Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

LOS DERECHOS HUMANOS ANTE LA VIGILANCIA INDISCRIMINADA DE LAS COMUNICACIONES PRIVADAS.

(Human Rights To The Wiretapping Private Communications)

Vanderlinder, Irene. Universidad del Zulia. Venezuela
irene.vanderlinder@gmail.com

Resumen

El objetivo del presente artículo va dirigido hacia el análisis de la seguridad en las comunicaciones privadas en entorno digitales, en un mundo altamente informatizado parte de las comunicaciones se producen en contexto de interconexión gracias a las tecnologías de la información y comunicación, deben crearse entornos seguros para la libertad en las comunicaciones, sin embargo, los derechos no deben concebirse como absolutos en tanto los límites a las prácticas de vigilancia y control por parte del Estado en resguardo de la soberanía ha de configurarse en un marco de respeto y garantía a los derechos fundamentales, los derechos humanos. La mirada internacional en el tema del espionaje ha generado respuesta a través de instrumentos jurídicos que prohíben la vigilancia indiscriminada las comunicaciones privadas por parte del Estado quien debe velar por el cumplimiento de un Estado de Derecho y de Justicia. El derecho al uso de la tecnología es también un derecho humano que forma parte del derecho a la información y comunicación aunado a ello el derecho a la privacidad y confidencialidad debe protegerse también en estos entornos digitales, en tal sentido activistas de derechos humanos recomiendan como una medida de seguridad a través del software libre resguardar la información personal.

Palabras Clave: Derechos Humanos, Vigilancia Indiscriminada, Comunicaciones Privadas

Abstract

The aim of this article is directed towards analysis of security in private communications in digital environment, in a highly computerized world of communications occur in context of interconnection thanks to information technology and communication, must create safe environments for freedom and communications, however, the rights should not be construed as absolute as the limits on surveillance practices and control by the state in defense of sovereignty must be set within a framework of respect and guarantee fundamental rights, human rights. The international look at the issue of espionage has generated response through legal instruments prohibiting wiretapping private communications by the State that must ensure compliance with the rule of law and justice. The right to the use of technology is also a human right which forms part of the right to information and communication together with it the right to privacy and confidentiality should also be protected in these digital environments, in that sense, human rights activists recommend as a security measure through free software protect personal information.

Keywords: Human Rights Watch Indiscriminate, Private Communications

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

Introducción

El fenómeno globalización ha venido a cambiar esquemas en las relaciones sociales siendo las comunicaciones en entornos cibernéticos una poderosa arma de interconexión de millones de personas alrededor del mundo gracias a las tecnologías de la información y comunicación. Es indudable el progreso que esto ha generado en las naciones prósperas y menos prósperas, sin embargo, el fenómeno comunicativo a través de las redes informáticas también han producido cambios en los esquemas de seguridad nacional de los Estados, hay posiciones que se contraponen el deber del Estado en proteger la soberanía política y en virtud de ello vigilar y controlar todo aquello que atente la propia seguridad y por el otro lado el uso indiscriminado de la vigilancia en las comunicaciones atentando contra la privacidad y confidencialidad. Ahora bien, activistas de los Derechos Humanos ante esta desmesurada vigilancia hacen voz de eco por el uso indiscriminado al intervenir millones de comunicaciones privadas atentando contra la el derecho a la privacidad y confidencialidad.

La era digital ha generado que se masifiquen comunicaciones a través de redes informáticas como lo es internet, el tema de la seguridad se ha puesto en duda debido a las revelaciones de informantes que han dejado en evidencia las prácticas indiscriminadas de vigilancia por parte de grandes potencias como lo es Estados Unidos, las revelaciones de Edward Snowden abrió el acalorado debate mundial del espionaje masivo en las comunicaciones privadas, lo que trajo como consecuencia el pronunciamiento internacional y la promulgación de instrumentos jurídicos y cartas que prohíben la vigilancia indiscriminada por parte de los Estados y el espionaje, vale decir, que el Estado en defensa de su soberanía puede acceder a información que vaya dirigida a la prevención de delitos y ponga en riesgo la seguridad de las personas y los Estados, sin embargo, deben limitarse los excesos que van en detrimento de los Derechos Humanos.

1- La Seguridad como eje central de la Política de Estado.

Mucho se ha hablado de los entornos digitales y del impacto que tienen en las comunicaciones, cada día más personas se suman a las redes de interconexión: internet, redes sociales, *twitter, instagram, youtube*, *whastapp* por otro lado mucho antes el correo electrónico fue pionero en el enlace de mensajes sustituyendo el correo tradicional, pasa a segundo plano con las redes en tiempo real intercambiando información desde una conversación entre personas hasta la descarga de contenidos de la noticia más emblemática como el bombardeo a aldeas y poblaciones lejanas de África por citar un ejemplo entre muchísimos que pudieran estar censurados por los medios de comunicación tradicionales.

La *soberanía digital* hace referencia a lo que se entiende por soberanía política, el deber del Estado de proteger su territorio, sus habitantes y todo lo que atente contra la seguridad nacional, por su parte la soberanía digital es concebido como poder que permite el resguardo de información pero en el ciberespacio. Este concepto de *soberanía* se transforma hacia la lógica gubernamental estadounidense, caracterizada por la ausencia de barreras o fronteras establecidas, en donde Internet constituye una

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

seria amenaza a la capacidad del Estado soberano de controlar los acontecimientos políticos y sociales que tienen lugar tanto dentro como fuera de sus fronteras. El almacenamiento de los datos es una cuestión de soberanía nacional ya que las multinacionales norteamericanas que ofrecen acceso y servicios en Internet no entregan información a los Estados argumentando que sus archivos están alojados fuera del país.

Las grandes corporaciones trasnacionales en materia de comunicaciones digitales al permanecer registradas en los Estados Unidos no se ven obligadas a aportar información solicitada, se presenta la problemática del choque entre decisiones judiciales y las cláusulas de confidencialidad en contratos de éstas empresas los cuáles prohíben revelar contenidos por cuanto atenta contra la confidencialidad de los usuarios de tales redes. Cabe preguntar, ¿Estarían estas empresas transnacionales incurriendo en desacato por no cumplir con órdenes judiciales violando la normativa interna de un Estado? La respuesta es sí, los Estados son soberanos y deben las empresas someterse en sus relaciones al ordenamiento jurídico interno del Estado donde desarrollan su actividad comercial. Sin embargo, existen otros riesgos en materia de seguridad con es el espionaje y la vigilancia indiscriminada que serán tratados en los siguientes puntos de este artículo.

Según el reporte del Banco de Desarrollo de América Latina, 2014, América Latina es el continente con las redes de telecomunicaciones más dependientes de Estados Unidos: más del 90% del tráfico en Internet de la región pasa por servidores norteamericanos y el 85% de los contenidos digitales de Latinoamérica también están alojados en el Estados Unidos. La metodología utilizada por la NSA para reunir una gran cantidad de comunicaciones, implica el acceso directo a muchos de los cables internacionales de fibra óptica que se utilizan para transmitir comunicaciones internacionales, incluidos los submarinos. La agencia también desvía hacia sus servidores, mensajes que atraviesan el sistema de los Estados Unidos, tal y como lo hace buena parte de las comunicaciones mundiales, y coopera con servicios de inteligencia de otros países, que le ayudan en su recopilación.

En este orden de ideas, las intervenciones en las comunicaciones no justifica esta práctica en razón de la seguridad, debe en consecuencia traer a colación el principio de proporcionalidad que en el tópico de estudio no podría si se aplica justificar el uso indiscriminado de la vigilancia cibernética por razones de seguridad, la interceptación de las comunicaciones sólo debe permitirse en consecución de los objetivos más importantes del Estado. Para Assange, 2013, el riesgo en que se encuentra la soberanía digital en Latinoamérica y el Caribe pues, como se menciona más arriba, gran parte del tráfico de sus comunicaciones transita a través de cables de fibra óptica que físicamente pasan por Estados Unidos. Y esto se traduce en una grave amenaza a la privacidad con el uso de Google o Facebook, un ejemplo que puede servir de muestra de los lazos de esta dependencia informática: un correo electrónico enviado entre dos ciudades limítrofes de Brasil y Perú, entre Río Blanco, capital de Acre, y Puerto Maldonado, va hasta Brasilia, sale por Fortaleza en cable submarino, ingresa a Estados Unidos por Miami, llega a California para descender por el Pacífico hasta Lima y seguir viaje hasta Puerto Maldonado, a escasos 300 Km de donde partió.

La ubicación de los servidores que almacenan la información. Para tomar conciencia de la realidad, en toda Sudamérica hay 43.552.918, mientras que en

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

Estados Unidos existen más de 498.000.000 servidores, dentro de los que se incluyen los de Microsoft, Facebook, Twitter, Google, AOL, Yahoo!, YouTube y Apple, entre otros. Estos son factores que posibilitan el espionaje desde Estados Unidos, que se traduce claramente en una soberanía debilitada. Mientras que el gobierno norteamericano justifica esta intervención con el pretexto de la lucha contra el terrorismo internacional, excluye el debate de lo que se entiende por *terrorismo*.

Esta problemática por la soberanía política y digital no es solo preocupación de países vulnerables, China y Rusia, por ejemplo, han venido desarrollando estrategias tecnológicas y de información para enfrentar el casi absoluto predominio norteamericano en la era de la Internet. China, Rusia, Irán, Cuba e Israel están entre los principales objetivos de las agencias estadounidenses de espionaje, según publicaciones de *The Washington Post*. También Brasil, España, Francia, México, Venezuela, y la Unión Europea han sido víctimas de intervenciones. Los teléfonos y correos de Dilma Rousseff, Angela Merkel y otros líderes mundiales, han sido objeto de dichas intervenciones (Indexmundi, 2014). En la inauguración del 68º Periodo de Sesiones de la Asamblea General de Naciones Unidas, la presidenta Dilma Rouseff denunció que la ONU debe desempeñar un rol de liderazgo en todos los esfuerzos destinados a regular la conducta de los Estados en lo referido a Internet pues considera que el pleno aprovechamiento de Internet requiere una reglamentación responsable que garantice la libre expresión y el respeto a los Derechos Humanos.

Ante esta situación, los Estados que integran el bloque subregional Mercosur adoptaron un documento especial de rechazo al espionaje estadounidense en el que expresan su preocupación por promover en las instancias multilaterales pertinentes la adopción de normas relativas a la regulación de Internet, con énfasis en los aspectos de seguridad cibernética y acordaron la formación de un Grupo de Trabajo con el fin de tomar acciones que hagan más seguras nuestras telecomunicaciones y reduzcan nuestra dependencia de la tecnología extranjera.

La vigilancia indiscriminada ha roto numerosas leyes nacionales en los Estados Unidos. Internet comenzó su fase de expansión rápida en un contexto global marcado por la guerra contra el terror, con el aumento de las restricciones y violaciones de los Derechos Humanos, especialmente a la privacidad, y la intensificación de la vigilancia estatal. Los poderes expansivos concedidos a las agencias de inteligencia después de 11 de septiembre de 2001 violentan incluso la Constitución de Estados Unidos. Dos años después del éxito contra SOPA (Stop Online Piracy Act) y PIPA (Protect IP Act) en los Estados Unidos, la comunidad activista por una Internet libre y sin espionaje, se está posicionando para la próxima batalla: el respeto a los derechos en la *era digital*. (Gellman y Miller, 2014).

2- Revelaciones de Espionaje: Caso Edward Snowden. Perspectiva Internacional.

La revelación que causó repudio ante el mundo marca un hito en la mirada internacional, Edward Snowden reveló la existencia de un aparato mundial de espionaje, en tanto los organismos de Derechos Humanos advierten el peligro de Estados que se transforman en vigilantes omnipresentes. Assange, por su lado, decidió difundir documentos filtrados de las bases de datos gubernamentales con la

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

clasificación de *ultra secreto* desde su página web: *Wikileaks,* la organización que ha revelado una gran cantidad de datos ocultos sobre la guerra de Afganistán.

Aunque *Wikileaks* comenzó a funcionar a partir de 2008, tomó difusión pública internacional en el 2010 con la publicación de un video en el que se ve cómo soldados estadounidenses disparan desde un helicóptero a un reportero, su ayudante, nueve personas armadas y otras que se acercaron a socorrer a los heridos. Assange, 2013, denunció que Internet ha sido ocupada militarmente por Estados Unidos y sus aliados para dominar a las sociedades atentando contra su soberanía nacional.

En junio de 2013, el periódico *The Guardian* publicó la primera de una serie de revelaciones de Snowden sobre el espionaje masivo de Estados Unidos, evidenciando la magnitud, los objetivos y los métodos con los que la NSA, que es la organización de vigilancia más grande y secreta de Estados Unidos, recopila información en todo el mundo. Estados Unidos, junto con sus cuatro aliados más cercanos: Reino Unido, Canadá, Australia y Nueva Zelanda, han construido una red de sistemas de vigilancia de comunicaciones digitales de alcance mundial llamado Cinco Ojos que conforma una alianza de intercambio de inteligencia. El Club de los Cinco Ojos nació a partir de la estrecha colaboración en materia de espionaje que mantuvieron Estados Unidos y Reino Unido durante la II Guerra Mundial, en particular por el trabajo realizado desde el centro británico Bletchley Park para descifrar los códigos alemanes y japoneses. La alianza de los Cinco Ojos funciona en base al principio de compartir información y no espiarse mutuamente. Entre estos países existe un alto grado de cooperación estratégica e intercambio de inteligencia; debido a ese trabajo conjunto el material reunido bajo el régimen de vigilancia de un país se comparte con el resto. La gran distancia que separa a estos países les permite vigilar la mayor parte del tráfico mundial de Internet. Otros, como Rusia y China, tienen sus propias redes omnipresentes de vigilancia y acuerdos que proteger.

La lista de países donde la NSA ejerce sus actividades de vigilancia, comprende a naciones tales como: Austria, Bélgica, República Checa, Dinamarca, Alemania, Grecia, Hungría, Islandia, Italia, Luxemburgo, Países Bajos, Noruega, Polonia, Portugal, España, Suecia, Suiza, Turquía, Japón y Corea del Sur. Hay países en los que Estados Unidos espía rutinariamente, pero con los que prácticamente nunca coopera, como Venezuela, China, Irán, y Siria. Pero en el tercer nivel se incluyen también países neutrales como: Brasil, México, Argentina, Indonesia, Sudáfrica y Kenia.

El primer documento revelado por Snowden fue una orden del Tribunal de Vigilancia de Inteligencia Extranjera de Estados Unidos (FISA) creado por el Congreso, después de que el Comité Church del Senado descubriera décadas de escuchas telefónicas abusivas del gobierno. El objetivo de creación de la FISA fue que el gobierno pudiera seguir involucrado en la vigilancia electrónica, pero para impedir abusos tenía que obtener permiso del FISA antes de llevar a cabo una operación. Este tribunal es una de las instituciones más secretas del gobierno estadounidense. Todos sus dictámenes son automáticamente caratulados como máximo secreto, y sólo un pequeño grupo de personas tiene autorización para acceder a sus decisiones. En ese documento, se le ordena a la empresa de comunicaciones Verizon Business que entregara a la NSA todos los registros en detalle de comunicaciones; entre el gobierno de Estados Unidos y el exterior, y las comunicaciones locales dentro de Estados

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

Unidos, eso significa que la NSA estaba recolectando secreta e indiscriminadamente los registros telefónicos de decenas de millones de estadounidenses. Por otro lado, la FISA dio permiso a la NSA para espiar a 193 países. (Assange, 2013).

Esta autorización también permitía a la NSA recolectar información de inteligencia de organismos como el Banco Mundial, el Fondo Monetario Internacional y la Unión Europea. A su vez, Snowden aportó pruebas de que la administración de Obama estaba realizando este tipo de actividades a través de la publicación de los documentos que el gobierno había tratado desesperadamente de ocultar.

Desde el 11 de septiembre de 2001, el gobierno de Estados Unidos reforzó dramáticamente las capacidades de sus servicios de inteligencia para recopilar e investigar la información de extranjeros y ciudadanos estadounidenses. Otro de los documentos altamente reveladores publicados por Snowden fue sobre el programa conocido con el nombre de PRISM. Este programa ejecutado por la NSA recoge datos electrónicos privados pertenecientes a los usuarios de los principales servicios de grandes empresas de Internet como Gmail, Facebook, Outlook, Microsoft, Apple y Yahoo, entre otros. Aunque el gobierno de Estados Unidos insiste en que sólo se le permite recoger datos cuando obtiene autorización por la FISA, en la práctica este programa también recoge datos de ciudadanos que no son sospechosos de conexión alguna con el terrorismo o cualquier delito.

Snowden también reveló lo que él denomina una arquitectura de la opresión refiriéndose a la infraestructura de espionaje de la NSA por medio de la cual se puede acceder directamente a las comunicaciones y los datos privados, y que constituyen una serie de programas de vigilancia ultra secretos que van más allá de lo que se ha dado a conocer públicamente. Su método de recolección de datos se resume en: detectar, conocer, recolectar, procesar, explotar y compartir todo. En definitiva, Snowden considera que la NSA se ha desviado mucho de su objetivo de proteger la seguridad nacional, violentando la vida privada, la libertad de Internet y las libertades fundamentales.

Junto con las revelaciones, Snowden escribió un documento, llamado *Manifiesto pro privacidad*, y firmado por ciudadanos de todo el mundo quedaba demostrado así que existía apoyo global para la protección de la privacidad. Por todos estos acontecimientos puede decirse que en 2013 el mundo tomó conciencia de que la vigilancia digital por los gobiernos del mundo no conoce límites. Y, por tanto, la vigilancia masiva no es una práctica aislada. Las filtraciones de Edward Snowden develaron que existe la tecnología para vigilar a millones de usuarios de Internet. La NSA, y otras entidades similares, vigilan masivamente miles de comunicaciones bajo el argumento de la seguridad nacional y la lucha contra el terrorismo. La naturaleza digital de la información en Internet implica que todo lo que hacemos en línea deja una *huella*.

La información en Internet está codificada para que terceras personas no puedan acceder a ella, es decir, que aunque la puedan ver no la puedan leer; aun así la vigilancia sigue siendo posible mezclando estrategias como intervenir los cables de internet, o forzar a las empresas privadas que recolectan datos masivos sobre sus usuarios a que entreguen esa información cuando una orden legal lo permite. Sin embargo, las publicaciones de Snowden dejan ver que la intervención a las comunicaciones va mucho más allá, por ejemplo cuando la NSA interviene los cables

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

de redes privadas que conectan los centros de datos de Google y Yahoo en todo el mundo; esas redes no son partes de Internet, y la información que circula por ahí no está codificada. Es así como hay una enorme cantidad de información de todas las personas usuarias y existen los caminos para que esa información llegue a los organismos encargados de vigilar.

La interpretación de metadatos hace coincidir la información de las personas con quienes se sostiene la comunicación; por ejemplo, el GPS del celular dice con precisión dónde se ha estado, pero si se compara con el GPS de otra persona se logra saber exactamente en dónde se ha estado y a qué hora. Para marcar el primer aniversario de las revelaciones de Snowden, organizaciones de la sociedad civil por los derechos en la *Era Digital* publicaron un informe en el que detallan cómo algunas de las operaciones de espionaje de la NSA violaron los estándares internacionales de Derechos Humanos cuanto los principios necesarios y proporcionales. El informe sostiene que los programas de vigilancia de la NSA muestran:

- Ausencia de “legalidad”, ya que las leyes de vigilancia de la NSA están gobernadas por un cuerpo secreto de legislación desarrollado por un tribunal secreto, el Tribunal de Vigilancia de Inteligencia Extranjera de Estados Unidos, FISA, que de manera selectiva publica sus interpretaciones de la ley;
- No ser ni “necesarios,” ni “proporcionales,” ya que los diversos programas mediante los que se obtienen datos de las comunicaciones en forma masiva son utilizados violando los derechos a la privacidad de millones de personas que no son sospechosas de tener conexión alguna con el terrorismo internacional;
- No cuentan con el apoyo de autoridad judicial competente debido a que la única aprobación judicial, si tienen alguna, deriva de la FISA, que opera fuera de los procedimientos contenciosos normales, por lo que los individuos cuyos datos se recolectaron carecen de acceso a la justicia;
- Falta de debido proceso puesto que la FISA no permite audiencias públicas;
- Falta de notificación a las personas usuarias ya que aquellos cuyos datos fueron obtenidos desconocen que sus comunicaciones han sido monitoreadas y por lo tanto no pueden apelar la decisión ni obtener representación legal para defenderse;
- Falta de la transparencia y de control público, debido a que operan en secreto y se basan en órdenes que exigen confidencialidad a las entidades de las que obtienen los datos, junto con procedimientos judiciales, en caso de que existan, secretos;

El debate sobre las restricciones de los poderes estatales para vigilar las comunicaciones de los ciudadanos y para almacenar sus datos, dentro de la sociedad civil se abre a partir de las revelaciones de Snowden, violando los derechos humanos a la privacidad ajena en las comunicaciones exponiendo informaciones y comunicaciones privadas por el interés perverso del dominio hegemónico mundial, en reacción en el marco de la 24ta. Sesión del Consejo de Derechos Humanos de las Naciones Unidas, diversas organizaciones de la sociedad civil encabezadas por la Fundación por las

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

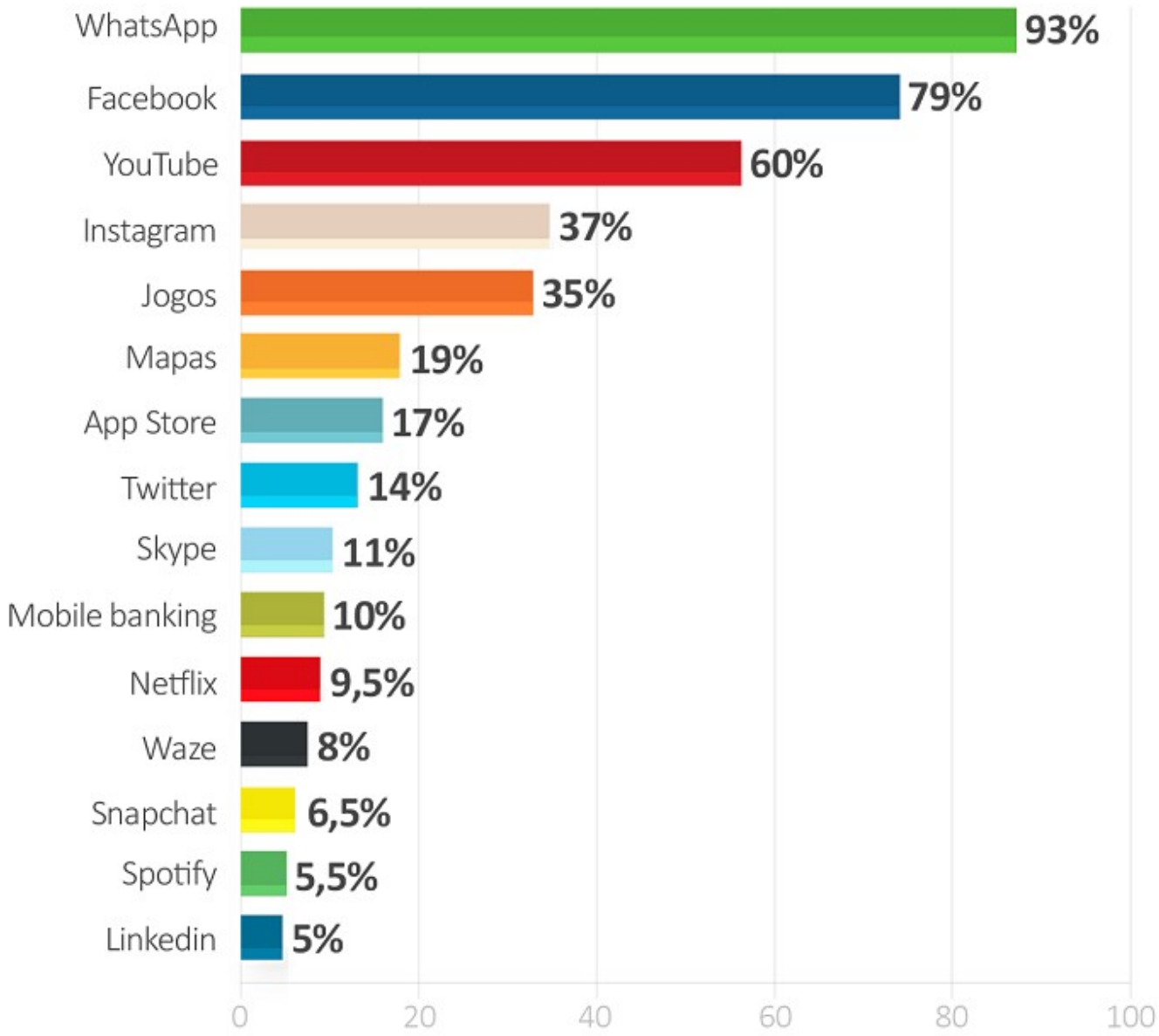
Fronteras Electrónicas (Electronic Frontier Foundation) manifestaron ante las naciones la urgente necesidad de cumplir y asegurar los Derechos Humanos y proteger a sus ciudadanos de los peligros que presenta la vigilancia digital masiva.

3- Brasil: Suspensión Temporal de la aplicación *WhatsApp*

Las aplicaciones para aparatos inteligentes que sirven para interconectarse millones de personas alrededor del mundo en entornos digitales, son una herramienta útil, sin embargo, se ha visto comprometida la interconexión de una de las aplicaciones con mayores seguidores, es el caso de *Whatsapp,* por orden judicial dictada por la Primera Corte Penal de Sao Bernardo do Campo, en virtud de un procedimiento penal. La acusación se basaba en que la aplicación móvil se negaba a colaborar con una investigación criminal relacionada con menores de edad involucrados en delitos. En materia de seguridad pueden intervenirse o bloquearse las comunicaciones, ahora bien, esta sentencia exacerbada a consideración de la investigadora es violatoria a los derechos humanos y desproporcionada en cuanto al daño causado a los usuarios de la aplicación por verse cercenados en el derecho a la comunicación, una sentencia el cual su contenido debe ser justo se vuelve injusta para los derechos colectivos.

Puede observarse en el siguiente gráfico como la aplicación *whatsapp* es la preferida frente a otras aplicaciones en el caso de Brasil por un gran porcentaje de la población cibernautica.

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016



Fuente: Encuesta realizada por Connect.

La sentencia fue dejada sin efecto por el Tribunal de Justicia de Sao Paulo, autorizando el desbloqueo de la aplicación Whatsapp, la motivación de la decisión se fundamenta en razón de los principios constitucionales, indica la referida sentencia: "*no es razonable que millones de usuarios sean afectados".*

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

4- Derechos Humanos en la Era Digital

El acceso a las nuevas tecnologías de la información y la comunicación conlleva retos y desafíos, sin embargo, se vulneran derechos en la sociedad digital como el derecho a la información, derecho a la comunicación, derecho a la intimidad y confidencialidad, derechos atinentes a la personalidad, que comportan derechos humanos, se comienza por definir cada uno para analizar el alcance y a su vez los límites de estos derechos y los derechos colectivos en una sociedad libre de la información y comunicación.

El derecho a la información abordado por la Cumbre Mundial de la Sociedad de la Información considera que éste es uno de los principios que sustenta la sociedad de la información y la misma comporta la participación plural de todos los actores sociales el cual se traduce en el derecho a recibir la información generada en el intercambio global comunicativo comportando igualmente este derecho la oportunidad de participar en la misma lo que implica la libertad de expresión. Ahora bien, los derechos humanos y el desarrollo humano duradero deben constituir las bases del desarrollo de sociedades de información y comunicación.

Como se indicó la construcción de sociedades de información y comunicación debe dar prioridad a la dignidad humana, como desarrollo humano duradero de los derechos humanos por encima de la tecnología, la cual es una herramienta necesaria en las comunicaciones de hoy en día, no puede entonces superponer la tecnología a la concepción de dignidad humana que conlleva el ejercicio de todos los derechos humanos en el uso y aprovechamiento de las nuevas tecnologías de información y comunicación, deben estar al servicio de la humanidad y no debe a través de ellas vulnerarse derechos. Por lo tanto el derecho a la información en entornos digitales debe desarrollarse bajo el marco de respeto y protección de la información y la libertad de expresión, así como el resguardo de datos personales, por lo que por el avance de la tecnología permite registrar todos los datos y recorrido cibernético en la red, los mismos van quedando registrados y la huella digital permanece.

El Derecho a la Comunicación, es entendido como el que permite el proceso interactivo esencial la coexistencia humana, a la organización de la experiencia humana que comporta la convivencia en un Estado Democrático que garantice entornos para el pleno desarrollo del ser humano y a la conformación de la ciudadanía, es un derecho que debe garantizarse en la sociedad de la información, siendo la comunicación una necesidad primordial para las relaciones interpersonales, debe fomentarse el ejercicio de la ciudadanía en entornos digitales seguros los cuáles comprenden el intercambio entre personas y de los bienes y servicios que contratan en la posición de consumidores a través del comercio electrónico nacional e internacional.

Ahora bien, se produce con las nuevas tecnologías de la información y comunicación una evolución en el concepto de protección de datos determinada por las nuevas tecnologías comunicacionales y la nueva configuración de la vida privada. La concepción del derecho a la vida privada como el derecho a ser dejado solo

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

corresponde a una época caracterizada por un marcado individualismo, por el contrario en la actualidad la vida privada ha dejado de concebirse por la libertad negativa de rechazar u oponerse al uso de la información sobre sí mismo, para pasa a ser la libertad positiva de supervisar el uso de la información. (Correa 1987).

Siendo Internet la red de redes, constituyendo la herramientas más poderosa de comunicación en la actualidad, la misma sirve de base receptora para todo el intercambio y almacenamiento de información y es través de la misma que se desarrollan relaciones entre personas que traspasan las fronteras y espacios geopolíticos, producto de este intercambio confluyen derechos humanos como constructos que vienen a dirigir tales relaciones, debe existir un equilibrio entre el derecho a la información, el derecho a la intimidad, confidencialidad por una parte y el control y vigilancia que debe realizar el Estado para el resguardo de la soberanía.

4.1 Derecho a la Privacidad y Confidencialidad

La privacidad es un derecho humano, y necesita ser protegida tanto como los demás derechos fundamentales. Los gobiernos alrededor del mundo están tomando conciencia sobre los riesgos que la vigilancia digital indiscriminada acarrea a las sociedades libres. Las actividades que restringen el derecho a la intimidad, incluida la vigilancia de las comunicaciones, únicamente pueden justificarse cuando están prescritas por ley, son necesarias para alcanzar un objetivo legítimo y son proporcionales al fin perseguido. Antes de la adopción pública de Internet, principios jurídicos bien definidos y cargas logísticas inherentes al monitoreo de las comunicaciones crearon límites a la vigilancia estatal de las comunicaciones

Al evaluar el carácter invasivo de la vigilancia de las comunicaciones por el Estado, es necesario considerar la potencialidad de la vigilancia para revelar información protegida, así como la finalidad para la que el Estado procura la información. La vigilancia de las comunicaciones da lugar a revelar información protegida y la gran probabilidad de poner a una persona en riesgo de ser investigada, de sufrir discriminación o violación de sus Derechos Humanos, lo que constituye una infracción grave a su derecho a la privacidad.

La Constitución de 1999, como texto político normativo del ordenamiento jurídico venezolano, establece en el artículo 60 lo siguiente:

> “Art.60 Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas en el pleno ejercicio de sus derechos”.

Se establece en esta norma constitucional el reconocimiento y protección del derecho a la confidencialidad y a la intimidad, así como el derecho al resguardo de su propia vida, lo que en el estudio del artículo se refiere a la protección de la información y

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

de las comunicaciones privadas, por lo que la seguridad de las mismas viene a estar regulada por la ley especial la cual establecerá los límites al uso de la informática, por tanto se observa la garantía constitucional como un derecho humano atinente a la inviolabilidad de los datos y las informaciones propias de cada persona.

Hay entonces un límite a la actividad de vigilancia de las comunicaciones, por tanto toda actividad que ponga en riesgo el resguardo de la privacidad es violación de derechos humanos, haciendo énfasis que los mismos se hacen valer frente al Estado y que quien transgrede y viola es el propio Estado, cualquier uso no autorizado de información privada por parte de los particulares constituye delito que viene a estar tipificado por las leyes, en consecuencia, debe el Estado Democrático garantizar la protección y seguridad de las comunicaciones privadas.

Un Estado de Derecho equivale a decir un Estado de Derechos Humanos, en tal sentido, la garantía a este derecho constituye la creación de políticas públicas eficaces en materia de seguridad de los ciudadanos y de la soberanía política y cibernética. La protección de estos derechos incluye el resguardo de datos personales sensibles como domicilio, estado de salud, tendencia política, preferencias sexuales, religión, relaciones con grupos determinados, la membresía en asociaciones, el derecho de asociarse, la información profesional, académica, familiar, los hobbies, facetas de la personalidad; las cuáles arrojan un perfil tipológico de la persona la cual la hace vulnerable en el uso de la información y de las comunicaciones privadas vigiladas.

La problemática se agudiza cuando los Estados potencia, Estados Unidos, en sus prácticas contra el terrorismo internacional viola éstos códigos internos de cada Estado, dejando abierta la posibilidad a través del espionaje cibernético de la vulnerabilidad de las informaciones y comunicaciones privadas, se hace necesario en este contexto en aras de garantizar la seguridad internacional y en la lucha contra el terrorismo, establecer por medio del Principio de Proporcionalidad un equilibrio en estas prácticas. El Derecho evoluciona en la medida en que surgen cambios en la sociedad y esta sociedad informatizada crear los mecanismos de protección de software libre como alternativa a la vigilancia cibernética desmesurada.

Debe el Derecho dar respuestas a los cambios vertiginosos en las nuevas relaciones sociales a la luz de la Informática, es pues la Informática Jurídica es una materia inequívocamente jurídica conformada por el sistema normativo integrado por un conjunto de normas dirigidos a la regulación de las nuevas tecnologías de la información y comunicación.

En la Sociedad de la Información y Comunicación, el Derecho debe regular las relaciones desarrolladas en entornos digitales, tomando en consideración que la informática aporta instrumentos para recoger, compilar, almacenar, clasificar, racionalizar y transmitir los datos e informaciones necesarios para la gestión de servicios y actividades comerciales. Pero qué de aquella información atinente a las personas, a su vida privada, información intrínseca que debe ser protegida y resguardada.

Este conjunto de atributos intrínsecos de la persona corresponden a los derechos de la personalidad, los cuáles conceden el poder a las personas para proteger su esencia y más importantes cualidades, uno de estos derechos es el derecho a la intimidad que puede verse vulnerado con la intervención de las comunicaciones

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

privadas por los sistemas tecnológicos, este tema es objeto actual de debate internacional que hace que los activistas de los Derechos Humanos hayan advertido una sociedad de riesgo inminente ante la violación de los derechos más íntimos e intrínsecos del ser humanos: el derecho de intimidad, derechos de privacidad y el derecho a la confidencialidad.

Con el uso de las nuevas tecnologías de la información y de la comunicación, las relaciones de las personas han tomado nuevos matices, las conversaciones se realizan por chats a través de aparatos electrónicos predominando el uso de teléfonos inteligentes, sin embargo esto ha traído otra manera de relacionarse con el mundo puede replicarse la vida de una persona con detalles que solo la persona conoce de sí mismo, estas actividades interactivas han permitido que se produzca una nueva sociedad informatizada y de relaciones interpersonales en la red de redes.

En este orden de ideas, el derecho a la intimidad personal está directamente vinculado a la dignidad de la persona, que es el valor y atributo exclusivo de los seres humanos que lo distingue de otros seres vivos, todo aquello que enaltece y embellece su vida, la información que sobre los ámbitos más reservados e íntimos de cada persona, pueda disponerse o utilizarse por terceros debe ser resguardada y protegida. La protección del derecho se manifiesta en este caso a través del control del interesado en relación con el acceso de otros a la información más personal, a los datos más reservados de cada uno (López y Plata, 1994: 277).

5- Principios y Retos ante la Vigilancia y el Espionaje

Estos principios son una propuesta a los Estados, que deberían tenerlos en cuenta siempre que quieran intervenir comunicaciones personales, y se basan en principios ya existentes en la legislación actual como la legalidad, la legitimidad, la necesidad, la idoneidad, la proporcionalidad, la autoridad judicial competente y el debido proceso. A éstos se les añaden otros principios menos comunes pero igualmente importantes y amparados por la legislación sobre derechos humanos, como:

- el principio de notificación al usuario (de que sus comunicaciones están siendo interceptadas),
- la transparencia (publicando datos de intercepciones, solicitudes a terceros, los procedimientos utilizados, etc.),
- la supervisión pública (esencial para la rendición de cuentas y el control democrático del estado),
- la integridad de comunicaciones y sistemas (incluyendo la no obligación de identificarse para utilizar determinados servicios),
- las garantías en los procesos de cooperación internacional (con tratados bilaterales, respeto por el principio de doble incriminación y aplicando la normativa más estricta en caso de disparidad) y, finalmente,
- las garantías contra el acceso ilegítimo, que incluyan sanciones penales y civiles por la vulneración de la privacidad y protección para los denunciantes de los casos de incumplimiento de estos principios (como Bradley Manning y Edward Snowden).

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

- La consolidación de estos principios proporcionaría cobertura legal a la denuncia de abusos y mala praxis por parte de organismos oficiales, protegiendo a la vez a denunciantes y periodistas.
- Que estos principios sean aplicables a los procesos de vigilancia evidencia que el debate sobre el espionaje va mucho más allá de las capacidades tecnológicas. La posibilidad de vigilar remotamente y generar archivos con datos personales (entradas y visitas a internet, llamadas telefónicas, interacción en redes sociales, matrículas de automóviles, acceso a transportes públicos con tarjetas inteligentes, control de huella dactilar en determinados accesos, etc.) en un mundo globalizado obliga a replantear cuáles son los límites físicos y legales de la privacidad y del derecho a la intimidad**.** Además, el intercambio rutinario de datos entre entes públicos y privados ya no es sólo de arriba abajo ni se dirige a sospechosos, los flujos de vigilancia son tan verticales como horizontales.

Los retos tecnológicos del siglo XXI, pues, son también retos legales, éticos y de derechos humanos con nuevos principios que aborden temas relacionados con la filosofía del derecho, la ética del comercio de datos personales, los límites del estado y las fronteras de la intimidad.

6- Principio de Proporcionalidad aplicado al Derecho a la Comunicación en Entornos Digitales y la Seguridad de Estado. Algunas Aproximaciones a sus Límites.

Recientemente se han producido sentencias que han ordenado la suspensión temporal de servidores de corporaciones trasnacionales en el área de la comunicación y la conexión en red como es el uso de la aplicación *whatsapp* por motivos de investigación penal, para citar la sentencia más emblemática en América Latina producida por la Primera Corte Penal de Sao Bernardo do Campo en Brasil, la cual ordenó la suspensión del servicio temporal, el cual surgió luego que la propia empresa no acatará la decisión en un primer momento, dejando desconectado del servicio de comunicación en red a millones de personas que son usuarios en el Brasil y que según el cuadro demostrativo en este artículo es el preferido de la población activa en red en un 93%. Este impacto ante la sociedad brasileña, demostró que no solamente es una herramienta de interconexión de entretenimiento sino que también es usado por ejemplo en médicos y pacientes que se comunican para atender requerimientos en el área de la salud y tratamientos.

La sentencia fue suspendida luego por órdenes de la Corte, sin embargo, se hace necesario analizar el impacto de la sentencia en cuanto a cuál fue la motivación de la misma. Una conceptualización esbozada por la investigadora sugiere que la sentencia es la producción intelectiva del juez aplicando el ordenamiento jurídico, principios de derecho, jurisprudencia, máximas de experiencia, para dar respuesta al caso concreto y la misma debe responder a la justicia como máximo valor. Ahora bien, la decisión de la sentencia *in comento*, no se corresponde a todas luces al Principio de Proporcionalidad, el cual viene a equilibrar derechos.

En este sentido, se considera necesario explicar cómo opera este principio el cual es aplicado en el Derecho Penal ante la aplicación de las penas, puede en los

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

demás casos en concreto ser un principio de aplicación necesaria que va a permitir decisiones más justas. Al respecto, Carbonell, 2010, afirma que el principio de proporcionalidad se vuelve relevante si aceptamos que no existen derechos absolutos, sino que cada derecho se enfrenta a la posibilidad de ser limitado. La cuestión que interesa entonces es de qué manera y con qué requisitos se pueden limitar los derechos.

El discurso sobre el principio de proporcionalidad no empata ni de lejos con el discurso conservador que quiere ver siempre limitados a los derechos fundamentales; por el contrario, se trata de una técnica de interpretación cuyo objetivo es tutelarlos de mejor manera, expandiendo tanto como sea posible su ámbito de protección, pero haciendo que todos los derechos sean compatibles entre ellos, en la medida en que sea posible, el principio de proporcionalidad constituye hoy en día quizá el más conocido y el más recurrente "límite de los límites" a los derechos fundamentales y en esa medida supone una barrera frente a intromisiones indebidas en el ámbito de los propios derechos.

Siendo el Principio de Proporcionalidad una herramienta hermenéutica necesaria para la protección de derechos fundamentales, las Constituciones de América Latina contemplan este Principio como principio rector, sin embargo, su no aplicación práctica en la sentencia referida deja mucho que decir. Los principios fundamentales se enfrentan a grandes dificultades ante regímenes autoritarios y autocráticos, sin embargo, se observa que en Estados Democráticos también hay puntos de quiebre en la hilación que debe existir entre las cartas fundamentales como texto político constitucional y la promulgación y protección en tanto de los derechos humanos. Esto se produce en sentencias proferidas por instancias inclusive superiores que contienen crasos errores de interpretación carentes inclusive de razonamientos lógicos.

Desde una perspectiva crítica considera la investigadora que no puede una sentencia ir en detrimento de derechos colectivos por un derecho individual sin una justa y equilibrada relación entre ambos derechos si a su vez se contraponen. Como se ha referido en esta investigación los derechos a la información y comunicación así como a la protección de la información generada en entornos digitales debe gozar de la misma protección jurídica dentro del marco normativo dando respuesta a los cambios vertiginosos de la era digital.

Existe en esta sociedad de riesgo grandes desafíos como el tema de la seguridad en espacios digitales comunicacionales y se ve vulnerado ante las nuevas formas en que los Estados utilizan la vigilancia de estos espacios, el punto es delimitar hasta donde aplicando el principio de proporcionalidad se deben intervenir las comunicaciones sin afectar masivamente a toda una población activa en redes, debe pues en este caso los jueces como operadores de justicia ser cuidadosos en las medidas dictadas para el aseguramiento de decisiones que también vendrían a ser justas. Cabe preguntarse ¿Cuáles serían las consecuencias que se producirían de no dictar una decisión que preventivamente va a beneficiar al colectivo, a la sociedad en su conjunto? La respuesta es no impartir justicia y la misma debe ir perfilada en el principio de proporcionalidad, el cual va a servir de herramienta efectiva para equilibrar y limitar temas como la seguridad y resguardo de información, comunicaciones privadas, y el acceso libre a la información y a la participación activa en la comunicación en redes.

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

Por su parte, el Estado Democrático en el ejercicio de la soberanía debe crear las condiciones de seguridad para el resguardo y protección de sus ciudadanos y ciudadanas en entornos digitales, se presenta la problemática que los mismos traspasan fronteras por el efecto de la globalización en las comunicaciones, sabiendo que las grandes corporaciones trasnacionales tienen sus centros de almacenamiento de datos en los Estados Unidos, donde están recolectados mensajes de correos electrónicos, chats en redes sociales, contenidos de videos por *youtube, instagram*, Skype, por mencionar algunos.

Al bloquearse las aplicaciones que interconectan a millones de personas en el mundo se está causando un perjuicio que se vuelve no cuantificable desde el médico que no puede recetar al paciente o la consulta de una emergencia, sabiendo que estos modos innovadores de comunicación operan en tiempo real dando respuesta efectiva ante los medios tradicionales de las comunicaciones. Es menester, en consecuencia de la masificación en el uso de la tecnología comunicacional en redes destacar que interconectan comunidades, universidades, escuelas superiores, secundarias, primarias, centro científicos y de investigación; bibliotecas públicas, centros culturales, museos, oficinas de correos y archivos; centros hospitalarios y sanitarios; departamentos de gobiernos locales, centrales, sitios web, todos los sectores de la economía y producción de bienes y servicios. El espacio de interconexión, se convierte en un espacio y dominio público, convirtiéndose el derecho a la tecnología, a internet una nueva escala en los derechos humanos que implica la herramienta necesaria para comunicarse efectivamente en esta era digital.

No puede una decisión emanada por un juez-en el caso de la sentencia referida- desproveer a millones de personas usuarias de las redes de su derecho a la comunicación y a la información, debe en consecuencia considerarse el respeto a los derechos humanos no sólo como una frase que sirve de bandera a las constituciones políticas de los estados, sino que debe ser práctica constante y permanente por parte del estado democrático la promoción y el respeto de los derechos humanos que como acertadamente indica Santos, 2002, en el marco de un Estado de Derecho el fundamento es un Estado de Derechos Humanos.

Conclusiones

Las comunicaciones producidas en contextos de interconexión traen consigo nuevos desafíos para los Derechos Humanos en especial el derecho a la información y a la comunicación y un nuevo derecho derivado de la comunicación es el derecho a la tecnología de la comunicación, debe en este sentido garantizarse el pleno ejercicio de estos derechos en la red mediante los cuales la libertad de expresión, de informarse, implica también la libertad de opinión y de responsabilidad por lo expresado así como la confidencialidad y resguardo de la vida privada. Los nuevos desafíos en materia de seguridad y confianza deben ser temas prioritarios para los Estados a través de instrumentos jurídicos y propuestas de organismos nacionales e internacionales en el abordaje de la vigilancia indiscriminada de las comunicaciones, debe en este sentido considerarse como tal violación de derechos humanos la intercepción y apropiación de las comunicaciones privadas.

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

Las revelaciones de Edward Snowden abrieron el debate y la mirada internacional hacia el reconocimiento de un aparato mundial de espionaje, en tanto los organismos de Derechos Humanos advierten el peligro de Estados que se transforman en vigilantes omnipresentes. Junto con las revelaciones, Snowden escribió un documento, llamado *Manifiesto pro privacidad*, y firmado por ciudadanos de todo el mundo, quedaba demostrado así que existía apoyo global para la protección de la privacidad, por todos estos acontecimientos puede decirse que en 2013 el mundo tomó conciencia de que la vigilancia digital por los gobiernos del mundo no conoce límites. El debate sobre las restricciones de los poderes estatales para vigilar las comunicaciones de los ciudadanos y para almacenar sus datos, dentro de la sociedad civil se abre a partir de las revelaciones de Snowden, violando los derechos humanos a la privacidad ajena en las comunicaciones exponiendo informaciones y comunicaciones privadas por el interés perverso del dominio hegemónico mundial, en reacción en el marco de la 24ta. Sesión del Consejo de Derechos Humanos de las Naciones Unidas.

Como se indicó la construcción de sociedades de información y comunicación debe dar prioridad a la dignidad humana, como desarrollo humano duradero de los derechos humanos por encima de la tecnología, la cual es una herramienta necesaria en las comunicaciones de hoy en día, no puede entonces superponer la tecnología a la concepción de dignidad humana que conlleva el ejercicio de todos los derechos humanos en el uso y aprovechamiento de las nuevas tecnologías de información y comunicación, deben estar al servicio de la humanidad y no debe a través de ellas vulnerarse derechos.

Un Estado de Derecho equivale a decir un Estado de Derechos Humanos, en tal sentido, la garantía a este derecho constituye la creación de políticas públicas eficaces en materia de seguridad de los ciudadanos y de la soberanía política y cibernética, por lo tanto la protección de estos derechos incluye el resguardo de datos personales sensibles como domicilio, estado de salud, tendencia política, preferencias sexuales, religión, relaciones con grupos determinados, la membresía en asociaciones, el derecho de asociarse, la información profesional, académica, familiar, los hobbies, facetas de la personalidad; las cuáles arrojan un perfil tipológico de la persona la cual la hace vulnerable en el uso de la información y de las comunicaciones privadas vigiladas.

Desde una perspectiva crítica considera la investigadora que no puede una sentencia ir en detrimento de derechos colectivos por un derecho individual sin una justa y equilibrada relación entre ambos derechos si a su vez se contraponen. Como se ha referido en esta investigación los derechos a la información y comunicación así como a la protección de la información generada en entornos digitales debe gozar de la misma protección jurídica dentro del marco normativo dando respuesta a los cambios vertiginosos de la era digital.

Referencias Bibliográficas

Asamblea Nacional Constituyente. Constitución de la República Bolivariana de Venezuela. 1999. Gaceta Oficial (Extraordinaria) Nº 5.453. Marzo 24, 2000.

Depósito Legal: PPX200602TR2436 / ISSN:1856-6936. Volumen 10 Edición No 2 – Año 2016

Assange, Julián. 2013. *Cypherpunks. Freedom and the future of the internet*. (La Libertad y el Futuro de Internet). Ediciones Trilce. Uruguay

Banco de Desarrollo de América Latina. 2014. Expansión de Infraestructura regional para la Interconexión de Tráfico en Internet en América Latina. Corporación Andina de Fomento.

Carbonell, Miguel.2010. El Principio de Proporcionalidad en el Estado Constitucional. Universidad Externado de Colombia.

Correa, Carlosy otros. Derechos Informático. Ediciones Depalma S.A. Buenos Aires. Argentina. 1987.

Indexmundi. Tabla Comparación de Países, Número de servidores Internet. Disponible en: http://www.indexmundi.com/g/r.aspx?v=140&l=es. Fecha de consulta: enero de 2016.

López, Vicente y Plaza, Carmen. 1994. El Defensor del Pueblo: Derecho, Tecnología de la Información y Libertades. En Revista Iberoamericana de Derecho Informático, Informática y Derecho. España Editorial UNED.

Santos, Boaventura, 2002. Hacia una Concepción Multicultural de los Derechos Humanos. Otras miradas de justicia. Revista El Otro Derecho, Número 28 Julio de 2002. ILSA. Bogotá D.C., Colombia.