POSIBILIDAD DE REGULAR INTERNET COMO FORMA DE COMBATIR EL CIBER-TERRORISMO

1. Generalidades

Existe una manifiesta utilización de Internet para causar gran impacto en la población. Dado que esta tendencia sólo puede incrementarse en el futuro, nadie puede desconocer las potencialidades que este medio ofrece para ampliar el alcance del terrorismo en el mundo.

Como consecuencia de lo anterior, se ha generado en la comunidad internacional la necesidad de regular Internet para evitar que mediante su utilización o mediante el aprovechamiento de las deficiencias de seguridad que las nuevas tecnologías de la información presentan, se produzca un alza en las tasas de delincuencia informática, ciber-crimen y ciber-terrorismo.

La necesidad de regular plantea una serie de problemas prácticos y jurídicos relacionados con las características propias de la red. Esto se debe principalmente a que Internet es una red global; por ello, un delito cometido haciendo uso del mismo puede

involucrar diferentes jurisdicciones y afectar diferentes bienes jurídicos al mismo tiempo.

En este sentido, Rodrigo Moya señala que "[l]a potencialidad que posee la informática y la telemática de rebasar los límites de las fronteras nacionales a su vez plantea problemas de carácter jurídico. La voz, texto e imagen que viaja por Internet puede tener como origen y destino cualquier parte del mundo. Así, se plantea uno de los principales conflictos en materia de responsabilidad por acciones antijurídicas: la determinación de la legislación aplicable, la eficacia de los mecanismos de control y la efectiva aplicación de las sanciones."[243]

Además, el uso de Internet y las nuevas tecnologías de la información y las comunicaciones afectan sensiblemente el pleno ejercicio de los derechos fundamentales de los ciudadanos, toda vez que se involucran temas como la protección de datos personales y la vida privada, la libertad de expresión y el derecho a recibir información, entre otros.[244]

No obstante lo anterior, aun cuando se pueda llegar a un acuerdo respecto a los aspectos del fenómeno de Internet que pueden ser susceptibles de ser regulados, surge la discusión sobre la forma de regulación que esta red necesita y sobre la urgencia de ir

[243] MOYA GARCÍA, Rodrigo. *La Libertad de Expresión en la Red de Internet*. Revista Chilena de Derecho Informático, Ejemplar N° 2, Universidad de Chile, Facultad de Derecho, Mayo de 2003.
[244] Piénsese en los casos prácticos analizados en el capítulo anterior.

modificando constantemente el sistema de regulación escogido para que se adapte a los nuevos requerimientos que la propia realidad les va imponiendo.

2. Algunos principios y derechos que regulan Internet[245]

Como cualquier medio de comunicación masivo, Internet se rige por una serie de principios, basados en los instrumentos internacionales de derechos humanos, que regulan el comportamiento de los usuarios en la red y establecen un marco normativo general aplicable.

Sin embargo, dadas las características propias de Internet, estos principios y derechos se plasman de manera heterogénea en diferentes sitios en la web aplicando los instrumentos internacionales de derechos humanos al contexto específico que se genera en el uso de Internet.

2.1. Igualdad en el acceso

En materia de desarrollo digital uno de los principios básicos es el acceso que debe brindarse al servicio de conexión a Internet. En este sentido, la calidad de la conexión debe avanzar conforme la evolución tecnológica lo permita para hacer posible la

[245] Este apartado se basa en la "Carta de Principios y Derechos en Internet", que en ningún caso contiene una enumeración taxativa de los mismos, pero que muestra algunos lineamientos generales en la materia. [en línea] <http://internetrightsandprinciples.org/site/wp-content/uploads/2012/12/Charter-on-Human-Rights-and-Principles-on-the-Internet-Version-1-1-Draft.pdf> [consultado: 21.08.2013].

inclusión digital (v.gr. desde la conexión asociada al servicio de telefonía fija hasta la conexión inalámbrica de Wifi).

La "Carta de Principios y Derechos en Internet" establece que, para garantizar la igualdad en el acceso, debe existir, además, flexibilidad a la hora de la utilización de los diferentes *software* con que operan los programas de los computadores con protocolos inter-operables y normas abiertas[246].

En términos de inclusión digital, para que las diferencias económicas y sociales no sean un problema, los gobiernos deberán poner a disposición de la ciudadanía puntos de acceso a Internet gratuitos y, dado que la red es un bien público global, su diseño debe favorecer la equidad y la igualdad en el acceso.

2.2. No-discriminación

En Internet no se puede discriminar arbitrariamente a los usuarios que acceden a la red, por razones de género, raza o religión.[247] En la práctica, esto se manifiesta en el

[246] La interoperabilidad entre sistemas hace referencia a la capacidad de las distintas redes de comunicaciones de conectar usuarios de otras redes, de manera que las variaciones en las aplicaciones y en los servicios prestados sean tolerables. La creación de sistemas interoperables está directamente relacionada con la aprobación de normas y estándares que definan las especificaciones de implementación y los interfaces para conectar entre sí sistemas diferentes. La Organización Internacional para la Estandarización (ISO) es uno de los principales organismos internacionales que desarrollan normas y estándares, que permiten el funcionamiento uniforme de cada una de las redes que forman a su vez Internet.

[247] En este punto se reproduce lo establecido en el artículo 2 de la Declaración Universal de Derechos Humanos.

hecho de que la red permite el anonimato que garantiza el trato igualitario a todos los usuarios, que virtualmente sólo se reconocen a través del número de la conexión IP.

2.3. Libertad de expresión

El uso de Internet se asocia con el ejercicio de la libertad de expresión y de opinión que se une a los derechos de recibir y difundir información, ambos consagrados en el artículo 19 de la Declaración Universal de Derechos Humanos, entre otros instrumentos internacionales.[248]

Esta garantía es la piedra angular de la justificación de la mayoría de las manifestaciones en contra de lo que se reconoce como censura o falta de transparencia en las acciones del gobierno (v.gr. el caso de las publicaciones de información confidencial en la página de Wikileaks[249]).

2.4. Privacidad

En el artículo 12 de la Declaración de Derechos Humanos se consagra el derecho de las personas a no ser víctimas de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia.

[248] Además, la libertad de opinión y expresión se encuentra reconocida en el artículo 5 del Pacto Internacional de los Derechos Civiles y Políticos, en el artículo 10 de la Convención Europea sobre Derechos Humanos, y en el artículo 13 de la Convención Americana de Derechos Humanos.
[249] Ver capítulo IV.

Según la “Carta de Principios y Derechos en Internet” este derecho se ve protegido por las legislaciones nacionales sobre la privacidad, la facilidad para encontrar las políticas de privacidad de los servicios y la forma de configurarlos (v.gr. configuración de privacidad de Facebook), la mantención de estándares mínimos de confidencialidad e integridad de los sistemas informáticos para impedir el acceso de terceros sin el consentimiento del usuario (v.gr. claves de acceso en los servicios de correo electrónico), la protección de la personalidad virtual y el derecho al anonimato en Internet (v.gr. nombres de usuario ficticios), entre otros.

2.5. Protección de datos

En el mismo marco del punto anterior, la “Carta de Principios y Derechos en Internet” señala que el derecho a la vida privada y a la honra se resguarda en la web a través de la aplicación de normas internacionales en materia del tratamiento de datos personales. En este sentido se hace necesario que la recolección, el uso, la publicación y la retención de datos personales se realicen bajo una política transparente de privacidad.

Una forma de garantizar lo anterior es requerir el consentimiento de la persona cuyos datos se recolectan para mantenerla informada sobre el contenido, el propósito, el lugar de almacenamiento, la duración y los mecanismos de acceso a la información, para

resguardar su derecho a corregir o eliminar los datos personales entregados en cualquier momento.

3. Formas de regular Internet

Debido a que Internet está en constante cambio y es fuente permanente de nuevos proyectos y aplicaciones, la regulación del mismo ha pasado por diferentes etapas. En los años noventa primaba el sistema de auto-regulación, ya que Internet era un fenómeno reciente y existía una marcada tendencia post Guerra Fría hacia la desregulación en general.

A principios de este siglo, el Estado manifestó un interés en re-regular aquellos sectores debido a las crisis potenciales que suponía un sistema sin ningún tipo de control estatal y los peligros que generaba la ausencia de regulación para la seguridad nacional.[250] En el caso de Internet, esta crisis se reflejó en el colapso de la "burbuja punto-com" (*dot-com bubble*) entre los años 2000-2002.

A partir del año 2005 se ha mostrado una (nueva) tendencia a la co-regulación, principalmente en Europa.[251]

[250] Recordemos la conmoción que generó en Estados Unidos y en el mundo el ataque a las Torres Gemelas el 11 de septiembre de 2001.
[251] MARSDEN, Christopher T. *Internet Co-Regulation. European Law, Regulatory Governance and Legitimacy in Cyberspace.* Cambridge University Press, Reino Unido, 2011, p. 9.

3.1. Auto-regulación

Bajo este sistema un grupo de agentes o individuos detentan el control sobre su propio comportamiento. Pertenecer al grupo regulado es voluntario y los participantes diseñan sus propias reglas utilizando herramientas como códigos de conducta o soluciones y estándares técnicos frente a los problemas recurrentes. Los miembros tienen la completa responsabilidad de monitorear el cumplimiento de las reglas autoimpuestas sin responder ante ninguna autoridad regulatoria establecida.[252]

Esta fue la respuesta inicial que se dio a la problemática regulatoria que presentaba Internet en sus comienzos. Existía plena libertad para crear sitios web y muchas compañías realizaron grandes inversiones en las páginas web ".com", sin poner demasiada atención en los contenidos que se publicaban en las mismas o en el verdadero valor de las compañías asociadas a Internet.

La falta de regulación en ese mercado creó una burbuja por la especulación generada respecto al valor real de los sitios web que se multiplicaban en la red, hasta que a principios de este siglo la burbuja reventó. Los inversionistas llegaron a la conclusión de

[252] MARSDEN, Christopher T. Op. Cit., p. 54.

que Internet era sólo una herramienta y que los sitios web no tenían un valor en sí mismos, sino que en base a su contenido y su capacidad de innovación.[253]

3.2. Regulación estatal directa

Este mecanismo consiste en la aplicación de leyes especiales por parte del Estado para desarrollar una regulación particular en un sector determinado. El cumplimiento es monitoreado y mantenido por agencias o entes estatales que tienen el poder de hacer cumplir la norma.[254]

Esta fue la opción adoptada por muchos países a fines de los noventa y principios del siglo XXI, donde existió una marcada tendencia a dictar leyes especiales que regulaban el uso de Internet en algunas materias, como por ejemplo en materia penal tipificando nuevos delitos asociados al uso de Internet o en materia de propiedad intelectual y derechos de autor, creando sistemas para su protección en la red.

Dentro de este contexto se crearon organizaciones como la ICANN en Estados Unidos[255], que controla la asignación de nombres de dominio a nivel internacional y que

[253] OFEK, Eli y RICHARDSON, Matthew. *DotCom Mania: The Rise and Fall of Internet Stock Prices*. The Journal of Finance, volumen 58, 2003, pp. 1113–1138. [en línea] < http://onlinelibrary.wiley.com/doi/10.1111/1540-6261.00560/abstract> [consultado: 30.10.2013].
[254] MARSDEN, Christopher T. Op. Cit., p. 54.
[255] *Internet Corporation for Assigned Names and Numbers* o Corporación de Internet para la Asignación de Nombres y Números.

opera bajo criterios técnicos que permiten que ninguna dirección en Internet se encuentre repetida.

3.3. Co-regulación

Es la combinación de una amplia gama de fenómenos de regulación donde el régimen regulatorio se crea a partir de la interacción compleja entre la legislación general y la auto-regulación. La co-regulación permite la inclusión de diversos actores, lo que le otorga gran legitimidad.[256]

Los gobiernos han aceptado en la práctica el hecho de que Internet requiere de un tipo de regulación lo más flexible posible para permitir una mayor innovación y libertad para los usuarios. Esto supone el uso de formas de regulación tanto de *hard law* como de *soft law*.[257]

Este tipo de regulación se muestra como la opción más adecuada para el caso de Internet debido a que los diferentes actores pueden participar del proceso regulador e intervenir de manera eficiente en su desarrollo. Lo anterior permite que se pueda reaccionar oportunamente frente a las nuevas problemáticas que plantea el uso de Internet en la sociedad contemporánea.

[256] MARSDEN, Christopher T. Op. Cit., p. 46.
[257] Ibíd., p. 48.

Como ejemplo de la adopción de este modelo de regulación se encuentra el hecho de que la ICANN se haya transformado en una organización no gubernamental, sin fines de lucro que ya no depende del gobierno norteamericano.

Otro ejemplo es la formación de la INHOPE (*International Association of Internet Hotlines*) en Europa, cuya función es operar una línea telefónica de carácter público que se utiliza para denunciar anónimamente y sacar de Internet contenidos ilícitos relacionados con la pornografía infantil.[258]

Diversos tipos de organizaciones ciudadanas trabajan en cooperación con agencias gubernamentales para mantener el buen funcionamiento de Internet en base a los principios y derechos bajo los cuales opera la red de redes, en estricta observancia de las convenciones internacionales sobre derechos humanos.

4. Seguridad en el ciber-espacio y guerra cibernética

Junto con la elección de la técnica de regulación más adecuada para Internet, surge la problemática asociada a la forma de mejorar la seguridad en el ciber-espacio para prevenir el ciber-terrorismo y los delitos informáticos en general.

A partir del 11 de septiembre de 2001, bajo el gobierno del Presidente Geoge W. Bush, comenzó a gestarse en EE.UU. una retorcida forma de abordar el problema del

[258] Ver detalles de la organización en www.inhope.org

terrorismo mundial, declarándole la guerra al mismo y justificando diversas violaciones de los derechos humanos en base a la supuesta defensa de la seguridad nacional, amparadas por las autoridades políticas de ese país.[259]

En materia de ciber-terrorismo, en EE.UU. se ha trazado un camino paralelo en la forma en que se enfrenta el problema de seguridad. En ese país se planteó la existencia de una ciber-guerra (*cyber-warfare*), se alertó sobre las amenazas (reales o ficticias) del ciber-terrorismo[260] y se ha creado un peligroso clima de desinformación entre los ciudadanos. [261]

Hoy en día, el concepto de ciber-guerra fue reemplazado por el de guerra de la información (*netwar*, *info-war*), como un esfuerzo por no demonizar el uso de las redes cibernéticas y una forma de no repetir los errores que se cometieron al enfrentar el terrorismo tradicional, ya que en el ciber-espacio el ejercicio de algunos derechos y libertades también podrían verse seriamente afectados con las prácticas de los Estados en la búsqueda por combatir el ciber-terrorismo.

Un caso que refleja el esfuerzo de los gobiernos por anticiparse a estas nuevas amenazas que presenta la tecnología fue la noticia sobre el programa de vigilancia de la

[259] CERVENAK, Christine. *Lecciones de El Lado Tenebroso: las moralejas de la historia de la guerra de EE.UU. contra el terrorismo.* Anuario de Derechos Humanos, Nº 5, 2009, p. 208 y ss. [en línea] <http://www.anuariocdh.uchile.cl/index.php/ADH/article/viewArticle/11529/11888> [consultado: 13.09.2012].
[260] Un claro ejemplo es la obra de Dan Verton y los términos en que aborda la problemática.
[261] ENGHELBERG, Hedi. *Ciberterrorimo 2010-2110*. Editorial ENG, Segunda Edición, 2010.

National Security Agency (Agencia de Seguridad Nacional) de Estados Unidos, que incluía la escucha telefónica, la lectura de correos electrónicos y la recolección de información que circulaba en Google y Facebook.

Esta información fue filtrada por primera vez por Edward Snowden y causó gran conmoción, ya que no sólo involucraba a las comunicaciones de los norteamericanos, sino que existía una recopilación de información a nivel internacional y de manera transversal (no sólo se vigilaba la comisión de posibles delitos vinculados al terrorismo, sino que se almacenaba información sobre el uso de los medios tecnológicos de todo tipo de ciudadanos).[262]

El método de espionaje que utilizaba esta agencia del gobierno norteamericano se basaba en el uso de un programa computacional llamado "Prism" que operaba a través de la recolección de todo tipo de información transmitida mediante cables de fibra óptica (que es el medio de transmisión de datos por excelencia en la actualidad), lo que le permitió acceder a millones de comunicaciones diariamente a lo largo de un par de años.

Lo anterior demuestra la importancia que ha alcanzado la información transmitida a través de las nuevas tecnologías, y a su vez, la necesidad de poner ciertos límites al uso de las mismas por parte de los gobiernos, puesto que este tipo de intervenciones es una

[262] BBC News. *Edward Snowden: Leaks that exposed US spy programme*. 25.10.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-23123964> [consultado: 31.10.2013].

clara violación de derechos fundamentales referidos principalmente a la inviolabilidad de las comunicaciones.

CONCLUSIONES

Los medios de comunicación de masas han sido utilizados históricamente para causar gran impacto en la población, pero en la sociedad contemporánea pueden convertirse en verdaderas armas de ataque. El uso de Internet asociado al ciber-terrorismo es un claro ejemplo de esta situación.

Usualmente se utiliza el concepto de ciber-terrorismo para calificar hechos que causan gran impacto en la población, pero que en realidad corresponden a delitos informáticos comunes, como el *hacking*.

La gran cantidad de definiciones existentes del concepto da cuenta de la dificultad de delimitar los elementos propios que distinguen a este fenómeno de otros actos similares. Es necesario tomar en consideración los elementos que definen el terrorismo tradicional para construir un concepto de ciber-terrorismo más preciso.

A pesar de que, en rigor, no existen casos prácticos comprobados que podamos calificar como ciber-terrorismo, la posibilidad de su ocurrencia hace años que dejó de ser ciencia ficción. Las herramientas que otorgan Internet y las tecnologías cibernéticas

permiten inferir que con algo de conocimiento sobre el funcionamiento de los sistemas informáticos es posible realizar un ataque terrorista de gran magnitud.

En este sentido, la amenaza del ciber-terrorismo se vincula directamente con la capacidad que tiene el uso de las tecnologías cibernéticas de expandir los efectos del terrorismo tradicional, dado que Internet no es un fin en sí mismo, sino que un mero instrumento que puede ser utilizado para diferentes fines.

Sin duda, este desarrollo es objeto de alarma por parte de los ciudadanos y las autoridades, por lo que se han buscado diferentes formas de regular el uso de Internet con el objeto de prevenir el mal uso de la red de redes, principalmente en la comisión de delitos informáticos.

Lo anterior permite afirmar la posibilidad de que estemos siendo testigos de la formación de nuevas técnicas de ataque terrorista a nivel internacional que con el paso del tiempo van a perfeccionarse hasta concluir en la creación de una nueva etapa del terrorismo, marcada por un hito como lo fue en su momento el ataque a las Torres Gemelas en Estados Unidos.

Frente a esta contingencia, surge la difícil tarea de elegir un método de regulación de Internet. La flexibilidad y cambio permanente que presenta este medio hace que las formas de regulación también deban adaptarse de manera constante. En este sentido, la

respuesta oportuna del legislador debe ir acompañada de la asesoría técnica correspondiente y de la inclusión en este debate de organizaciones de internautas que participan activamente en la construcción de un Internet más seguro.

Finalmente, se hace necesario recalcar que el hecho de que el ciber-terrorismo sea una amenaza real a la seguridad de los Estados y que pueda tener consecuencias potencialmente devastadoras para sus ciudadanos, no es una excusa para que los gobiernos atenten contra garantías fundamentales en la persecución del mismo. Sobre todo si todavía estamos hablando de respuestas pre-emptivas a la problemática.

BIBLIOGRAFÍA

a) LIBROS, ARTÍCULOS E INFORMES

ABRAMS, Marshall y WEISS, Joe. *Malicious Control System Cyber Security Attack Case Study- Maroochy Water Services, Autralia*. 23.07.2008. [en línea] < http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf> [consultado: 12.08.2013].

ALANDETE, David. Coto al poder de Google. El País. 25.06.2009. [en línea] <http://elpais.com/diario/2009/06/25/sociedad/1245880801_850215.html> [consultado: 31.03.2013].

BARBIER, Frédéric y BERTO LAVENIR, Catherine. *Historia de los medios: de Diderot a Internet.* Ediciones Colihue, Buenos Aires 2007.

BELLAMY, Alex. *Guerras Justas. De Cicerón a Irak*. Fondo de Cultura Económica, Buenos Aires, 2009.

BRIGGS, Asa y BURKE, Peter. *De Gutenberg a Internet. Una historia social de los medios de comunicación.* Editorial Taurus, Madrid, 2002.

CABEZAS Logan, P. y MOYA Muñoz, F. (2008).*El Derecho al anonimato del usuario de internet*. Disponible en: <http://tesis.uchile.cl/handle/2250/107854> [consultado: 19.03.2013].

CANEDO ANDALIA, Rubén. *Aproximaciones para una historia de Internet*. *ACIMED*. 2004, vol.12, n.1 [en línea] http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000100005&lng=es&nrm=iso [consultado: 18.02.2013].

CANTRIL, Hadly. *The Invasion from Mars: A study in the psychology of panic*. Princeton University Press, Washington, 2009.

CASERMEIRO, Alicia. *Surgimiento, desarrollo y adopción de los principales medios masivos de comunicación*. 1993.

CERVENAK, Christine. *Lecciones de El Lado Tenebroso: las moralejas de la historia de la guerra de EE.UU. contra el terrorismo.* Anuario de Derechos Humanos, Nº 5, 2009, p. 208 y ss. [en línea]

<http://www.anuariocdh.uchile.cl/index.php/ADH/article/viewArticle/11529/11888> [consultado: 13.09.2012].
COMER, Douglas. *Internetworking with TCP/IP. Principles, protocols and architectures.* Cuarta Edición, Prentice Hall, New Jersey, 2000.

Comisión Interamericana de Derechos Humanos. Informe sobre terrorismo y Derechos Humanos. 2002. [en línea] < http://www.cidh.org/Terrorism/Span/resumen.htm> [consultado: 13.09.2012].

COX, Simon. *Anonymous, hacktivism and the rise of cyber protesters*. BBC News. 26.11.2012. [en línea] <http://www.bbc.co.uk/news/technology-20446048> [consultado: 31.03.2013].

DAVEL. *Harbor to Harbour.* 04.09.2012. [en línea] <http://harbor2harbour.com/?p=144> [consultado: 12.08.2013].

DENNING, Dorothy. *Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy.* En ARQUILLA, John y RONFELDT, David. Networks and Netwars: The Future of Terror, Crime, and Militancy. Editorial RAND, Estados Unidos, 2001, p. 241. [en línea] <http://books.google.cl/books?hl=es&lr=&id=VKFMTDnapl4C&oi=fnd&pg=PA239&dq=activism,+hacktivism+and+cyberterrorism&ots=jEeGN5QkHe&sig=l8uRBWbpwhMsWC1LbFesgVlZ28&redir_esc=y#v=onepage&q=activism%2C%20hacktivism%20and%20cyberterrorism&f=false> [consultado: 22.09.2012].

_____. Declaración hecha el 23 de Mayo de 2000 en una audiencia frente al Congreso de EE.UU. en el marco de la discusión de un panel de expertos sobre las Amenazas Terroristas para los Estados Unidos. [en línea] <http://www.fas.org/irp/congress/2000_hr/00-05-23denning.htm> [consultado: 28.08.2012].

DIZARD, Wilson. *Old Media/ New Media: Mass communication in the information age*. Longman, Nueva York, 1994.

ELLISON, Nicole, STEINFIELD, Charles y LAMPE, Cliff. *The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites.* Journal of Computer-Mediated Communication, Volumen 12, Tema 4, Julio 2007, pp. 1143-1168. [en línea] <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00367.x/full> [consultado: 10.03.2013].

ENGHELBERG, Hedi. *Ciberterrorimo 2010-2110*. Editorial ENG, Segunda Edición, 2010.

FAUS, Ángel. *La era audiovisual. Historia de los primeros cien años de la radio y la televisión*. Ediciones Internacionales Universitarias, Barcelona, 1995.

FILDES, Johnathan. *Stuxnet virus target and spread revealed*. BBC News. 2011. [en línea] <http://www.bbc.co.uk/news/technology-12465688 > [consultado: 27.03.2013].

FLEMMING, Peter y STOHL, Michael. *Myths and Realities of Cyberterrorism.* Paper preparado para la International Conference on Countering Terrorism Through Enhanced International Cooperation, 22-24 de Septiembre de 2000, Courmayeur, Italia.

FOLKERTS, Jean; LACY, Stephen y LARABEE, Ann. *The Media in your life. An Introduction to Mass Communication*. Pearson Education, Inc., Cuarta Edición, Estados Unidos, 2008.

GARCÍA, Pablo. *Principios de Derecho de Internet*. Tirant Lo Blanch, Segunda Edición, Valencia, 2005.

GONZÁLEZ RUS, Juan José. *"Los ilícitos en la red (I): hackers, crackers cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes"*. En ROMEO CASABONA, Carlos María y Otros. *El Cibercrimen: Nuevos retos jurídico-penales. Nuevos desafíos político-criminales.* Editorial Comares, Granada, 2006.

HALL, Kevin. *The 7 worst cyberattacks in history (that we know about)*. 22.07.2010. [en línea] <http://www.dvice.com/archives/2010/09/7_of_the_most_d.php> [consultado: 14.08.2013].

HOBSBAWN, Eric. *Historia del siglo XX*. Traducción de Juan Faci, Jordi Ainaud y Carme Castells, Editorial CRÍTICA (Grijalbo Mondadori, S.A.), Buenos Aires.

JAIN, Gaurav. *Cyber Terrorism: A Clear and Present Danger to Civilized Society?* Information Systems Education Journal, Volume 3, Number 44, August 12, 2005, p. 3. [en línea] <http://isedj.org/3/44/> [consultado: 31.08.2012].

KOCH, Howard. *La emisión del pánico*. Centro de Creación Experimental, Cuenca, 2002.

KRASAVIN, Serge. *What is Cyber-terrorism?*. Computer Crime Reseasrch Center (CCRC). [en línea] <http://www.crime-research.org/library/Cyber-terrorism.htm>. [consultado: 28.08.2012].

LAQUEUR, Walter. *Una historia del terrorismo.* Editorial Paidós, Buenos Aires, 2003.

LEWIS, James. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. En Center for Strategic and International Studies (CSIS), December 2002.

LORDOÑO MARTÍNEZ, Fernando. *Los delitos informáticos en el proyecto de reforma en actual trámite legislativo*. No. 4 (2004): Revista de Derecho Informático, 2004, p. 172-174. [en línea] <http://www.boletinfilologia.uchile.cl/index.php/RCHDI/article/viewPDFInterstitial/10679/10959> [consultado: 20.09.2012].

MARSDEN, Christopher T. *Internet Co-Regulation. European Law, Regulatory Governance and Legitimacy in Cyberspace.* Cambridge University Press, Reino Unido, 2011

MARSHALL, John. *Method and system for file blocking in an electronic messaging system.* 2000. [en línea] <http://www.google.com/patents?hl=es&lr=&vid=USPAT7017187&id=lzN4AAAAEBAJ&oi=fnd&dq=i+love+you+worm&printsec=abstract#v=onepage&q=i%20love%20you%20worm&f=false> [consultado: 27.03.2013].

MCQUAIL, Denis. *La acción de los medios.* Amorrortu Editores, Buenos Aires, 1998.

MOYA GARCÍA, Rodrigo. *La Libertad de Expresión en la Red de Internet*. Revista Chilena de Derecho Informático, Ejemplar N° 2, Universidad de Chile, Facultad de Derecho, Mayo de 2003

_____. *La Libertad de Expresión en la Red de Internet.* Separata para el curso de Derecho Informático, Primer Semestre, 2005.

OFEK, Eli y RICHARDSON, Matthew. *DotCom Mania: The Rise and Fall of Internet Stock Prices*. The Journal of Finance, volumen 58, 2003, pp. 1113–1138. [en línea] < http://onlinelibrary.wiley.com/doi/10.1111/1540-6261.00560/abstract> [consultado: 30.10.2013].

O'GUINN, Thomas, ALLEN, Chris y SEMENIK, Richard. *Publicidad y comunicación integral de marca.* Thompson Editores, 4ª Edición, México, 2006.

OLSZEWSKI, Anthony. *Internet War waged against Hal Turner, Hudson County hate monger and FBI informant.* 07.04.2010. En Hudson County Facts. [en línea] < http://hudsoncountyfacts.com/hudsoncounty/?p=1165> [consultado: 06.08.2013].

OVALLE, José Ignacio. *Derecho de las Telecomunicaciones*. Santiago, 2010.

RENIZ, Doris. *La información en tiempos de guerra y terrorismo*. En: Revista Javeriana (Ago. 2002). p. 39-55. [en línea] < http://hdl.handle.net/10720/524> [consultado: 25.12.2012].

ROMEO CASABONA, Carlos María. *"De los delitos informáticos al cibercrimen. Una aproximación conceptual y político- criminal."* En ROMEO CASABONA, Carlos María y Otros. *El Cibercrimen: Nuevos retos jurídico-penales. Nuevos desafíos político-criminales.* Editorial Comares, Granada, 2006.

SÁNCHEZ, Gema. *Ciberterrorismo. La guerra del siglo XXI*. Revista El Viejo Topo, Nº 242, 2008, p. 23. [en línea] <http://dialnet.unirioja.es/servlet/articulo?codigo=2542384> [consultado: 28.08.2012].

SLOBBE, J. y VERBERKT, S.L.C. *Hacktivists: Cyberterrorists or Online Activists?* An Exploration of the Digital Right to Assembly. 2012, p. 5. [en línea] <http://arxiv.org/abs/1208.4568> [consultado: 02.09.2012].

STOHL, Michael. *Old myths, new fantasies and the enduring realities of terrorism*. Critical Studies of Terrorism, Vol. 1, No. 1, April, 2008.

STREET, John. *Mass Media, Politics and Democracy*. PALGRAVE, Nueva York, 2001.

SUAZO VEJARES, Sótero ; MARTÍNEZ ORTIZ, Javier ; ELGUETA RUIZ, Álvaro Patricio. *Redes sociales como herramientas de ciberactivismo: el caso de los grupos de Facebook en Chile y el Gran Concepción (2009)*. En Ecos de la Comunicación, Año 4, Nº 4, 2011, p. 155. [en línea] <http://bibliotecadigital.uca.edu.ar/repositorio/revistas/redes-sociales-como-herramientas- ciberactivismo.pdf > [consultado: 24.09.2012].

SUBIJANA, Ignacio. *El ciberterrorismo: Una perspectiva legal y judicial*. Revista ENGUZKILORE, Número 22, San Sebastián, Diciembre 2008.

Twitter. *Twitter turn six*. 21.03.2012. [en línea] <https://blog.twitter.com/2012/twitter-turns-six> [consultado: 23.09.2013].

VERTON, Dan. *Black Ice: La amenaza invisible del ciberterrorismo*. Editorial Mc Graw- Hill/ Interamericana de España, Madrid, 2004.

WARD, Mark. *A decade on from the ILOVEYOU bug*. BBC News. 2010 <http://www.bbc.co.uk/news/10095957> [consultado: 27.03.2013].

WEIMANN, Gabriel. *Cyberterrorism. How real is the threat?* United States Institute of Peace (USIP), Special Report Nº 119, 2004

WEINSTOCK, Jeffrey. *Mars attacks! Well, Welles, and radio panic: or, the story of the century*. En BROWNE, Ray y NEIL, Arthur. Ordinary Reactions to Extraordinary Events, Bowling Green State University Popular Press, 2001.

WILSON, Clay. *Computer Attack and Cyberterrorism: Vulnerabilities and Policy issues for Congress.* En LINDEN, Edward L. Focus on Terrorism, Vol 9, Nova Science Publishers, Inc., 2007.

YAR, Majir. *Cybercrime and Society*. SAGE Publications Ltd, Londres, 2006, p. 48. [en línea] <http://books.google.cl/books?id=LyNEk9y9GOUC&pg=PA48&lpg=PA48&dq=virtual+sitin&source=bl&ots=J1WCpktPp&sig=mNtF7rXEDAnNVfYKtSAEH4innSE&hl=es&sa=X&ei=kW1gUJ3pGqu_0QG1goHgBA&ved=0CEEQ6AEwAw#v=onepage&q=virtual%20sit-in&f=false> [consultado: 24.09.2012].

ZALAQUETT, José. *Chile ratifica la Convención Interamericana contra el Terrorismo*. En No. 2 (2006): Anuario de Derechos Humanos, 2006, p. 181. [en línea] <http://www.anuariocdh.uchile.cl/>

b) TEXTOS NORMATIVOS Y DOCUMENTOS OFICIALES

Nacionales

Ley N° 18.168. Ley General de Telecomunicaciones. Publicada en el Diario Oficial de 27 de Febrero de 1987.

Ley N° 19.223 que tipifica figuras penales relativas a la informática. Publicada en el Diario Oficial de 7 de Junio de 1993.

Internacionales

Convención Americana sobre Derechos Humanos.

Convención Europea de Derechos Humanos.

Convención Interamericana contra el Terrorismo de 2002.

Convención Internacional Contra la Toma de Rehenes de 1979.

Convención sobre la Protección Física de Materiales Nucleares de 1980.

Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear de 2005.

Convenio Internacional para la Represión de Actos Terroristas Cometidos con Bombas de 1997.

Convenio Internacional para la Represión de la Financiación del Terrorismo de 1999.

Convenio para la Represión del Apoderamiento Ilícito de Aeronaves de 1970.

Declaración Universal de Derechos Humanos.

Pacto Internacional de Derechos Civiles y Políticos.

c) NOTICIAS

24 Horas. Las *increíbles cifras de lo que sucede en internet en un minuto*. 21.03.2013. [en línea] <http://www.24horas.cl/tendencias/mundodigital/las-increibles-cifras-de-lo-que-sucede-en-internet-en-un-minuto-568982> [consultado: 21.03.2013].

BBC News. *Bradley Manning sentenced to 35 years in Wikileaks case.* 21.08.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-23784288> [consultado: 25.08.2013].

_____. *Bradley Manning supporters stage UK events.* 23.02.2013. [en línea] <http://www.bbc.co.uk/news/uk-21556107 > [consultado: 31.03.2013].

_____. *Clock ticking for hacker McKinnon*. 15.01.2009. [en línea] <http://news.bbc.co.uk/2/hi/uk_news/7831481.stm> [consultado: 28.08.2013].

_____. *Data of Sun website users stolen.* 02.08.2011. [en línea] <http://www.bbc.co.uk/news/technology-14371738> [consultado: 06.08.2013].

_____. *Diplomatic leaks 'more embarrassment than damage'*. 29.11.2010. [en línea] <http://news.bbc.co.uk/today/hi/today/newsid_9237000/9237029.stm> [consultado: 10.08.2013].

_____. *Edward Snowden: Leaks that exposed US spy programme*. 25.10.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-23123964> [consultado: 31.10.2013].

_____. *Edward Snowden says he is NSA Prism leak source in interview*. 09.06.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-22836419> [consultado: 11.08.2013].

_____. *Gary McKinnon: Mother urges President Obama to pardon son*. 14.12.2012. [en línea] <http://www.bbc.co.uk/news/uk-20732801> [consultado: 30.08.2013].

_____. *Griffin says leaked BNP list fake*. 20.10.2009. [en línea] <http://news.bbc.co.uk/2/hi/uk_news/politics/8315928.stm> [consultado: 10.08.2013].

_____. *Hacker Gary McKinnon will not face UK charges*. 14.12.2012. [en línea] <http://www.bbc.co.uk/news/uk-20732804> [consultado: 28.08.2013].

_____. *Inside PayPal's high-tech control room*. 18.12.2010. [en línea] <http://www.bbc.co.uk/news/technology-12018487> [consultado: 06.08.2013].

_____. *Iran Stuxnet leak probe: US Gen James Cartwright 'target'*. 28.06.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-23094353> [consultado: 20.08.2013].

_____. *Julian Assange: Wikileaks to release 'million more files in 2013'*. 20.12.2012. [en línea] <http://www.bbc.co.uk/news/uk-20806355> [consultado: 31.03.2013].

_____. *Leaks expose UK and US fears over Pakistan nuclear arms*. 30.11.2010. [en línea] <http://www.bbc.co.uk/news/world-us-canada-11883230> [consultado: 10.08.2013].

_____. *LulzSec hacker group handed jail sentences*. 16.05.2013. [en línea] < http://www.bbc.co.uk/news/technology-22552753> [consultado: 06.08.2013].

_____. *North Korea 'behind South Korean bank cyber hack'*. 03.05.2011. [en línea] <http://www.bbc.co.uk/news/world-asia-pacific-13263888> [consultado: 28.08.2013].

_____. *Palin's e-mail account plundered.* 18.09.2008. [en línea] <http://news.bbc.co.uk/2/hi/technology/7622724.stm> [consultado: 09.08.2013].

_____. *Profile: Edward Snowden*. 07.08.2013. [en línea] <http://www.bbc.co.uk/news/world-us-canada-22837100> [consultado: 11.08.2013].

_____. *Pro-Wikileaks activist abandon Amazon cyber attack*. 09.12.2010. [en línea] <http://www.bbc.co.uk/news/technology-11957367> [consultado: 06.08.2013].

_____. *Snowden affair puts Wikileaks back into spotlight.* 28.06.2013. [en línea] <http://www.bbc.co.uk/news/world-latin-america-23077279> [consultado: 11.08.2013].

_____. *Stuxnet worm hits Iran nuclear plant staff omputers*. 26.07.2010. [en línea] <http://www.bbc.co.uk/news/world-middle-east-11414483> [consultado: 20.08.2013].

_____. *Stuxnet worm 'targeted high-value Iranian assets'*. 23.07.2010. [en línea] <http://www.bbc.co.uk/news/technology-11388018> [consultado: 20.08.2013].

_____. *Soca website taken down after LulzSec 'DDoS attack'*. 20.06.2011. [en línea] <http://www.bbc.co.uk/news/technology-13848510> [consultado: 06.08.2013].

_____. *South Korea blames North Korea for bank and TV cyber-attacks.* 10.04.2013. [en línea] <http://www.bbc.co.uk/news/technology-22092051> [consultado.23.08.2013].

_____. *Timeline: sexual allegations against Assange in Sweden*. 16.08.2012. [en línea] <http://www.bbc.co.uk/news/world-europe-11949341> [consultado: 10.08.2013].

_____. *US embassy cables: The background*. 29.11.2010. [en línea] <http://www.bbc.co.uk/news/world-us-canada-11862320> [consultado: 10.08.2013].

_____. *US prepares first-strike cyber-forces.* 12.10.2012 [en línea] <http://www.bbc.co.uk/news/technology-19922421 > [consultado: 31.03.2013].

_____. *Whistle-blower site taken offline*. 18.02.2008. [en línea] <http://news.bbc.co.uk/2/hi/technology/7250916.stm> [consultado: 09.08.2013].

_____. *Who stands to gain from Wikileaks?* 13.03.2007. [en línea] <http://news.bbc.co.uk/2/hi/technology/6443437.stm> [consultado: 08.08.2013].

_____. *Wikileaks release of embassy cables reveals US concerns.* 28.11.2010. [en línea] <http://www.bbc.co.uk/news/world-us-canada-11858895> [consultado: 10.08.2013].

Fox News. A Brief History of the LulzSec Hackers. 21.06.2011. [en línea] < http://www.foxnews.com/tech/2011/06/21/brief-history-lulzsec-hackers/> [consultado: 06.08.2013].

La Tercera. *Día de la Tierra: Anonymous ataca sitios web en protesta por el proyecto Alto Maipo*. 22.04.2013. [en línea] <http://www.latercera.com/noticia/tendencias/2013/04/659-519968-9-dia-de-la-tierra-anonymous-ataca-sitios-web-en-protesta-por-el-proyecto-alto.shtml> [consultado: 05.08.2013].

Noticias Montreal. *Grupo de hackers LulzSec anuncia el fin de sus operaciones*. 26.06.2011. [en línea] <http://noticiasmontreal.com/4795/grupo-de-hackers-lulzsec-anuncia-el-fin-de-sus-operaciones/> [consultado: 06.08.2013].

_____. *Una nueva víctima de los hackers: el gobierno de Brasil*. 22.06.2011. [en línea] <http://noticiasmontreal.com/4789/una-nueva-victima-de-los-hackers-el-gobierno-de-brasil/> [consultado: 06.08.2013].

The guardian. *Twitter heads for stock market debut by filing for IPO*. 13.09.2013. [en línea] < http://www.theguardian.com/technology/2013/sep/12/twitter-ipo-stock-market-launch?CMP=EMCNEWEML6619I2&et_cid=48826&et_rid=7107573&Linkid=http%3a%2f%2fwww.theguardian.com%2ftechnology%2f2013%2fsep%2f12%2ftwitter-ipo-stock-market-launch> [consultado: 23.09.2013].

The New York Times. *Obama Ordered Sped up Wave of cyberattacks against Iran*. 01.06.2012. [en línea] <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0> [consultado: 20.08.2013].

The Washington Post. *Britain deals blow to U.S. extradition treaty, blocks handover of hacker*. 16.10.2012. [en línea] <http://www.washingtonpost.com/world/europe/britain-deals-blow-to-us-extradition-treaty/2012/10/16/39c123b8-1792-11e2-a346-f24efc680b8d_story_1.html> [consultado: 28.08.2013].

_____. *CIA Web site hacked; group LulzSec takes credit.* 16.06.2011. [en línea] <http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html> [consultado: 06.08.2013].

_____. *Estonia recovers from massive denial-of-service attacks*. 17.05.2007. [en línea] <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/17/AR2007051701049.html> [consultado: 22.08.2013].

_____. *FBI is increasing pressure on suspects in Stuxnet inquiry*. 26.01.2013. [en línea] <http://www.washingtonpost.com/world/national-security/fbi-is-increasing-pressure-on-suspects-in-stuxnet-inquiry/2013/01/26/f475095e-6733-11e2-93e1-475791032daf_story.html> [consultado: 20.08.2013].

_____. *LulzSec to release Sony data this afternoon.* 02.06.2011. [en línea] <http://www.washingtonpost.com/blogs/post-tech/post/lulzsec-to-release-sony-data-this-afternoon/2011/06/02/AGOD1JHH_blog.html> [consultado: 06.08.2013].

_____. *Name and faces: PBS website hacked.* 30.05.2011. [en línea] <http://www.washingtonpost.com/blogs/reliable-source/post/names-and-faces-pbs-website-hacked-christopher-knight-and-adrianne-curry-separate/2011/05/30/AGoVlwEH_blog.html> [consultado: 06.08.2013].

_____. *Student fined for attack against Estonian Web site.* 25.01.2008. [en línea] <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012500064.html> [consultado: 23.08.2013].

d) SITIOS DE INTERÉS EN INTERNET

Asociación para la Investigación de Medios de Comunicación. En: <http://www.aimc.es/>

Comisión Interamericana de Derechos Humanos. En: <http://www.oas.org/es/cidh/>

Comité contra el Terrorismo del Consejo de Seguridad de la ONU. En: <http://www.un.org/es/sc/ctc/>

Computer Crime Research Center. En: <http://www.crime-research.org/library/Cyber-terrorism.htm>

International Association of Internet Hotlines. En: <http://www.inhope.org/gns/home.aspx>

Internet Corporation for Assigned Names and Numbers. En: <http://www.icann.org/>

Internet Rights and Principles Coalition. En: <http://internetrightsandprinciples.org/site/>

Naciones Unidas. En: <http://www.un.org/es/index.shtml>

NIC Chile. En: <http://www.nic.cl/>

Observatorio para la Cibersociedad. En: <http://www.cibersociedad.net/>

United Nations Office on Drugs and Crime. En: <https://www.unodc.org/>

United States Holocaust Memorial Museum. En: <http://www.ushmm.org/>

WikiLeaks. En: <http://www.wikileaks.org/>

e) VIDEOS

Aleteuk. (17/01/2008). *Tom Cruise Scientology Video - (Original UNCUT)*. [en línea] <http://www.youtube.com/watch?v=UFBZ_uAbxS0> [consultado: 05.06.2013].

Church0fScientology. (01/02/2008). *Code of Conduct*. [en línea] Disponible en <http://www.youtube.com/watch?v=-063clxiB8I> [consultado: 05.06.2013].

Church0fScientology. (21/01/2008). *Message to Scientology*. [en línea] <http://www.youtube.com/watch?v=JCbKv9yiLiQ> [consultado: 05.06.2013].

Gastón Ocampos. 10.12.2010. *1-Gary McKinnon DOCUMENTAL COMPLETO-sistemas de la NASA_1_PARTE.wmv.* [en línea]<http://www.youtube.com/watch?v=Cyq5Pn7mEC8&list=PL71349476460F64DD&index=2> [consultado: 29.08.2013].

PRABHJEET, Kaptaan (27.02.2013) *How Hackers Changed the World - BBC documentary 2013*. [en línea] <http://www.youtube.com/watch?v=Rj35GguOAGE> [consultado: 05.06.2013].