Ciberseguridad en Venezuela y su impacto en las redes sociales: protección vs. violación de derechos*

Gladys Rodríguez**

SUMARIO: I. Introducción. II. Algunas consideraciones previas. III. Clases de ataques y atacantes en las redes sociales virtuales. 1. Ataques. 2. Tipos de atacantes. 3. Iniciativas internacionales humanitarias frente a estas categorías de ataques y atacantes IV. Redes sociales y ciberseguridad en Venezuela. 1. Marco legal relativo a la libertad de expresión e información. 2. Impacto de la ciberseguridad en el entorno digital en Venezuela. V. Algunas consideraciones finales.

Resumen

El presente artículo expone el impacto que implica la ciberseguridad de la información en Venezuela, con especial referencia a las redes sociales virtuales. Se analiza la providencia administrativa 01/09 de fecha 22 de diciembre de 2009 de la Comisión Nacional de Telecomunicaciones (CONATEL) y los informes anuales 2009 y 2013 del Programa Venezolano Educación-Acción en Derechos Humanos (PROVEA), sobre "Derecho a la libertad de expresión e información", concluyendo que los intentos de dominación y control del ciberespacio menoscaban los derechos de los ciudadanos a la libertad de expresión, derecho a la información, secreto a las comunicaciones y su inviolabilidad.

Palabras Clave: Ciberseguridad. Redes sociales virtuales. Venezuela. Derechos de los ciudadanos.

Recibido: 11/8/2014 • Aceptado: 12/9/2014

* Este trabajo ha sido realizado en el marco del proyecto de Investigación intitulado: Regulación de la ciberseguridad de la información en el Estado venezolano: avances y desafíos en las redes sociales virtuales, financiado por el Consejo de Desarrollo Científico y Humanístico adscrito al Vicerrectorado Académico de la Universidad del Zulia.

** Abogada. Magister en Planificación y Gerencia de Ciencia y Tecnología, Doctora en Derecho. Postdoctora en Gerencia en las Organizaciones. Profesora Titular de la Universidad del Zulia. Investigadora adscrita al Instituto de Filosofía del Derecho de la Facultad de Ciencias Jurídicas y Políticas de L.U.Z.

Abstract

This paper presents the impact of cybersecurity of information in Venezuela, with special reference to social networks. The administrative ruling 01/09 dated December 22, 2009 of the National Commission Telecomunicacione (CONATEL), and annual reports 2009 and 2013 from Venezuelan Program Education-Action in Human Rights (PROVEA) on "Right to Freedom of Speech and Information" are analyzed, concluding that attempts to dominate and control of cyberspace, impair the rights of citizens to freedom of speech, right to information, communications secrecy and inviolability.

Key words: Cybersecurity. Social Networks. Venezuela. Citizens' rights.

I. Introducción

El presente trabajo reflexiona cualitativamente sobre la base de una investigación documental que expone el impacto que implica la ciberseguridad de la información en Venezuela, con especial referencia a las redes sociales virtuales. Se parte de la revisión de varios autores. De igual modo es objeto de referencia la providencia administrativa 01/09 de fecha 22 de diciembre de 2009 de la Comisión Nacional de Telecomunicaciones (CONATEL) (sustituida por la actual providencia administrativa N° 027, publicada en la Gaceta Oficial N° 40.415, de 20 de mayo de 2014)[1], y los informes anuales 2009 y 2013 del Programa Venezolano Educación-Acción en Derechos Humanos (PROVEA), sobre "Derecho a la libertad de expresión e información". Un primer aspecto a abordar es precisar conceptualmente algunos términos que se usaron a lo largo de la investigación, seguidamente se describen los principales ataques y atacantes en el entorno de las redes sociales virtuales, así como las iniciativas internacionales para enfrentar este fenómeno. Finalmente se explica la relación: redes sociales virtuales y ciberseguridad en Venezuela, destacándose el marco legal y el impacto que la ciberseguridad ha significado en el ámbito digital. Se concluye que los intentos de dominación y control del ciberespacio menoscaban la libertad de expresión, el derecho a la información, el secreto a las comunicaciones y su inviolabilidad, entre otros derechos y, son efectuados tanto por *totalitarios*, como por sedicentes democracias, en ambos extremos se tienen

1 Esta providencia contiene la actual Norma Técnica sobre los Servicios de Producción Nacional Audiovisual y otros Servicios de Producción Audiovisual y deja sin efecto el instrumento legal de 2009. Siguiendo el objeto de la investigación, se hace referencia a la norma de 2009 en el entendido que los hechos que se analizan ocurrieron bajo la vigencia de la norma derogada, aunque en el trabajo se hará una breve referencia comparativa entre ambas providencias y el impacto de la nueva "Norma Técnica" en materia de libertad de expresión.

como ejemplos por un lado: China, Arabia Saudita, entre otros y, por el otro: a los países *Echelon*[2].

II. Algunas consideraciones previas

En el marco de esta investigación, resulta oportuno precisar algunos conceptos básicos tales como: Internet o ciberespacio, ciberseguridad, computación en la nube y redes sociales virtuales. En atención a ello, Internet la define Joyanes (1997: 79)[3] como *"una red mundial de computadoras que permite la comunicación directa y transparente, compartiendo información y servicios a lo largo del mundo…"*. Por su parte, Boizard (1996: 1)[4] argumentan que *"la Internet es como la red de computadoras más grande del mundo, que conecta cientos de redes, permitiendo la comunicación de personas con distintos lugares o países y una posterior transferencia de información (documentos) a distancia"*. Así también, Internet permite que el concepto de comunicación que contiene en su definición la palabra –distancia– fuente básica de concepción de la realidad no represente una limitación, incorporándose a un modelo vecinal, por lo que sumergirse en ésta conlleva sorprenderse de la capacidad ilimitada que se adquiere de adentrarse en otros mundos. Estas definiciones se acercan a la idea de una sociedad interconectada, donde la red de redes, que se conoce como Internet, da paso a un escenario hoy denominado ciberespacio. Por ello, resulta conveniente agregar la definición del Diccionario de la Real Academia Española (DRAE) en su 22ª edición[5], el cual define ciberespacio, con una única acepción, como el *"Ámbito artificial creado por medios informáticos"*. En realidad, se entiende que la RAE se está refiriendo a un entorno no físico creado por un equipo informático con el objetivo de interoperar en una Red. En consecuencia, el mayor ámbito del ciberespacio es Internet.

El término fue utilizado por primera vez en la obra Neuromante del escritor norteamericano William Gibson y publicada en el emblemático 1984 que presagia Orwell. También podríamos definir el ciberespacio desde su perspectiva original como un conjunto o realidad virtual donde se agrupan usuarios, páginas web, chat y demás servicios de Internet además de otras redes. En definitiva el

2 Se considera que ECHELON, que pasó de un sistema de control contra la ex URSS a un sistema global de espionaje, controla el 90% de las comunicaciones en el ámbito global. Involucra a fieles aliados de Estados Unidos de América, léase: Australia, Nueva Zelanda, Canadá y Gran Bretaña en el marco del acuerdo UKUSA (conocido también como proyecto cinco ojos y que se remonta a la segunda guerra mundial) cuyo propósito principal era compartir información de inteligencia. Jofré, P (2013) **Echelon: Espionaje global** En: http://radio.uchile.cl/2013/09/13/echelon-espionaje-global consultado 4 de agosto de 2014)

3 JOYANES, L. (1997) *Cibersociedad: los retos sociales ante un nuevo mundo digital*. Editorial McGraw-Hill, Interamericana de España. p.155

4 BOIZARD, A. (1996) *Internet en acción*. México: Editorial McGraw-Hill. P. 237

5 www.rae.es (Consulta: 2014, julio, 30)

ciberespacio es, como apunta Joyanes (2011:30)[6], *"El espacio donde se navega por Internet, se realizan conversaciones por Skype o en las redes sociales, o estamos cuando consultamos el correo electrónico, chateamos o visitamos un periódico digital"*.

No obstante, los evidentes beneficios que resultan de tal combinación de realidad y virtualidad, el autor Castells (2003: 159)[7]:

> …defiende la idea que la expansión de Internet está conduciendo hacia un aislamiento social y una ruptura de la comunicación social y la vida familiar, porque los individuos se refugian en el anonimato y practican una sociabilidad aleatoria, abandonando la interacción personal cara a cara en espacios reales.

En consecuencia, se ha acusado a Internet de incitar gradualmente a la gente a vivir sus propias fantasías *on line* y huir del mundo real, en una cultura cada vez más dominada por la realidad virtual (Olivares, Vera y Durante, 2010)[8]. Ello ha significado ver el otro lado, quizás no tan positivo del fenómeno tecnológico en su interacción con el ser humano, y de allí que algunos como el propio Castells (1999)[9], se apunten por la idea de regular la Internet, concluyendo:

> Internet, en nuestro tiempo, necesita libertad para desplegar su extraordinario potencial de comunicación y de creatividad. Asimismo, la libertad de expresión y de comunicación ha encontrado en Internet su soporte material adecuado. Pero tanto Internet, como la libertad, sólo pueden vivir en las mentes y en los corazones de una sociedad libre, libre para todos, que modele sus instituciones políticas a imagen y semejanza de su práctica de libertad.

Por su parte, Castro (2003: 16)[10] afirma:

> La aplicación del derecho a Internet se fundamenta en el debate entre la defensa de la autonomía, privacidad y anonimato del usuario individual, y por otra parte la preocupación por el derecho de empresa a la libre actuación en Internet y a la defensa de la seguridad colectiva, aun si ésta implica un menoscabo de la seguridad individual.

6 JOYANES, L (2011). "Introducción. El estado del arte de la Ciberseguridad". *Ciberseguridad. Retos y Amenazas a la seguridad nacional en el ciberespacio*. Cuadernos de Estrategia. Grupo No. 03/10. Ministerio de Defensa. Instituto español de estudios estratégicos. Instituto Universitario "General Gutiérrez Mellado". Febrero, 2011

7 Castell, M. (2003). *La Galaxia Internet.* Primera Edición. Barcelona: Editorial Debolsillo.

8 OLIVARES, VERA y Durante 2010. "Sociedad de la información: Regulación del tejido de redes". *En: Revista Espacio Abierto*. Vol 19, No. 1 enero –marzo, 2010, pp. 137-147.

9 CASTELL, M. (1999) *La era de la Información: Economía, sociedad y cultura***.** Vol 1. La sociedad red. Madrid: Alianza Editorial.

10 CASTRO, A (2003). La regulación de Internet: un reto jurídico**.** Disponible: http://www.uned.ac.cr/redti/documentos/regulacion.pdf. (Consulta 2008, abril 08)

Como se puede observar, se trata de dos primeros significados –Internet y ciberespacio– íntimamente relacionados entre sí y con la propuesta de una regulación.

De igual manera, otro significado a exponer, es la ciberseguridad, a criterio particular de la autora, la ciberseguridad es un conjunto de estrategias tanto técnicas, militares, políticas y jurídicas que permiten evitar que principalmente los Estados y las organizaciones, públicas y privadas sean objeto de daño, amenazas y acciones terroristas a sus instalaciones físicas y de telecomunicaciones en su mayoría de carácter estratégico, para la defensa y seguridad del Estado o la organización mismo, empleando para ello sistemas sofisticados de virus, software y cualquier tecnología maliciosa.

Frente a potenciales amenazas, desde hace varios años, los Estados se han preocupado por mantener bajo sistemas de seguridad sus bienes, servicios y ciudadanos. De ello han surgido varios mecanismos de espionaje por parte de los Estados, uno de los casos ejemplificantes es la organización multinacional de escuchas UKUSA, creada por varios tratados secretos de posguerra entre Estados Unidos de América y Gran Bretaña, se llama hoy a sí misma los Cinco Ojos. Las agencias que forman parte de ella compiten por ver quién tiene más penetración en las comunicaciones privadas y comerciales a través de Internet. Los Cinco Ojos son los servicios de inteligencia de señales (SIGINT) de los Estados Unidos de América, el Reino Unido, Canadá, Australia y Nueva Zelanda. Engloban la Agencia de Seguridad Nacional estadounidense (NSA) y el Cuartel General de Comunicaciones del Gobierno Británico (GCHQ). En los documentos se encuentran numerosos comentarios informales que demuestran que la mayor satisfacción, para los agentes de los servicios de inteligencia, es vigilar todo, franquear el mayor número posible de sistemas de privacidad y, hoy es lo que se conoce como países Echelon. (Campbell, D 2013.)[11]

En este sentido, Venezuela ha venido denunciando, a través de la Comisión Nacional de Telecomunicaciones (CONATEL), una amenaza de ciberguerra, especialmente, si resulta aprobada la Ley S.2148[12] por parte del Congreso de los Estados Unidos de América. *"El estatuto tiene como escenario la instalación de posibles bases para la emisión de señales radioeléctricas, lo que podría crear una posible invasión de dicho espacio en Venezuela*

11 CAMPBELL, D (2013.) Bajo la vigilancia de los cinco ojos. http://internacional.elpais.com/internacional/2013/07/05/actualidad/1373038892_139217.html (Consulta 2014, agosto, 04)

12 Esta ley legaliza la ciberguerra contra Venezuela y coartaría el acceso libre a internet en el país, lo que le permitiría a los Estados Unidos desarrollar estrategias mediáticas en el aspecto radioeléctrico y tener acceso a la distribución de contenidos", dijo durante su participación el Presidente de CONATEL, en el programa "Temprano Con", que transmite el Sistema Radio Mundial. En: Correo del Orinoco (2014) Director de CONATEL: Ley S.2148 legaliza la ciberguerra contra Venezuela. En www.aporrea.org. (Consulta: 2014, agosto, 04)

tal y como ha ocurrido en Cuba, Irak y Siria, aseguró su Presidente". (Correo del Orinoco. 2014)[13].

En consecuencia, Venezuela al igual que el resto del mundo, ve amenazados sus intereses y en el caso particular, Venezuela ha creado un comando cibernético para enfrentar las situaciones de amenazas, entre otras estrategias a las que se harán referencia más adelante. El problema no es crear estrategias de seguridad y, en especial de ciberseguridad por parte de los Estados o las organizaciones, sino cuando estos mecanismos de protección frente a posibles amenazas y, en este caso, ciberguerras o ciberamenazas trascienden los límites y se cometen abusos o se impide el ejercicio de algún derecho a los ciudadanos.

La realidad es que existen cientos de software maliciosos como el *malware*, que atentan contra la seguridad de un terminal y, hoy evolucionan de los computadores de escritorio hacia los móviles, donde las redes sociales son un caldo de cultivo perfecto para acceder de manera maliciosa. Es entendible: acceder a un dispositivo móvil desde, por ejemplo, una red *wi-fi* desconocida, la cual puede ser la puerta de entrada perfecta para algún ansioso. Y el fin es el mismo: provocar daño o recoger datos personales "a la mala". Una de las regiones más propensas a caer en estas trampas virtuales es Latinoamérica.

La razón es sencilla, según explica Dmitry Bestuzhev[14], encargado de la región por parte de la empresa de Kaspersky Lab.. *"El mayor problema de los latinos es que son demasiado sociales. Esa región es más confiada y cálida con sus contactos. Sospechan menos, o puede ser que haya más ingenuidad por parte de los usuarios"*. El blanco de los creadores de *malware* apunta principalmente al Cono Sur, específicamente a cuentas bancarias. Otro riesgo es el denominado *phishing* (correos fraudulentos que se hacen pasar por casas comerciales o bancarias para obtener datos) y, que es altísimamente común. Porque saben que en esta región los usuarios son más curiosos a la hora que les llega un *link*, ya sea vía *Facebook* o a través de un mensaje directo en *Twitter*. Agrega Bestuzhev,

> …la amenaza tampoco deja afuera a los videojuegos, en aquellos multijugadores, donde uno se puede encontrar virtualmente con cualquier persona en el mundo, las posibilidades de acceder a un *link* o código virulento son altas. Por otro lado, también está el tema de las monedas virtuales (como *Bitcoin*) y los bienes en juegos de rol (como el *World of Warcraft*) que son vendidos en el mercado negro virtual por dinero real. Eso técnicamente también es un crimen, por el no pago de impuestos.

13 Correo del Orinoco. 2014. *Director de CONATEL: Ley S.2148 legaliza la ciberguerra contra Venezuela.* www.aporrea.org. (Consulta: 2014, agosto, 04)

14 Revista Qué pasa (Chile): La ciberseguridad de Mr. K.http://www.quepasa.cl/articulo/tecnologia/2013/08/23-12457-9-tecnologia (Consulta 2014, abril, 03)

Estos aspectos de ciberseguridad se retomarán más adelante. Continuando con las consideraciones previas, otro concepto empleado en el entorno digital recién es la computación en la nube. La nube o en inglés *Cloud Computing:* Es el conjunto "infinito" de servidores de información (computadores) desplegados en centros de datos, a lo largo de todo el mundo donde se almacenan millones de aplicaciones web y enormes cantidades de datos (*big data*), a disposición de miles de organizaciones y empresas, y cientos de miles de usuarios que se descargan y ejecutan directamente los programas y aplicaciones de software almacenados en dichos servidores tales como *Google Maps, Gmail, Facebook, Tuenti o Flickr*. La nube está propiciando una nueva revolución industrial soportada en las nuevas fábricas de "datos" (Centros de Datos, *Data Centers*) y de "aplicaciones web (*Web Apps*). (Joyanes, 2011)[15].

Existen organismos internacionales, uno de estos organismos más reconocido es el *National Institute of Standards and Technology (NIST*)[16], señala que el modelo de la nube se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue. La nube en sí misma, es un conjunto de *hardware* y *software*, almacenamiento, servicios e interfaces que facilitan la entrada de la información como un servicio. Los servicios de la nube incluyen el software, infraestructura y almacenamiento en Internet, bien como componentes independientes o como una plataforma completa –basada en la demanda del usuario–. Los modelos de entrega y despliegue de servicios en la nube más usuales que se ofrecen a los clientes y usuarios de la nube (organizaciones, empresas y usuarios) son: PaaS (*Platform as a Service*), plataforma como servicio, IaaS *(Infrastructure as a Service*), infraestructura como servicio y SaaS (*Software as a Service*), software como servicio.

Finalmente, en estas consideraciones previas el constructo referente a las redes sociales virtuales, es necesario abordarlo. Desde el ámbito jurídico, en Venezuela no hay una definición legal sobre qué entender por redes sociales. Sin embargo, el Grupo de Trabajo sobre Protección de Datos del artículo 29 de la Directiva 95/46/CE de protección de datos, de fecha 12 de junio de 2009, en su Dictamen 5/2009 sobre redes sociales en línea, define a éstas como: *"plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes…"*

Por su parte, Gil indica (2012:219)[17]:

15 JOYANES, L (2011). *Introducción. El estado del arte de la Ciberseguridad*…. op.cit.p.13 y ss

16 El NIST es una Agencia del Departamento de Comercio de los Estados Unidos de América. Dentro del NIST, el *Computer Security Resource Center* (CSRC) se encarga de los estándares de las Tecnologías de la Información y, en concreto, de *Cloud Computing.*

17 GIL, A (2012) "El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales" En *Revista de Derecho UNED*, No. 10, 2012, pp. 209-255

> …se puede definir en forma genérica, una red social *on line* como aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través de Internet para que estos generen un perfil con sus datos personales facilitando la creación de redes con base a criterios comunes y permitiendo la conexión de unos usuarios con otros y su interacción.

En definitiva se tiene que las redes sociales virtuales (RSV en adelante), independientemente de la tipología a la que pertenezcan, comparten un conjunto de características. Estas características comunes incluyen un fácil acceso, con conexión rápida y dinámica de los usuarios que forman parte de la RSV, la compartición de todo tipo de información entre los usuarios de la RSV, la difusión viral a través de sus usuarios y los riesgos a los que se ven expuestos los usuarios. Nos quedaremos con este último concepto. Los usuarios de las RSV están expuestos a un conjunto de amenazas y riesgos que, en mayor o menor medida, pueden afectar a su seguridad. En la actualidad, las RSV basadas en perfiles son la topología de RSV que exponen a sus usuarios a un mayor número de amenazas y riesgos[18]. Esto se debe, fundamentalmente, a que se trata de la topología que solicita y maneja mayor cantidad de datos de carácter personal[19]. Acciones tan cotidianas, dentro de una RSV, como publicar datos de carácter personal, enviar mensajes privados, publicar fotos, etiquetar amigos, descargar aplicaciones, etc. llevan asociados un conjunto de amenazas y riesgos contra nuestra privacidad y, por ende, contra la propia ciberseguridad en su conjunto.

III. Clases de ataques y atacantes en las redes sociales virtuales

1. Ataques

Según Caro (2011)[20], los ataques surgen al mismo tiempo que las Tecnologías de la Información, en estas tecnologías no sólo se engloban los ordenadores sino cualquier dispositivo electrónico, como es el caso de los teléfonos móviles, las agendas electrónicas, GPS, las tabletas electrónicas, etc., así como las comunicaciones. Estos ataques pueden afectar a cualquier nivel: ciudadanos,

18 La perspectiva interna del negocio abarca todos los procesos relacionados con la gestión de la seguridad de la plataforma que da soporte a la RSV como la seguridad lógica, el control de accesos, la continuidad del servicio, la gestión de incidencias, el cifrado de las comunicaciones, el *hacking* ético, los permisos sobre el contenido publicado, etc.

19 Por último, la perspectiva financiera incluye todas las cuestiones relacionadas con el comercio electrónico y las plataformas de pago de las RSV

20 CARO, M (2011) "Alcance y ámbito de la seguridad nacional en el Ciberespacio. *Ciberseguridad. Retos y Amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia*. Grupo No. 03/10. *Cap. II*. Ministerio de Defensa. Instituto español de estudios estratégicos. Instituto Universitario "General Gutiérrez Mellado". Febrero, 2011. pp. 49-82

empresas, administración, infraestructuras críticas, sector bancario, etc. Se habla incluso de amenazas avanzadas[21].

La mayoría de los ataques se aprovechan de vulnerabilidades de los sistemas informáticos, agujeros de seguridad que surgen de una deficiente programación que no tiene en cuenta la seguridad en el ciclo de vida del desarrollo del software y los diversos protocolos de comunicación.

Con el tiempo muchos protocolos fueron avanzando hacia versiones más seguras, por ejemplo Telnet y SSL, http y https, ftp y sftp, etc. Un caso especial son las redes sociales cuya falta de seguridad afecta a la ciudadanía, en particular a los menores, que en ocasiones son objeto de la llamada ingeniería social y acaban siendo víctimas de acoso sexual, o revelación de información personal.

Algunos de los tipos de ataques más conocidos y cuya definición figura en una de las guías del Centro Criptológico Nacional (CCN) y en sus siglas en inglés *Computer Emergency Response Team* (CERT). En este caso CCN-CERT del gobierno español[22] son:

- Virus: programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.
- Código dañino, también conocido como código malicioso, maligno o "malware" en su acepción inglesa: software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial[23].
- Bomba lógica: segmento de un programa que comprueba constantemente el cumplimiento de alguna condición lógica (por ejemplo, número de accesos a una parte del disco) o temporal (satisfacción de una cierta fecha). Cuando ello ocurre, desencadenan alguna acción no autorizada. En ocasiones, si la condición a verificar es una cierta fecha, la bomba se denomina temporal.
- Troyano: programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc.
- Gusano: es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana

21 Aunque las "amenazas avanzadas" cada vez son más numerosas y difíciles de detectar, las organizaciones carecen de medios, tecnología y personal para abordarlas. Este es el principal hallazgo del estudio "*Growing Risk of Advanced Threats*" realizado por el Instituto Ponemon, para cuya elaboración encuestó a 591 trabajadores del ámbito de las TIC's y de la seguridad, asentados en los EEUU. Este informe define "amenaza avanzada" como "*una metodología empleada para evadir las medidas de protección de una compañía, con el fin de desencadenar una variedad de ataques con un objetivo concreto"*

22 Guía de seguridad de la Seguridad de las Tecnologías de Información (STIC) de la serie de Manuales del (CCN-STIC-401), Glosario y abreviaturas, 1 de febrero de 2010.

2. Tipos de atacantes

Los atacantes se pueden clasificar atendiendo a su motivación: como puede ser la búsqueda de un cambio social o político, un beneficio económico, político o militar, o satisfacer el propio ego; su objetivo: ya sean individuos, empresas, gobiernos, infraestructuras, sistemas y datos de tecnologías de la información, ya sean públicos o privados; el método empleado: código dañino, virus, gusanos, troyanos, etc.

Atendiendo a su autoría se pueden clasificar en:

- **Ataques patrocinados por Estados**: los conflictos del mundo físico o real tienen su continuación en el mundo virtual del ciberespacio. En los últimos años se han detectado ciberataques contra las infraestructuras críticas de países o contra objetivos muy concretos, pero igualmente estratégicos. El ejemplo más conocido es el ataque a parte del ciberespacio de Estonia en 2007, que supuso la inutilización temporal de muchas de las infraestructuras críticas del país báltico o los ciberataques sufridos por las redes clasificadas del gobierno estadounidense a manos de atacantes con base en territorio chino o el último ataque reconocido por Irán a los sistemas informáticos de decenas de industrias que fueron atacados por un virus antes de este verano[24] y del que Irán dice haberse recuperado[25]. Aquí también puede incluirse el espionaje industrial.
- **Servicios de inteligencia y contrainteligencia**: empleados por los Estados para realizar operación de información. Suelen disponer de bastantes medios tecnológicos y avanzados.
- **Terrorismo, extremismo político e ideológico**: los terroristas y grupos extremistas utilizan el ciberespacio para planificar sus acciones, publicitarlas y reclutar adeptos para ejecutarlas, así como herramienta de financiación. Estos grupos ya han reconocido la importancia estratégica y táctica del ciberespacio para sus intereses.
- **Ataques de delincuencia organizada**: las bandas de delincuencia organizada han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que éste ofrece. Este tipo de bandas tienen como

23 En el informe de inteligencia de seguridad aparece España entre los países con más infecciones por malware del mundo detrás de Corea del Sur con 12,4 infecciones por cada 1.000 computadoras escaneadas). *Battling Botnets for Control of Computers*. SIR -Microsoft Security Intelligence Report, volume 9, January through June 2010

24 El Mundo: Irán reconoce un ataque informático masivo por el gusano Stuxnet contra sus sistemas industriales. Artículo publicado en la edición digital del diario El Mundo. Enlace http://www.elmundo.es/elmundo/2010/09/27/navegante/1285571297.html. (consulta: 27.9.2010)

25 *Revista Atenea*: Irán dice haber limpiado todos los ordenadores infectados por virus Stuxnet. http://www.revistatenea.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_3060_ESP.asp. (Consulta: 4.10.2010)

objetivo la obtención de información sensible para su posterior uso fraudulento y conseguir grandes beneficios económicos[26].

• **Ataques de perfil bajo.** Este tipo de ataques son ejecutados, normalmente, por personas con conocimientos en Tecnologías de Información y Comunicación (TIC) que les permiten llevar a cabo ciberataques de naturaleza muy heterogénea y por motivación, fundamentalmente, personal.

En perfecta armonía con lo planeado, debe ser considerado el tema de los delitos. En el caso de Venezuela y quizás coincidiendo con otros Estados, se tiene, entre los más relevantes:

- Delitos contra la intimidad: delitos contra la intimidad y el derecho a la propia imagen (arts. 60 Constitución Nacional, en concordancia con la Ley especial contra Delitos Informáticos, Capítulo III, relativo a los delitos contra la privacidad de las personas y de las Comunicaciones). Asimismo, la ley expone el delito de pornografía y prostitución infantil con el uso de las TIC. (arts. 23 y 24).
- Delitos contra la propiedad: hurtos (art.13), fraude (art. 14) obtención indebida de bienes y servicios (art. 15), manejo fraudulento de tarjetas inteligentes e instrumentos análogos (art.16), delitos relativos a la propiedad intelectual (art.25), delitos relativos al mercado y a los consumidores (Capítulo V, relativo a los delitos contra el orden económico).
- Otras referencias indirectas: en relación con la utilización de medios o instrumentos informáticos, cabe señalar: Ley Orgánica de Telecomunicaciones, Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos. Ley sobre protección a la privacidad de las comunicaciones, entre las más afines a la problemática.

3. Iniciativas internacionales humanitarias frente a estas categorías de ataques y atacantes

Igualmente, desde una perspectiva humanitaria afirman Cossío, Martínez, Nuñez, Cesteros, Liñero, Becana y Martín (2013)[27]; es indudable que estas actuaciones, a las que se hizo referencia producen un daño indiscriminado, y son perseguidas porque pueden ser utilizadas en el curso de un conflicto bélico.

26 Según datos del *Federal Bureau of Investigation* (FBI), en 2009 el impacto de la ciberdelincuencia por la acción de bandas organizadas ocasionó unas pérdidas, tanto a empresas como a particulares estadounidenses, por un valor superior a 560 millones de dólares.

27 Cossío, Martínez, Nuñez, Cesteros, Liñero, Becana y Martín (2013) "Ciberseguridad: El nuevo reto del Siglo XXI". *Aspectos económicos de la ciberseguridad*. Grupo No. 1. 30 de mayo de 2013.Centro Superior de Estudios de la Defensa Nacional. (CESEDEN). España.

El Comité Internacional de la Cruz Roja, (en adelante, CICR)[28], ha abordado la cuestión de las amenazas cibernéticas en numerosos documentos. Entre ellos cabe mencionar el que contempla las cuestiones jurídicas que se plantean ante la posibilidad de que se conduzcan hostilidades en el ciberespacio.

En este sentido y de un análisis de los principios generales sobre "empleo de las armas", y a la luz de las normas 70 y 71 de la Compilación del Derecho Internacional Humanitario Consuetudinario se examinará su aplicación a los ciberataques.

La norma 70, establece que "*queda prohibido el empleo de medios y métodos de guerra de tal índole que causen males superfluos o sufrimientos innecesarios*".

En cuanto a los supuestos de ataque cibernético, con efectos económicos, en la mayoría de los casos tienen una duración limitada en el tiempo y pasado el momento de la agresión sus efectos no permanecen, es decir, no producen un efecto de devastación permanente. Puede decirse que si quedan constatados, entrarían dentro del concepto de "daño o destrucción", pues en todo caso producen perjuicios de carácter moral en la población.

Dada la definición que el propio Comité Internacional de la Cruz Roja ofrece sobre los medios y métodos de guerra de tal índole que causen males superfluos o sufrimientos innecesarios, nada impediría la aplicación de esta norma a aquellos ataques que, utilizando la red, fueran lanzados en un contexto como el señalado.

La norma 71 establece que "*queda prohibido el empleo de armas de tal índole que sus efectos sean indiscriminados*".

El Informe del CICR emitido tras la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, "El derecho internacional humanitario (DIH en adelante) y los desafíos de los conflictos armados contemporáneos", aclara que en el supuesto de que se propagara un virus o una serie de virus en los sistemas informáticos de un determinado Estado, elegido como objetivo, el DIH sería aplicable.

A juicio del Comité, no cabe duda de que estos virus podrían considerarse ataques indiscriminados de conformidad con el DIH vigente, toda vez que no pueden dirigirse contra un objetivo militar concreto y, por lo tanto, tendrían la consideración de un medio o método de combate cuyos efectos no pueden ser limitados, tal como lo exige el DIH.

Una cuestión particular que surge y que requiere atenta reflexión es si en la práctica es posible anticipar totalmente las consecuencias o los efectos secundarios que un ataque dirigido contra un objetivo militar legítimo pueda tener en la población civil y los objetos de carácter civil.

A juicio del CIRC, en este caso es necesario, igualmente respetar los principios de distinción y proporcionalidad lo que, a su vez, implica que es indispensable

28 Comité Internacional de la Cruz Roja. (CICR) Compilación del Derecho Internacional Humanitario. Consuetudinario. Norma 70 y 71.

tomar algunas precauciones en el ataque. Ello incluye la obligación de que el autor del ataque tome todas las precauciones factibles al seleccionar los medios y métodos de ataque con miras a evitar y, en cualquier caso a reducir al mínimo las víctimas y los daños civiles incidentales. Concluye el mencionado Informe que, puesto que en determinados casos las operaciones cibernéticas podrían causar un número menor de víctimas civiles incidentales y menos daños civiles incidentales, en comparación con los que ocasionan las armas convencionales, en ese caso y en tales circunstancias esta norma requeriría que un Alto Mando considerara la posibilidad de lograr la misma ventaja militar utilizando un medio y método de guerra que recurra al uso de la tecnología cibernética, en caso de que pudiera ponerse en práctica.

Otro esfuerzo en el ámbito internacional es el Convenio sobre Ciberdelincuencia[29], aprobado y abierto a la firma por el Plenario del Consejo de Ministros en Budapest, el 23 de noviembre de 2001. Este Convenio pretende armonizar la legislación de los diversos países que lo ratifiquen, no sólo en materia de derecho penal sustantivo, sino también de derecho procesal para hacer frente a ese tipo de delincuencia. El Convenio define los delitos informáticos agrupándolos en cuatro grupos:

a) ***Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos***. Engloba las conductas de acceso ilícito, interceptación ilícita, interferencia de datos, interferencia de sistemas y el abuso de dispositivos.

b) ***Delitos por su contenido***. Comprende las conductas que se engloban en los delitos relacionados con la tenencia y distribución de contenidos de pornografía infantil en la Red.

c) ***Delitos relacionados con la informática***. Se definen dos tipos penales, la falsificación informática y el fraude informático.

d) ***Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines***. En este grupo, el Convenio hace una remisión normativa a los tratados y convenios internacionales sobre propiedad intelectual. En un Protocolo adicional al Convenio, de enero de 2003, se incluyeron las conductas de apología del racismo y la xenofobia a través de Internet, como delitos de contenido.

29 Consejo de Europa. Serie de Tratados Europeos No. 185. Convenio sobre Ciberdelincuencia, Budapest 23.XI.2001. El Convenio, hasta la fecha, sólo ha sido firmado por 46 países y ratificado por 30 estados firmantes. Se puede ver la lista actualizada de los países firmantes y los que lo han ratificado en http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=29/ (Consulta 2014, julio, 30)

Como puede observarse, es un catálogo de sucesos que pueden escenificarse en la red y hoy cuenta con la calificación de delitos y, por tanto ser objeto de sanción.

Salom (2013)[30], señala que la importancia del Convenio no está tanto en el número de países que lo han firmado y ratificado sino en que se ha constituido en el referente internacional a la hora de hablar de la delincuencia informática, y de aproximarnos a una legislación global.

En definitiva, los primeros escenarios de la delincuencia organizada se focalizaban en el fraude en el comercio electrónico y en la banca electrónica, como instrumentos más rápidos para obtener beneficios. Pero hoy, esas acciones delictivas pueden abarcar temas como la privacidad y la intimidad, configurando uno de los atentados mayores a los derechos humanos.

IV. Redes sociales y ciberseguridad en Venezuela

De acuerdo con los aspectos antes descritos en materia de ciberseguridad se observará el reto frente a la tensión que generan estas medidas a los derechos de los ciudadanos, algunos autores, en la materia entre ellos, Suñé (2013)[31] señala que en los tiempos actuales, en los que la sociedad se debate sobre los derechos y libertades de las personas en un mundo cada vez más global y estructurado con base a las nuevas tecnologías, se hace imprescindible que el mundo del Derecho haga su aportación en defensa de los mismos.

1. Marco legal relativo a la libertad de expresión e información

En el caso de Venezuela se puede decir que existe un marco legal encaminado a otorgar un orden a la actividad que se desarrolla por Internet, pero que peligrosamente debe mantener un equilibrio y proporcionalidad entre el derecho de los ciudadanos a estar informados y expresarse y el derecho del Estado a mantener en secreto algunas comunicaciones o regular de manera excesiva con base a algunas atribuciones. A continuación, se hará referencia a los documentos legales en la materia y con especial referencia a las telecomunicaciones y redes sociales, a saber:

30 SALOM (2011) "El Ciberespacio y el crimen organizado". *Ciberseguridad. Retos y Amenazas a la seguridad nacional en el ciberespacio Cuadernos de Estrategia.* Grupo No. 03/ 10.*Cap. III*. Ministerio de Defensa. Instituto español de estudios estratégicos. Instituto Universitario "General Gutiérrez Mellado". Febrero, 2011, pp.131-164

31 SUÑÉ, LLINAS, E (2013) "Hacia una Declaración de Derechos del Ciberespacio". http:/ /oiprodat.com/2013/06/24/hacia-una-declaracion-de-derechos-del-ciberespacio/ (Consulta 2014, julio, 30)

a) Constitución Nacional[32]

La máxima norma del país, consagra en su art. 48 el derecho al secreto e inviolabilidad de las comunicaciones. El art. 57 de la Carta Magna, consagra el derecho a la libertad de expresión y, el art. 58 establece el derecho a la información.

b) Ley Orgánica de Telecomunicaciones[33]

Esta ley tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, a *fin de garantizar el derecho humano de las personas a la comunicación* y a la realización de la actividad económica de telecomunicaciones necesarias para lograrlo, sin más limitaciones que las derivadas de la Constitución y las leyes…. (Art. 1) La ley también contempla en su art. 11 en concordancia con el art. 35, la creación de una Comisión Nacional de Telecomunicaciones[34], hoy CONATEL. En su Título II De los Derechos y Deberes de los Usuarios y Operadores, Capítulo I, contempla los derechos y deberes de los usuarios (Art. 12) y en su Capítulo II los derechos y deberes de los operadores (Art. 14). En su Título VI De los Recursos Limitados, Capítulo II Del Procedimiento para la Concesión de Uso y Explotación del Espectro Radioeléctrico (Arts. 76 al 78), serán estos los artículos a los que haremos alusión más adelante.

c) Ley de Responsabilidad social en Radio, Televisión y Medios electrónicos[35]

Esta ley tiene por objeto establecer, en la difusión y recepción de mensajes, la *responsabilidad social de los prestadores de los servicios de radio y*

32 Asamblea Nacional Constituyente. Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria No. 5453. Caracas, 24 de marzo de 2000.

33 Comisión Legislativa Nacional Ley Orgánica de Telecomunicaciones. Gaceta Oficial No. 36.970, 12 de junio de 2000. Ediciones Babosan, C.A.

34 La Comisión Nacional de Telecomunicaciones (CONATEL), es un instituto autónomo, dotado de personalidad jurídica y patrimonio propio e independiente del Fisco Nacional, con autonomía técnica, financiera, organizativa y administrativa (Art. 35 de la Ley Orgánica de Telecomunicaciones). CONATEL es el organismo del Estado venezolano que ejerce la regulación, supervisión y control sobre las telecomunicaciones. La Ley Orgánica de Telecomunicaciones, promulgada el 12 de junio de 2000, otorgó las competencias estatales para la regulación del sector a CONATEL. Esta Comisión, inicialmente fue creada mediante el Decreto Nº 1.826 del 5 de septiembre de 1991 (Gaceta Oficial Nº 34.801 de fecha 18 de septiembre del mismo año) atribuyéndosele el carácter de servicio autónomo sin personalidad jurídica, y la jerarquía de una Dirección General del Ministerio de Transporte y Comunicaciones. Reemplazo al Consejo Nacional de Telecomunicaciones (CNT)

35 Asamblea Nacional. Ley de Responsabilidad social en radio, televisión y medios electrónicos. Gaceta Oficial 39579 de fecha 22 de diciembre de 2010.

televisión, proveedores de medios electrónicos, los anunciantes, los productores y productoras nacionales independientes y los usuarios y usuarias, *para fomentar* el equilibrio democrático entre sus deberes, derechos e intereses *a los fines de promover la justicia social y de contribuir a ….los derechos humanos,…."* Entre sus objetivos, el artículo 3, los refiere y en particular el objetivo 2 señala*: "Garantizar el respeto a la libertad de expresión e información, sin censura, dentro de los límites propios de un Estado Democrático y Social de Derecho y de Justicia y con las responsabilidades que acarrea el ejercicio de dicha libertad,….* y 5 *"Promover la difusión de producciones nacionales y producciones nacionales independientes y fomentar el desarrollo de la industria audiovisual nacional*". En su Capítulo VII Del Procedimiento Administrativo Sancionatorio, hace alusión a los sujetos sobre los cuales recae el mismo, solo señala: *"Se sancionará al prestador de servicios de radio, televisión o difusión por suscripción…"* (Art. 28) y el art. 29 ejusdem refiere a las sanciones de suspensión y revocatoria de los sujetos anteriormente indicados cuando a) promuevan, hagan apología o inciten a alteraciones del orden público y, b) promuevan, hagan apología o inciten al delito, entre otros actos.

d) Ley sobre Protección a la Privacidad de las Comunicaciones[36]

Esta ley fue publicada en la Gaceta Oficial No. 34.863, de fecha 16 de diciembre de 1991, tiene por objeto proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas (Art. 1). En concatenación con la Constitución Nacional que en su art. 48, que establece el derecho al secreto e inviolabilidad de las comunicaciones.

e) Providencia 01/09 de CONATEL, de fecha 22 de diciembre de 2009[37]

Norma técnica sobre los servicios de producción nacional audiovisual (sustituida por la actual providencia administrativa N° 027, publicada en la Gaceta Oficial N° 40.415, de 20 de mayo de 2014). Su objeto era desarrollar el régimen jurídico aplicable a los servicios de producción nacional audiovisual, de conformidad con la Ley de Responsabilidad Social en Radio y Televisión; en la vigente providencia Nº 027 el objeto de la misma se mantiene igual. En su

36 Congreso de la República de Venezuela. Ley Sobre Protección a la Privacidad de las Comunicaciones Gaceta Oficial de la República Bolivariana de Venezuela Nº 34863 de fecha 16 de Diciembre de 1991.

37 República Bolivariana de Venezuela. Directorio de Responsabilidad Social. Providencia Administrativa. 01/09. CONATEL Norma Técnica sobre los servicios de producción nacional audiovisual. 22 de diciembre de 2009.

artículo 3 se definía al servicio de producción nacional audiovisual[38]. En la actual providencia se mantiene la misma definición. Por su parte, el art. 5 de la providencia del año 2009, contemplaba lo relativo a las transmisiones de mensajes o alocuciones oficiales. En la actual providencia del año 2014, esto está contemplado en el art. 7 *ejusdem*[39]. Por su parte, la providencia 01/09 en sus artículos 7, 9 y 11, aludía al proceso de notificación del interesado para prestar el servicio a CONATEL, la calificación que CONATEL hace y el registro respectivo. En la providencia Nº 027, esto está establecido de igual manera en los artículos 4 y 5.

Finalmente, la nueva Providencia Administrativa 027 publicada en la Gaceta Oficial 40.415, del martes 20 de mayo de 2014, dictamina bajo la denominada "Norma Técnica" que los prestadores de servicios de producción nacional audiovisual deberán introducir dentro de su red de programación, bajo contrato previo, al menos 8% de servicios de producción audiovisual nacional en proporción al resto de canales ofrecidos (art. 9). Esta medida no estaba contemplada en la providencia 01/09, significando que pudiese ser aplicada esta norma con discrecionalidad y afectar la operación tanto de los canales de televisión por suscripción como a las empresas operadoras. Por esta razón, al igual que la providencia derogada (vigente frente a los hechos referenciados en esta investigación), la nueva providencia también se pudiese considerar contraria a los estándares de protección de la libertad de expresión, por configurar un uso abusivo del poder estatal, ante controles en telecomunicaciones arbitrarios que podrían restringir la libertad en la labor de algunos medios por suscripción.

2. Impacto de la ciberseguridad en el entorno digital en Venezuela

Una vez revisados los artículos de las leyes, incluida la Constitución Nacional, con mayor incidencia en la materia del derecho a la libertad de expresión e información, se hará una descripción de la vulnerabilidad de este derecho en

38 Se consideran como servicios de producción nacional audiovisual, a aquellos canales cuya recepción y/o difusión de imágenes y sonidos ocurran dentro del territorio de la República Bolivariana de Venezuela, y se difundan sólo a través de la red de un prestador del servicio de difusión por suscripción habilitado por la Comisión Nacional de Telecomunicaciones, con excepción, de al menos, uno de los siguientes supuestos:

1. Que el canal contenga en su programación semanal más del 70% de programas, publicidad o propaganda que, en su conjunto, no califiquen como producción nacional, de conformidad con lo establecido en el artículo 2 de la presente norma técnica.
2. Que el canal contenga en el tiempo total de su programación semanal más del 70% de programas, publicidad o propaganda que, en su conjunto, no califiquen como producción nacional, de conformidad con lo establecido en el artículo 2 de la presente norma técnica.

39 **Providencia Nº 027**. **Artículo 7 Transmisiones de mensajes o alocuciones oficiales**. "Los Servicios de Producción Nacional Audiovisual, deben transmitir gratuitamente los mensajes o alocuciones oficiales conforme a lo establecido en el artículo 10 de la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos".

forma general y, en particular en el medio digital. Se seguirá para los fines correspondientes los dos Informes de PROVEA[40], correspondientes a enero-diciembre 2009[41] y, enero-diciembre 2013[42], sobre Derecho a la Libertad de Expresión e Información, con referencia a restricciones administrativas que se desprenden de las Providencias de CONATEL, en los últimos años y que se han aplicado bajo la excusa de la defensa de la patria. Estos informes servirán para evidenciar el impacto que el tema de la ciberseguridad en el país ha significado para los usuarios de los medios de información y comunicación y especialmente para los usuarios de las RSV.

Entre estas acciones se encuentran: las privativas de libertad que se dictaron como consecuencia de investigaciones penales iniciadas contra dirigentes políticos de oposición, dueños de medios y periodistas en virtud de su opinión política; la sentencia de censura previa que prohibió a todos los medios impresos del país publicar información sobre violencia durante un mes; la sentencia que condenó a un comunicador social en Valencia a prisión e inhabilitación profesional por un lapso de 3 años y medio por haber denunciado nepotismo en una alcaldía del Partido Socialista Unido de Venezuela (PSUV); los cierres temporales y definitivos de medios de comunicación privados, entre los cuales destaca la salida definitiva de RCTV (Radio Caracas Televisión) de la programación disponible en la televisión por suscripción; el aumento de detenciones arbitrarias por parte de funcionarios policiales para incautar material periodístico; y la creación del Centro de Estudio Situacional de la Nación y de las guerrillas comunicacionales, ambos órganos vigilantes de los intereses del Ejecutivo en la información que difunden los medios de comunicación privados. Desde octubre de 2009 hasta septiembre de 2010 se registraron 81 casos que implicaron 98 violaciones a la libertad de expresión. También durante este período, concretamente el 04 de agosto de 2010, CONATEL pasó a depender de la vicepresidencia de la República, con lo cual el Ejecutivo incumplió con el artículo 35 de la Ley Orgánica de Telecomunicaciones, antes indicado y le resta autonomía e independencia que por ley le corresponde.

Además, PROVEA en su informe de 2009, resalta que este ente ha aplicado una serie de restricciones administrativas, lo cual es otro elemento violatorio a los derechos de los ciudadanos. Las restricciones administrativas ocupan el 13,26% de los ataques a la libertad de expresión y han dejado fuera del aire

40 El Programa Venezolano de Educación-Acción en Derechos Humanos (PROVEA) es una organización no gubernamental (ONG) independiente venezolana dedicada a analizar la situación de los derechos humanos en Venezuela y a la promoción y defensa de los mismos. El trabajo de la organización, se resume en un informe anual que publica y distribuye a entidades públicas y privadas, nacionales e internacionales

41 PROVEA Informe Anual enero-diciembre 2009. Derecho a la Libertad de Expresión e Información

42 PROVEA Informe Anual enero-diciembre 2013. Derecho a la Libertad de Expresión e Información

definitivamente: un canal de televisión privado con señal abierta, un canal de televisión por suscripción y una radio comunitaria. También, cinco canales de televisión por suscripción, cuatro emisoras de radio y dos periódicos regionales fueron cerrados temporalmente; y una radio privada se vio afectada con la reducción significativa de su ámbito de transmisión. Esto como consecuencia, de la aplicación de la Providencia Administrativa de CONATEL, antes referida, que da un control excesivo al Estado sobre los servicios de programación nacional. Con relación a estas acciones administrativas hasta la fecha no ha habido pronunciamiento del Tribunal Supremo de Justicia (TSJ) sobre el fondo en los procedimientos administrativos adelantados por CONATEL contra emisoras y canales de televisión.

En este mismo sentido, cabe resaltar la creación por parte del Presidente venezolano, del Centro Estratégico de Seguridad y Protección de la Patria (CESPPA), cuyo presidente pasó a tener muy amplias facultades ya que podrá "*declarar el carácter de reservada, clasificada o de divulgación limitada, cualesquiera información, hecho o circunstancia que en cumplimiento de sus funciones tenga conocimiento*". Lo cual atenta y viola lo consagrado en la Constitución y las leyes en la materia (arts. 47,57 y 58, de la Constitución)

Ahora bien en el tema de los medios digitales, es de resaltar que el Informe de PROVEA 2013, señala que el 63,8% de los medios afectados (periódicos, radios, televisoras y medios digitales) resultaron de carácter privado, como ha sido una tendencia clara de los últimos años. Al desagregar por sectores específicos, la gran novedad de este 2013 ha sido la aparición de un sector como lo es "proveedores de Internet", para dar cuenta de las limitaciones impuestas por CONATEL contra los principales proveedores de Internet del país, con la finalidad de restringir información que el gobierno consideró ilegal (caso de la "caída" de las páginas que informaban sobre la tasa del dólar negro). El 10 de noviembre de 2013, el Presidente Nicolás Maduro le ordenó a CONATEL bloquear las páginas de Internet que difundían las cotizaciones del llamado dólar paralelo, en el marco de lo que el gobierno denominó "la guerra económica". Esta acción de censura fue seguida de la apertura de un inédito proceso administrativo sancionatorio contra ocho empresas proveedoras del servicio de Internet por tener alojadas dichas páginas o políticamente inoportuna, (suspensión de sitios con información que revelaban la gravedad en el estado de salud del Presidente Chávez).

Otro caso fue el de la jueza María Lourdes Afiuni, quien quedó obligada a presentarse cada 15 días al tribunal y no salir del país, ambas son medidas tradicionales; pero además se le impuso la prohibición de comunicarse por la red social Twitter, en la cual contaba con más de 250 mil seguidores.

De igual manera, la web también ha sido la herramienta de los medios y periodistas que han salido del aire por las presiones gubernamentales. Un caso emblemático es el de Alberto Federico Ravell, quien después de ser obligado a dejar la dirección editorial de Globovisión abrió el sitio web www.lapatilla.com.

Luego de su salida de la programación de televisión por suscripción, RCTV Internacional también transmite su noticiero a través de la web. Los portales de noticias han adquirido popularidad por la misma razón que explica el crecimiento de los usuarios del *Twitter*: muchos de estos ofrecen la posibilidad a sus lectores de comentar y/o agregar información.

En Venezuela son seguidos por muchos usuarios los noticieros web Noticiero Digital y Noticias 24, que recogen opiniones sobre el desempeño del gobierno como de la oposición. El Ejecutivo Nacional y la Asamblea Nacional han seguido de cerca la información producida en los medios de comunicación digital y en el último año solicitaron en dos oportunidades al Ministerio Público que investigara a los dueños de estas páginas, entre ellas a quienes conducen Noticiero Digital. Gracias a la providencia de CONATEL 01/09, antes indicada, ahora estos son servicios de producción nacional y como tales se les ha aplicado algunas restricciones pues lo somete a una regulación que implica más que regulación control y autocensura, en lo relativo a las transmisiones de mensajes o alocuciones oficiales, estos servicios deben transmitir las cadenas oficiales, para su legalidad deben llevar a cabo el proceso de notificación del interesado para prestar el servicio a CONATEL, luego esperar la calificación que debe hacer CONATEL y el registro respectivo, de acuerdo a los artículos antes referidos de esta providencia.

En perfecta armonía con lo planteado, desde el año 2010, en el país se tiene como antecedentes la detención de personas por difundir mensajes en las redes sociales. En ese año fueron aprehendidas dos personas por críticas al sistema bancario vía Twitter. Posteriormente, un ingeniero de CORPOELEC[43] corrió la misma suerte por comentarios en la red que, a juicio del CICPC[44], "incitaban al magnicidio". Todo de acuerdo con lo planteado en la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, en su artículo 29, letras a y b, como se hiciera referencia antes. En marzo de 2013, una mujer de 53 años fue privada de libertad por presuntamente "descubrírsele algunos mensajes desestabilizadores". Luego, en abril, un joven fue acusado de difundir un video en YouTube en el que aparecía el entonces Ministro de Hábitat, Ricardo Molina, amenazando a empleados que apoyaban al candidato presidencial Henrique Capriles.

En este sentido, se puede agregar que CONATEL hizo un exhorto para castigar a los medios que hicieran apología de la violencia en la cobertura de las

43 Empresa Eléctrica Socialista, adscrita al Ministerio del Poder Popular de Energía Eléctrica, es una institución que nace con la visión de reorganizar y unificar el sector eléctrico venezolano a fin de garantizar la prestación de un servicio eléctrico confiable, incluyente y con sentido social.

44 El Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), antes conocido como Cuerpo Técnico de Policía Judicial (CTPJ) y en sus orígenes como Policía Técnica Judicial (PTJ), es el principal organismo de investigaciones penales de Venezuela. Se encarga del esclarecimiento científico de los delitos con miras a la posterior aplicación de la justicia por los órganos competente

protestas desarrolladas en el país a partir del mes de febrero de 2014, incluyendo por primera vez a las páginas de Internet. (De Abasolo, 2014)[45]. Esto otra vez con base a las sanciones contempladas en la Ley sobre Responsabilidad Social en Radio, Televisión y Medios Electrónicos.

Stelling (2014)[46], experta socióloga en materia de comunicación social, define la medida impulsada por CONATEL sobre la cobertura de protestas como *"una línea muy débil entre el exhorto y la censura"*. Considera que desde hace tiempo las redes sociales están en el ojo del huracán debido a que generan una suerte de normas propias. No obstante, califica de "peligroso" cualquier intento de control mediante amenazas. *"Eso podría convertirse en un error grande para el gobierno porque avalaría esas acusaciones de totalitarismo, violación de los derechos humanos y ataque a la libertad de expresión que tanto denuncian internacionalmente"*.

La experta resalta que las redes sociales "*tienen un altísimo nivel de penetración en Venezuela*", y se han convertido en un canal de información, estimulación y hasta de provocación entre un sector y otro. Lo define como una ventana vital para el ciudadano y hasta para el mismo gobierno que estratégicamente ha apelado a su uso para conectarse con sus seguidores. *"La mejor manera de abordar a los medios de comunicación es con responsabilidad y compromiso, pero sin presiones*". (De Abasolo, 2014)[47].

Por su parte, Carlos Correa, Director de la organización no gubernamental "Espacio Público", señala que el llamado de CONATEL pretende "*generar autocensura e inhibición"* en los medios de comunicación, lo que a su vez, se extiende a la interacción de las redes. "Hay consciencia de la importancia de estas redes; tanto, que existe *un viceministerio. Al reducirse los espacios la gente busca opciones y éstas se han convertido en las más importantes"*. (De Abasolo, 2014)[48].

Correa cree que atentar contra las redes sociales es complicado, no solo porque el gobierno también hace uso de éstas, sino porque tales sistemas tienen mecanismos que permiten burlar cualquier tipo de censura. A su juicio, el control no solo atentaría contra la Constitución sino que generaría más incertidumbre en una población que se mantiene en la constante búsqueda de espacios de

45 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

46 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

47 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

48 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

expresión *"debido a la censura y autocensura que ya ha sido impuesta en los medios tradicionales"* (De Abasolo, 2014)[49].

Por ello, se ha observado que en el país durante estos últimos años de conflictividad social, se han desarrollado una serie de eventos, que merecen ser objeto de estudio, frente a la evidente vulnerabilidad de algunos derechos fundamentales que ahora se extiende a los sitios web y RSV.

V. Algunas consideraciones finales

En consecuencia a lo expuesto, hoy tiene mucho más sentido el documento sobre la Declaración de Derechos del Ciberespacio, en el cual se expresa el derecho a la protección de los datos personales y al secreto de las telecomunicaciones, la regulación de derechos y obligaciones, de la fiscalidad (regulando las transacciones, cada vez más comunes, que se realizan por este medio), la elaboración de una normativa global penal (encaminada a perseguir, de forma efectiva, aquellos delitos que superar la estructura, física y política, de los Estados), un desarrollo coherente de la propiedad intelectual, y el amparo de los derechos fundamentales inherentes a la persona. Señala Suñé (2008)[50]:

> *…En esencia, los mecanismos de dominación y de limitación de los derechos humanos en este nuevo espacio de información o ciberespacio tienen más que ver con la limitación del acceso a las condiciones necesarias (ya sean técnicas, económicas o culturales) que permitirían el desarrollo de formas más avanzadas de participación pública y de intercambio y libre expresión de ideas y creencias…..".*

Por su parte, son variadas las formas de ataque y los atacantes en el medio digital, frente a ello los Estados, desde los más conservadores o de izquierda hasta los más modernos o de democracias representativas, buscan evitar daños a sus ciudadanos y bienes, no obstante las acciones de Estado en la mayoría de las ocasiones violentan los derechos humanos de quienes quieren expresarse y estar informados. Por otro lado, es peligroso dejar de tomar medidas frente a los posibles ataques en la red, que pueden significar verdaderas amenazas no sólo para los Estados en sí mismos sino para la humanidad. Es necesario pues encontrar un acuerdo que armonice y otorgue proporcionalidad, tanto por una parte, al derecho de los Estados y organizaciones a protegerse frente a los ciberataques, pero por otro lado, reconocer y respetar el derecho ciudadano y humano a expresarse e informarse por medios lícitos, creándose foros de

49 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

50 Suñé Llinás, E. (2008). La ausencia de privacidad en Internet: Hacia una Constitución y Declaración de Derechos del Ciberespacio. *Contrastes*, 50. Págs. 66 ss.

participación multidisciplinarios donde tanto los entes gubernamentales, como organizaciones internacionales y la sociedad organizada puedan conformar planes estratégicos de defensa sin menoscabo de los derechos ciudadanos.