Evaluación Legal de la utilización de la Inspección Profunda de Paquetes o DPI en la redes de telecomunicaciones en Colombia

Edwin José Basto Maldonado, Octavio J. Salcedo Parra

ejbastom@unal.edu.co, octavionetworking@gmail.com

Universidad Nacional de Colombia

Resumen. *La Inspección Profunda de Paquetes o DPI ha generado debates y expectativas en cuanto a su funcionamiento. Si tomamos como base que los operadores e ISP interfieren la red de servicios con plataformas y equipos capaz de analizar todo el "tráfico" de los suscriptores hacia Internet, este hecho ha suscitado todo tipo de controversias en cuanto a quién o qué ente regula que los datos interferidos y analizados no se hagan públicos, conserven su integridad y no se comercialicen en ningún modo, respetando la privacidad de los usuarios. El presente artículo realiza una evaluación de los procedimientos legales y el marco jurídico cuyo alcance es la protección de los datos y la información, ante la utilización de la Inspección Profunda de Paquetes o DPI por parte de los operadores y proveedores de servicio en Colombia. Posteriormente se analiza la composición de Internet y los entes encargados de regular los servicios ofrecidos en la red. Por último, se concluyen una serie de sugerencias y recomendaciones hacia los actores que inciden directamente en la inspección profunda de paquetes, referenciando casos reales, leyes y modelos que rigen en otros países, como Estados Unidos y Canadá, y tomando en cuenta las recomendaciones de la ITU al respecto, con el fin de ayudar de la mejor forma a la implantación de la tecnología DPI en los proveedores de servicio.*

Palabras claves: DPI, Firewall, Habeas Data, ISP, Petabyte.

Abstract: *Deep Packet Inspection technology has generated such recent debates and expectations for their operation, if we take as a basis the operators and ISPs interfering network service platforms and equipment capable of analyzing all traffic to Internet subscribers, this fact has led to all kinds of disputes as to who or what agency regulates that interfered and analyzed data are not made public, maintain their integrity and are not marketed in any way, respecting the privacy of users. This article provides an assessment of the legal proceedings and legal framework whose scope is the protection of data and information , with the use of deep packet inspection or DPI, by operators and service providers in Colombia, subsequent analyzes the composition of the Internet and the authorities responsible for regulating the services offered in the network, and finally a number of suggestions and recommendations to the actors that directly affect the deep packet inspection will conclude by referencing real cases, laws and models governing other countries like the U.S. and Canada, and taking into account the recommendations of the ITU in this regard, to help in the best way to implement the DPI technology in the service providers .*

Keywords: DPI, Firewall, Habeas Data, ISP, Petabyte.

1. Introducción

Sin lugar a dudas la protección y seguridad de la información ha sido, durante los últimos años, el punto clave dentro de lo que podríamos llamar la politización de servicios ofrecidos por los proveedores e ISP. Por otro lado, el nacimiento de nuevas tecnologías cada vez compromete más esta seguridad, y se hace necesario tener claro las leyes que nos cobijan como usuarios y consumidores.

La adopción de tecnologías como la "*Inspección Profunda de Paquetes",* en adelante DPI por sus siglas en Inglés, entre los operadores de servicio, ha generado desconfianza y desatado controversia debido a que la acción que se ejecuta en cierto modo atenta contra las leyes de protección de información de los usuarios. Imagine pensar que cada vez que se envía un mail con información de carácter urgente y secreta, esta información personal y delicada pasa de forma obligada por su operador del servicio. Ahora piense que su tráfico es como una caja que es abierta y analizada, generando quizás reportes o tendencias de uso sobre usted y su información. El presente documento muestra los dos lados de DPI, en cuanto a los peligros que representa para usuarios y consumidores de Internet la *Inspección Profunda de Paquetes*, y aquellas ventajas como la optimización y seguridad de las redes, que ofrece la tecnología en la operación de servicios por parte de los proveedores. Todo expuesto dentro de un marco legal y dentro del contexto de las leyes en Colombia y Latinoamérica, tomando como referencias a Estados Unidos, Canadá. Posteriormente a esto, se expone un apartado que explica algunos de los entes internacionales que participan en la "Gobernanza de Internet", y, finalmente, un apartado de conclusiones donde se expone la manera en que esta tecnología pudiera ser controlada y aplicable, involucrando al sector gobierno, fundaciones, academia, entidades públicas y privadas.

2. Qué es y qué ofrece DPI

La inspección profunda de paquetes o DPI es la interceptación de las comunicaciones en cualquier punto de la red de datos que no sea el final del canal, analizando el tráfico y la carga útil que corre por allí con algún propósito en específico. El escenario ideal se da cuando un usuario realiza solicitudes a un servidor para acceder a determinado servicio dentro o fuera de la nube de Internet. Precisamente, la inspección se realiza en esta línea y puede arrojar datos valiosos y privados acerca del trafico de cada usuario o suscriptor que es interceptado.

La Figura 1 muestra un ejemplo claro de cómo funciona DPI al interferir, analizar y devolver la información en un servicio de correo desde un usuario hasta su destino.

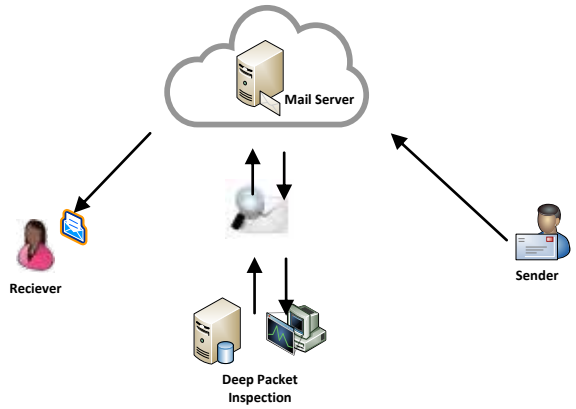

Figura 1. Ejemplo de Inspección Profunda de Paquetes o DPI. Fuente, Propia.

Por otro lado, es importante señalar que la tecnología de inspección profunda de paquetes fue desarrollada también para gestionar y optimizar la red, defenderla y protegerla de ataques, al igual que aplicar políticas de servicio de los operadores hacia cada suscriptor. Los operadores de servicios de internet justifican la utilización de DPI en la necesidad de gestionar sus redes debido al rápido crecimiento de estas (móviles y fijas), y al aumento en la utilización de su ancho de banda proporcional al incremento de usuarios y suscriptores, tal y como se aprecia en un informe generado por el Mintic[29], en el que se consolidan datos relevantes respecto al uso de las Tics en Colombia, incluyendo los medios de comunicación utilizados, número de usuarios, entre otros. El informe corresponde al cuarto y último trimestre del 2013 y fue divulgado en marzo de 2014.

En la figura 2, se ve claramente como existe un incremento de los usuarios identificados como "Suscriptores" aquellos que mantienen un contrato de servicios mensual vigente con su operador. El incremento promedio es de 677.292,5 usuarios nuevos por cada trimestre, una cifra bastante alta y que justifica lo antes expuesto.

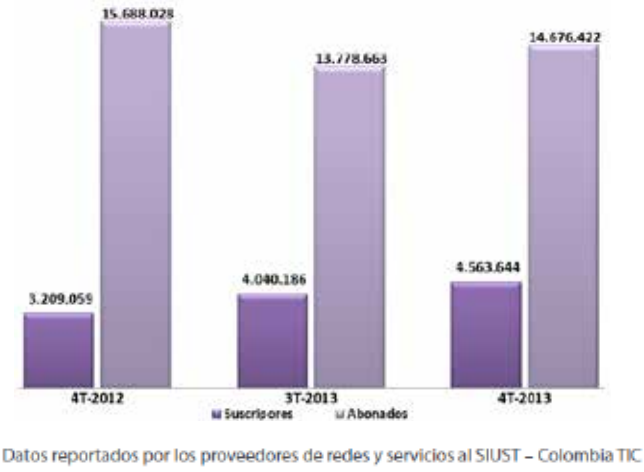

Figura 2. Internet Móvil, Subscritores Vs. Abonados. Fuente, Boletín trimestral de las TIC - Cifras cuarto trimestre de 2013.

A este aumento substancial de usuarios, se debe agregar el acceso a los diferentes contenidos, especialmente los relacionados con multimedia que han ocasionado un uso abusivo del ancho de banda, que es donde realmente las redes de datos se ven más afectadas. Bajo este escenario, se puede utilizar DPI, como tecnología para crear y sostener políticas de servicio en la red, implementando soluciones, como la de restringir servicios donde la velocidad de archivos sea constante y de mayor demanda, servicios Torrents, Streaming, protocolos PPP y otros. Se pueden limitar para controlar el uso y la capacidad de los canales de internet, garantizando a otros usuarios con quienes también se comparte el canal los mismos derechos de acceso a la red.

Pero, ¿por qué DPI puede realizar esta acción, y un simple Firewall no? Un Firewall realiza una búsqueda / bloqueo sobre puertos conocidos y esto a veces no resulta eficaz arrojando poca información al ISP sobre los servicios consumidos. Es decir, mirando sólo la dirección IP no se puede identificar el tráfico que se quiere filtrar, por lo tanto se necesita mirar más allá de los encabezados de datos y es aquí donde DPI muestra sus ventajas. Por ejemplo, en aplicaciones, como los navegadores web que utilizan constantemente el puerto 80, se necesitarían muchos más datos en la información que circula para saber qué contenido permitir y cuál bloquear.

¿Qué cantidad de tráfico HTTP es vídeo? Ellacoya, recientemente, completó un estudio de uso de banda ancha y dice que el 20 por ciento de todo el tráfico web es realmente sólo de secuencias de vídeo de YouTube. Según una publicación de Bret Swason para el Wall Street Journal en 2007[30], cada año el contenido original en los canales de radio, televisión por cable y de difusión en el mundo asciende a unos 75 petabytes de datos. Por ejemplo, un cambio de alta definición de videoclips por usuarios de YouTube inundaría Internet con suficientes datos a más del doble del tráfico de todo el ciberespacio, y YouTube es sólo una empresa de muchas con una aplicación de contenidos multimedia. Dado el crecimiento de las cámaras de vídeo de todo el mundo, pronto podríamos producir hasta 5 exabytes de vídeo amateur anualmente. Las actualizaciones de alta definición estarán en el tiempo aumentar ese número por otro orden de magnitud a unos 50 exabytes o más, o 10 veces la corriente de tráfico anual de Internet. Sin duda alguna, estas cifras preocupan y dan un alcance de los anchos de banda que se deben manejar de parte de un ISP y lo importante que es para ellos administrar y optimizar este recurso.

DPI también ofrece otras características, la primera de ellas es la inyección de publicidad o "Ad Injection", es decir, anuncios de oferta y demanda de productos y servicios orientados a los perfiles de consumo de los usuarios, perfiles que únicamente conocen los proveedores e ISP, pues es por allí por donde circula nuestro tráfico. El hecho de conocer la orientación de consumo de cada suscriptor de por sí ya es una situación

[29] Boletín trimestral de las TIC - Cifras cuarto trimestre de 2013, Mintic, http://colombiatic.mintic.gov.co/602/w3-article-5550.html.

[30] Swanson, Bret. "The Coming Exaflood." Wall Street Journal, 20 January 2007.

crítica, pero lo realmente responsable por parte del ISP es mantener esa información como privada y no divulgarla, ni comercializarla bajo ninguna circunstancia. De no hacer esto, el proveedor incurriría en un delito informático, e iría en contra de las leyes recientemente aprobadas a favor de la protección de datos que se analizarán en el siguiente apartado.

La otra ventaja de la utilización de DPI en los operadores es el de Cumplimiento de Derechos de Autor, o "*Copyright enforcement*", debido a que muchos usuarios comparten a través de sus redes material P2P con copyright, razón por la cual las compañías de contenidos multimedia como música y vídeo han presionado a los ISP a detectar y filtrar este tipo de contenido bloqueando el acceso a este servicio.

Por último, un punto más juega a favor de los operadores y proveedores de servicio ya que esta tecnología también ayuda a prevenir los problemas de seguridad asociados con la integridad de la información, siendo capaz de controlar y repeler ataques informáticos como la intrusión, los virus, el malware, y otros. Esta es una de las bases fuerte en la que los operadores vuelven a justificar la inspección y el análisis de la información haciéndola necesaria y aceptable de parte de los usuarios. Por ejemplo, un estudio de Adalip Corp, revela que el 97,5% de los colombianos han sufrido incidentes referentes a delitos informáticos como phishing, robo de dinero e información, entre otros.

Las implementaciones reales de DPI no tienen que poner en práctica todas las funciones anteriormente mencionadas, su uso solo podría ser limitado a el filtrado de contenido que nadie quiere en ningún caso (virus y otro malware). Su utilización también puede estar restringida a la gestión de ancho de banda en función de las necesidades prioritarias de las diferentes aplicaciones. A continuación se muestra una tabla que resume los distintos propósitos con los que se puede implantar DPI dentro de las redes, de qué forma se hacía antes de que la tecnología apareciera, y cómo DPI lo ha remplazado.

Purpose	Old	New	Drivers
lawful interception, surveillance	TCPdump, Wireshark, dsniff etc. (store & analyze)	DPI (analyze packets and make decisions in real-time)	police, intelligence community
content regulation	blocking based on DNS, IP#, URL	hash-based blocking or surveillance	efforts against hate-speech, child-porn, political censorship
copyright enforcement	DRM Lawsuits	hash-based filtering	content industry
bandwidth management	TCP congestion management, QoS	application-based routing	ISPs: last mile over-subscription, P2P and video traffic
subscriber management	pay per minute, pay per volume	differentiated services and pricing	ISPs: heterogenous user behaviour and user needs in context of bandwidth scarcity
network security	stateful firewalls, asynchronous monitoring (TCPDump etc.)	content-based real-time monitoring	corporate network operators; anti-spam and malware efforts by ISPs
vertical integration	product tying	block or discriminate competing services	video on demand, integrated phone & internet providers, triple play.
behavioural-based advertising	cookies (website owners)	ad injection	ISPs, ad networks

Tabla 1. Use Cases and Drivers for DPI. **Fuente,** Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection, International Studies Annual Convention, New York City, 15-18 February 2009, Ralf Bendrath.

Recientemente, la UIT presentó ante la Asamblea Mundial de Normalización de las Telecomunicaciones AMNT, en la Conferencia de la UIT Mundial de Telecomunicaciones Internacionales (CMTI) celebrada en Dubái en noviembre de 2012, la recomendación ITU-T Y.2770 *"Requerimientos para la inspección profunda de paquetes en redes de siguiente generación"*[31]. En la que fue aprobada y se resolvió la duda si la inspección iba enfocada a los contenidos de usuario. Descartándose esta idea la recomendación se enfoca en la identificación de las aplicaciones que se utilizan en la inspección, garantizando de esta forma el secreto de la correspondencia, pues esta norma no permite el acceso a la información privada. Éstas son solo recomendaciones que la ITU ha diseñado para frenar un poco el gasto incremental con el que los operadores tienen que expandir su infraestructura, y busca mejorar las calidades de servicio y experiencia (QoS & QoE) en los usuarios, al tiempo que optimizar las redes y el consumo continuo y creciente de ancho de banda.

La recomendación UIT -T Y.2770 trata de definir un estándar internacional para la inspección profunda de paquetes DPI, y se describen los requisitos técnicos de identificación y gestión de las aplicaciones de red a través de protocolos, puertos y aplicaciones. UIT -T Y.2770. Afirma, además en su ámbito de aplicación, que los ejecutores y los usuarios de las técnicas descritas deberán cumplir con todas las leyes, reglamentos y políticas nacionales y regionales aplicables. La norma también hace referencia a las reglas complementarias que trabajan en arquitecturas inteligentes de gestión del tráfico, en el que DPI juega un papel importante.

Así, DPI presenta una solución de gestión de tráfico para ayudar a los ISP, al contender con volúmenes de información de subida a un ritmo exponencial, y se ha convertido en un atractivo para los operadores gracias al uso que tiene frente a varios problemas en la gobernanza de Internet, la optimización de los servicios y la monetización de éstos.

3. Alcance Legislativo en COLOMBIA

Para empezar a hablar de la inspección de un flujo de tráfico donde, es claro, viaja información crítica acerca de los usuarios y suscriptores, es necesario colocarnos en un marco legal local es decir en Colombia, qué leyes existen y cómo está amparada esta tecnología.

El alcance legal en Colombia nace de la constitución Política de 1991, con el artículo 15, el cual textualmente dice *"La Correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptados o registradas mediante orden judicial, en los casos y con las formalidades que establezca la Ley"*[32].

Posterior a este artículo fundamental de la ley, se desarrollaron otras leyes con el fin de proteger la integridad de los datos y sus dueños entre ellas la ley 1273 de 2009 y la 581 de 2012, esta última la más

[31] Recomendación UIT-T Y.2770, Requisitos para la inspección detallada de paquetes en las redes de la próxima generación, http://www.itu.int/rec/T-REC-Y.2770

[32] Constitución Política de Colombia, Artículo 15, Año 1991.

conocida de todas como "Ley de Datos Personales", la cual tiene define su objeto en el artículo 1[33] "*La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política…*" y donde se vuelve a citar el artículo 15 de la carta magna en Colombia. A todas éstas, se añade la ley 1377 de 2013 la cual establece parcialmente la Ley de Habeas Data, el cual se analizará en profundidad en el siguiente apartado.

En cuanto a leyes acerca de interceptaciones en Colombia se cuenta con el decreto 1704 de 2012, el cual expidió el Ministerio de las Tecnologías de Información y Comunicaciones MINTIC, donde se cita textualmente: "*…disposiciones a cumplirse por los proveedores de redes y servicios de telecomunicaciones con el objeto de apoyar de manera eficaz y oportuna la labor de interceptación de comunicaciones .que adelanten las autoridades competentes*", algo así como un procedimiento oficial para realizar las interceptaciones que empiezan con autorización previa de la Fiscalía General de la Nación, y que en pos de la seguridad definen la interceptación de comunicaciones como un mecanismo de seguridad pública, punto crucial e importante para entender el marco legal en el que se desenvuelve la inspección profunda de paquetes en Colombia, *"…mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la Ley.*" Artículo 1, Decreto 1704 de agosto de 2012[34].

Como delito, se debe indicar que la inspección profunda de paquetes no debe caer en el de interceptación de datos, el cual señala, "*El que, sin orden judicial previa, intercepte datos en su origen, destino o en el interior de un sistema informáticos, o en las emisiones electromagnéticas proveniente de un sistema informático que los transporte, incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses*"[35].

Todo lo anterior hace que el panorama no sea muy claro respecto a que si existen todas estas normas, por qué los ISP ejecutan tal análisis, escudriñando nuestra información y sin nuestra previa autorización. Lo más preocupante es que los entes gubernamentales no se pronuncian de ningún modo. Afortunadamente, para los usuarios las leyes existen en Colombia, pero aunque públicas son de poco conocimiento. El problema grave es que no existen políticas ni entes gubernamentales que hagan cumplir las normas, y este artículo señala que es deber del Estado garantizar la seguridad del país y sus habitantes. Aunque la seguridad de una nación es prioridad, ninguna acción que pretenda proteger ésta, deberá estar en contra de los derechos fundamentales de las personas, vulnerar su privacidad y mucho menos actuar al margen de la ley.

4. Habeas Data en COLOMBIA y Latinoamérica

El Habeas Data, como acción constitucional en los países de Latinoamérica consiste en el derecho de cualquier persona en solicitar, modificar o eliminar la información que exista sobre sí, en los bancos o registros de datos públicos o privados.

Como se mencionó en el apartado anterior, bajo la Ley 1377 de 2013, en Colombia se reglamenta parcialmente el "Habeas Data", cuyo valor reside en señalar 6 capítulos, y 28 artículos en donde, de forma concisa, aborda el tema de la protección de datos personales. Dentro de la ley quedan señalados las Disposiciones Generales, Autorización, Políticas de Tratamiento, Ejercicio de los derechos de los titulares, Transferencias y transmisiones internacionales de datos personales, Responsabilidad demostrada frente al tratamiento de datos personales.

Según un informe de la revista colombiana Dinero, especializada en temas económicos del año 2013[36] el mismo año en que la ley vio la luz, se han extraído 7 puntos de los anteriores 6 capítulos, que se consideran vitales para entender el contexto en el que los titulares de la información se encuentran amparados por la presente ley.

- Los titulares de la información tienen derecho a encontrar de manera ágil y sencilla la información suministrada por ellos y que se encuentra bajo la administración de otros.
- Los ciudadanos podrán consultar de manera gratuita sus datos personales, al menos una vez por mes.
- En caso de no recordar haberse inscrito en una base de datos, el dueño de la información podrá solicitar una prueba de la autorización inicial por la que fue inscrito.
- El propietario de los datos tiene derecho a que se le describa para qué y cómo será utilizada su información.
- También se tendrá derecho a la actualización, rectificación y supresión cuando el titular lo considere conveniente (en cualquier momento).
- Todo administrador de la información deberá designar una persona o área que asuma la función de protección de datos personales, la cual también debe dar trámite a las solicitudes de los ciudadanos.
- En caso de sentir que alguno de éstos derechos no son atendidos o cumplidos, el dueño de la información podrá recurrir al ente de control para radicar una queja formalmente.

En Latinoamérica este derecho constitucional ha sido adoptado en varios países, entre los cuales se encuentran, Argentina, Uruguay, Brasil, entre otros, una tabla detallada con las leyes, y fecha de publicación se muestra a continuación.

[33] Congreso de Colombia, Ley estatutaria 1581 de 2012.
[34] MINTIC, Decreto 1704 de Agosto de 2012
[35] Interceptación de datos informáticos, Artículo 269c, Ley 599 de 2000.
[36] Sus derechos en el Habeas Data, http://www.dinero.com/Imprimir/181020, 2013.

País	Legislación	Fecha
Argentina	Ley 25.326, Ley de Protección de los Datos Personales.	Octubre de 2000
Bolivia	Ley 2631 Art. 23 reformada en 2004 - Constitución Política del Estado Arts. 103 y 131.	Abril de 2004
Brasil	LEI Nº 9.507, Regula o direito de acesso a informaí§íµes e disciplina o rito processual do habeas data.	Noviembre de 1997
Chile	Artículo 12 de la ley 19.628, Protección de Datos de Carácter Personal.	Agosto de 1999
Colombia	Ley 1581, Ley de Protección de Datos.	Abril de 2012
México	Ley federal de transparencia y acceso a la información pública gubernamental.	Junio de 2006
Nicaragua	Ley de Acceso a la Información, Ley de Protección de datos personales y su decreto reglamentario.	Marzo de 2012
Panama	Ley 6, Que dicta normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones.	Enero de 2002
Paraguay	Artículo 135 del Habeas Data, Constitución Nacional.	Junio de 1992
Perú	Ley 29733, Ley de Protección de datos Personales.	Junio de 2011
Uruguay	Leyes 18.331 y 18.381.	Noviembre de 2008
Guatemala	Ley de Acceso a la Información Pública, decreto 57-2008.	2008

Tabla 2. Leyes de Protección de Datos en Latinoamérica.. **Fuente,** Habeas Data Org. www.habeasdata.org, **Modificado:** Edwin José Basto.

Todo lo explicado anteriormente tiene como fin hacer respetar y prevalecer los derechos a la protección de la información, consolidado en los "*13 Principios Internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones*", instituido por las Naciones Unidas, y que cuenta con una traducción al español con fecha de julio de 2013[37].

5. Alcance legislativo en Estados Unidos y Canadá

a. Estados Unidos

Estados Unidos se rige por varias normas que garantizan la protección y seguridad de la información y de sus habitantes, al tiempo que existe esto también las leyes y los entes gubernamentales tratan de garantizar la seguridad de la nación, aunque bajo este lema algunas veces se pase por encima de los derechos civiles.

Para empezar, tenemos la Cuarta Enmienda de la constitución de los Estados Unidos, la cual cita "*El derecho de toda persona a tener seguridad de que su casa, persona, documentos y efectos personales no serán inspeccionados o decomisados sin una razón justificada...*"[38]. Por otra, parte Estados Unidos también cuenta con la Ley de Vigilancia de Inteligencia Extranjera FISA, la cual establece procedimientos para el monitoreo y vigilancia física y electrónica, e interceptación y recolección de información local o extranjera, la cual represente una amenaza de espionaje o terrorismo. Sin embargo, en Estados Unidos se debe cumplir con la ley de interceptación Legal "Communications Assistance to Law Enforcement Act" CALEA, para ejecutar estas acciones, que comenzaron su vida como una actualización de las leyes de escuchas telefónicas tradicionales. Ahora se ha extendido a los operadores de VoIP y proveedores de Internet, que necesitan una manera de captar, archivar y presentar a las autoridades cualquier información que escucha telefónica solicitada en una orden judicial.

Posterior a esto, en el año 2006 la Comisión Federal de Comunicaciones FCC, adoptó las reglas del Título 47 Subparte Z[39], que deben cumplir los proveedores de servicio de telecomunicaciones, en Estados Unidos para proceder con la inspección profunda de paquetes.

Partiendo de estos derechos constitucionales y las entidades a cargo de hacer cumplir las leyes, se creería que Estados Unidos es un país donde la protección de datos no es vulnerada. Sin embargo, a continuación se mencionan dos de los varios casos ya sonados en los últimos años. En cuanto a la interceptación de datos e infiltración de información, donde queda claro que a pesar de las leyes los organismos de seguridad encargados siempre juegan a favor del gobierno por encima de los derechos primordiales de las personas.

Es bien sabido por todos que Estados Unidos es el Estado que lidera y está a la cabeza en temas de regulación y organización de todos los asuntos que tienen que ver con Internet, pero qué sucede cuando toda esta política es derrumbada debido al exceso de poder. Un ejemplo claro viene de la NSA, Agencia Nacional de Seguridad de Estados Unidos, la cual durante mucho tiempo se dedicó a realizar filtraciones e interceptaciones en varios sectores públicos y privados no solo de Estados Unidos sino también en países de Europa y América Latina, que gracias a las revelaciones de un exagente de la CIA, llamado Edward Snowden, a los principales diarios del mundo, como The Guardian, The Washington Post, y Spiegel se pudieron conocer.

El segundo caso tiene que ver con la NSA y la cooperación de operadores como AT&T, quienes han utilizado la tecnología de inspección profunda de paquetes para hacer más inteligente la supervisión, clasificación y envío del tráfico de Internet. El caso sucedió en un área de San Francisco donde el tráfico asociado con la red troncal común de AT&T fue separado en dos fibras, dividiendo la señal de manera equitativa 50/50. Una de las fibras fue derivada a un sitio seguro que contenía analizadores de tráfico y servidores dispuestos por a la NSA, mientras que la otra fibra fue llevada al equipo de conmutación de AT&T.

[37] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones https://es.necessaryandproportionate.org/text

[38] La Constitución de los Estados Unidos de América 1787, http://www.archives.gov/espanol/constitucion.html

[39] Rules & Regulations for Title 47, http://www.fcc.gov/

Este hecho fue respaldado por un técnico trabajador de AT&T, de nombre Mark Klein, que según las declaraciones publicadas en la página de "Electronic Forontier Foundation"[40], denunció la captura de tráfico en un cuarto oculto situado en la instalación de AT&T en Folson Street, California. Klein también revela detalles de los equipos específicamente instalados y utilizados en este cuarto secreto, uno de ellos una máquina denominada "Narus Semantic Traffic Analyzer", una poderosa herramienta utilizada para la inspección profunda de paquetes o DPI, donde cada máquina con Narus fue capaz de analizar 10 Gigabits de paquetes IP, y alrededor de 2.5 Gigabits de tráfico web incluido e-mail por segundo. Adicionalmente, Narus es capaz de reconstruir los paquetes interceptados y enviar la información a su central para su posterior almacenamiento y análisis[41].

Esta acción, sin lugar a dudas, dejó muy planteadas las políticas de interceptación utilizadas por el gobierno de los Estados Unidos, desencadenando un escenario de desconfianza en el que ningún ente público o privado externo a Estados Unidos quiere utilizar los servicios de IT ofrecidos por compañías estadounidenses, tanto como para llegar a la prohibición de usar cuentas de correo de Outlook en línea, Google y Yahoo. Obviamente, la desconfianza de los clientes y la posible pérdida de éstos, es una de las preocupaciones actuales y será un grave impacto en la industria estadounidense tal y como lo revela un estudio de la revista Forrester Research del 2013[42] en el que el mercado podría llegar a perder hasta 180 billones de dólares, un equivalente aproximado al 25% del mercado actual de IT en ese país.

La constante vigilancia de la NSA en los Estados Unidos y la presión gubernamental que existe luego de la situación del 9/11, prácticamente ha obligado a la mayoría de ISP a que cumplan la demanda del gobierno para instalar hardware o software de espionaje. Yahoo fue la única empresa que se opuso a la entrega de información, sin embargo en el año 2008 perdió la batalla ante el gobierno estadounidense con el argumento de que la seguridad Nacional estaba por encima de cualquier cosa.

Es decir que con estas acciones nos alejamos más de un internet global y podemos pensar en que cada gobierno se encargue de ofrecer servicios a sus territorios, sería algo similar al internet local que empezó a difundirse en 2013, cuando se supo de las interceptaciones de Angela Merkel, Canciller Alemana[43], y cuyo gobierno ha empezado a pensar en un internet Local.

Probablemente, una consecuencia final en un mediano plazo a todo esto será la "Independencia" de Internet, en la que cada país o región tendrá su propia red de servicios, aunque la independencia radica es ser libres y autómatas fuera de un mundo regulado y vigilado por Estados Unidos, el riesgo de este nuevo modelo sería que aquellas redes de servicios que surjan no permitan su interconexión con otras, lo que restaría al concepto de Internet como lo conocemos hoy una "Red de Redes".

Sin duda alguna la monopolización que tiene Estados Unidos sobre los entes regulatorios de los servicios que hoy ofrece internet, es la que más ha permitido que todas estas leyes se vulneren, y que no se respeten los derechos de privacidad, cuando el actor principal no sea Norteamérica, y se permita una interacción de todos a nivel mundial, la protección de la información y la regulación de los servicios será posible y mucho más fácil.

b. Canadá

En cuanto a la protección de los datos en Canadá, existe la Ley de Protección de Información Personal y Documentos Electrónicos PIPEDA[44], la cual se aplica a información personal a cargo de los ISP en el curso de la prestación de servicios de Internet a sus clientes, por tanto esta ley es una de las más importante, y requiere que haya un consentimiento informado y significativo para cualquier propósito que se tenga con la información.

Ahora bien, centrándonos en el papel de los entes reguladores ante la inspección profunda de paquetes, en el año 2009, la oficina del comisionado de privacidad de Canadá OPC, preparó un informe dirigido a la CRTC o Comisión Canadiense de Radio-Televisión y Telecomunicaciones, citando a diferentes comunidades académicas, privadas, y de investigación en la cual señalaba lo importante de la tecnología DPI y el impacto sobre lo usuarios en el país.

Desde noviembre de 2008 y como parte de los procesos de revisión, la CRTC inició un procedimiento público para revisar las prácticas de gestión del tráfico de Internet de los proveedores de servicios o ISP. Desde 6 julio hasta 14 julio 2009 la CRTC llevó a cabo 7 días de audiencias públicas para tal fin. La CRTC tomó declaración a los grupos de interés público de defensa, organizaciones de la industria, fabricantes de equipos y las tecnologías utilizadas para la gestión de redes, proveedores de Internet y los particulares interesados. Lo más relevante del documento preparado por la OPC y entregado a la CRTC en julio de 2009 se señala en el apartado 5, el cual indica "*El OPC reconoce que los proveedores de Internet dieron pruebas ante el Panel de Audiencia que DPI no se utiliza actualmente por los operadores para fines distintos de gestión de red. Los proveedores de Internet afirmaron la que información personal del cliente que se está manejando en las prácticas de gestión del tráfico de Internet (ITMP) como DPI, no está siendo utilizada para fines de marketing específicamente. En concreto los ISP alegaron que no se dedican a la publicidad dirigida o de comportamiento utilizando la información obtenida a través de DPI*".

El documento cita, finalmente, "*La comunicación de la OPC y la respuesta definitiva se realizan de acuerdo a*

[40] Public Unredacted Klein Declaration, https://www.eff.org/node/55051

[41] How the NSA's Domestic Spying Program Works, https://www.eff.org/nsa-spying/how-it-works

[42] Forrester Research, The Cost of PRISM Will Be Larger Than ITIF Projects, http://blogs.forrester.com

[43] Überwachungsskandal: NSA speicherte mehr als 300 Berichte über Merkel, http://www.spiegel.de

[44] Section 2 of PIPEDA provides that "personal information" means "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."

nuestro mandato legislativo para proteger los derechos a la privacidad de las personas, fomentar la comprensión pública de la vida privada, y promover la protección de la privacidad disponibles en Canadá. Ambas presentaciones OPC en este procedimiento se centran en las implicaciones de privacidad sobre los usos potenciales de inspección profunda de paquetes (DPI) y más en general la necesidad crucial -y cada vez mayor expectativa- de los canadienses que su información personal esté protegida en línea".[45]

Claramente, la posición del gobierno Canadiense a consideración de este autor es una de las más claras y objetivas, pues inicialmente cuenta con las leyes que regulan la protección de la información. Posteriormente, también existe un ente regulador que hace cumplir dicha ley, tal y como es el caso de Estados Unidos y propiamente Colombia, a diferencia que los entes de regulación Canadienses involucran diferentes comunidades para el estudio, análisis y posterior decisión en temas relevantes, en una posición muy transparente el gobierno deja claro que los operadores de servicio no está comercializando con la información personal de sus suscriptores, y a juzgar por las pautas y procedimientos que se describe en sus informes, se hace veraz y da tranquilidad a sus habitantes.

6. Gobernanza de Internet

Luego de tener referencias de dos grandes Estados y conocer la forma cómo abordan la discusión de temas tecnológicos, específicamente uno tan vital como DPI, entramos a definir términos como "Gobernanza de Internet", y entender qué papel juega dentro de los modelos de servicios jurídicos y tecnológicos. Se puede definir "Gobernanza" como todos aquellos temas relacionados con las aplicaciones, normas, reglas y principios que construyen y dan forma a Internet, y que permiten su evolución. Dentro de los actores y parte que conforman internet, tenemos el sector gobierno, entidades privadas, comunidades académicas, comunidades tecnológicas y sociedad civil. Pero quienes gobiernan Internet, repasemos muy rápido las principales organizaciones, y su función principal.

IANA, es la Autoridad para la Asignación de Números de Internet, responsable de la coordinación global de los protocolos de Raíz DNS, direccionamiento IP y otros recursos del Protocolo de Internet. *ICANN*, La Corporación de Internet para la Asignación de nombres y números de dominios, es una organización sin fines de lucro que opera a nivel de asignar espacio de direcciones numéricas de protocolo de Internet (IP), identificadoras de protocolo y de la administración del sistema de servidores raíz. *LATINO AMERICANN*, es una organización para la difusión de información y dialogo en temas de Nombres de Dominio, Números IP y Gobierno de Internet en América Latina y el Caribe, su misión, así mismo, es la de colocar información en español, portugués y francés de acceso para todos, considerando que la información en los idiomas de la región resulta siendo un elemento para poder comprender los fenómenos propios del internet, desde una perspectiva regional en el contexto global. *LACTLD*, es una organización sin fines de lucro que busca agrupar a los administradores de los ccTLD[46] de América Latina y el Caribe, con el objeto de Coordinar políticas en conjunto, así como estrategias de desarrollo de los nombres de dominio a nivel regional. *INTERNIC*, es un servicio y marca registrada del Ministerio de Comercio de los Estados Unidos de América y licenciado a *IANA* para la gestión de disputas públicas relacionadas con el registro de nombres de dominios. *LACNIC,* es la organización para el Registro de Direcciones de Internet para América Latina y el Caribe. Su objetivo es la construcción y articulación de esfuerzos colaborativos para el desarrollo y estabilidad de Internet en América Latina y el Caribe.

Queda claro que algunas de las organizaciones antes mencionadas han nacido en o para el gobierno de Estados Unidos. Por ejemplo, después de la IANA, se crearía la ICANN y esta absorbería la organización anterior, con el leve detalle de ser un estamento que opera en Estados Unidos y se rige bajo las leyes de California, pero por que una organización de este tipo con la responsabilidad que maneja es regulada por leyes estadounidenses?, éstas son las preguntas que aún quedan por resolver dentro de la gobernanza de Internet.

Para incentivar a la cooperación ICANN ha desarrollado un modelo de trabajo en conjunto conocido como "Multi-stakeholder model" de forma experimental este modelo busca la interacción de múltiples partes en la adopción y desarrollo de diferentes políticas que ayuden al desarrollo y evolución de Internet, que según Grace Ayres en su artículo "ICANN's Multi-Stakeholder Model"[47], ayuda a lidiar con errores y conflictos de cara a los negocios y funcionamiento de Internet. A continuación la Figura 3 detalla el modelo mencionado.

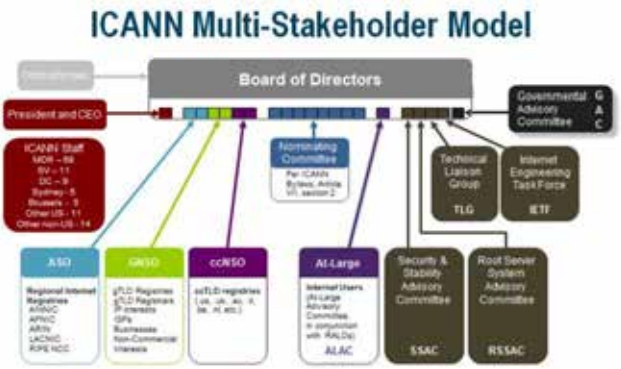

Figura 3. ICANN Multi-Stakeholder Model. Fuente, http://www.icann.org

Adicional para fomentar el trabajo de los diferentes actores de Internet, desde el año 2005 existe el foro para la gobernanza de internet, en donde concluyen sociedad civil, gobierno, entidades privadas, académicas y técnicas, estas no tienen poder de decisión alguno, pero legitima el

[45] Review of the Internet traffic management practices of Internet service providers, http://www.priv.gc.ca/

[46] ccTDLs, Country code top-level domain, http://www.icann.org/en/resources/cctlds

[47] ICANN's Multi-Stakeholder Model, Grace Ayres, http://www.icann.org/en/help/ombudsman/icann-multi-stakeholder-model-14apr08-en.pdf

modelo Stakeholder a través de un espacio de diálogo libre y directo con todos los actores.

7. Conclusiones

La inspección Profunda de Paquetes o DPI debe ser una aplicación lo suficientemente ponderada, respetuosa, y estar limitada por las leyes y normas del ente territorial donde se utilice, pero sobre todo debe asegurarse que bajo ninguna circunstancia se atente contra la privacidad, seguridad, y voluntad de las personas y bajo este derecho fundamental utilizarse. Es claro que DPI va a tener un impacto estructural de medio y largo plazo en Internet y las interacciones sociales basadas en ella que conocemos hoy. No importa la cantidad de usuarios, o reguladores que se opongan y traten de luchar contra esta tendencia, es claro que debido a las múltiples ventajas que esta presenta va a terminar utilizándose. DPI es una tecnología pensada para ser más que un complemento adicional a las redes prestadoras de servicios. Su futuro inmediato como se menciona es estar incrustada en el núcleo de la red de Internet, actualmente los ISP que desean hacer inspección de profunda de paquetes deben utilizar una caja especializada para tal fin e insertarla en sus redes, pero pronto estas características harán parte de los principales backbone de internet en el mundo, como una particularidad más y no adicional, e implícita dentro de la red.

Por otro lado, los intereses económicos en esta tecnología saltan a la vista, y enmarcan actores de tipo público y privado, entre fabricantes y operadores cuyo fin está en canalizar ofertas y productos en los consumidores generando mayores ingresos, por ejemplo, con la inyección de anuncios, entre otros. Por tal motivo es, importante ejercer políticas que prevengan la comercialización y el marketing con la información privada.

Habiendo evaluado los componentes legales tanto en Colombia como en otros países, este apartado concluye con algunas recomendaciones que en teoría podrían ser las mejores prácticas de inspección profunda de paquetes, ya que es evidente que no se puede parar y se debe adaptar a nuestros requerimientos, necesidades y sobre todo derechos, incluidas las leyes y regulación.

A continuación se mencionan las políticas que podrían implementarse generando el menor impacto posible hacia los usuarios y brindando todos los beneficios que ya conocemos de la tecnología en las redes operadoras y de servicios.

- Políticas abiertas de consulta y opinión pública acerca del uso y parte de la tecnología.
- Documentos de recomendación de las diferentes comunidades tecnológicas, académicas y gubernamentales, hacia los operadores de servicio.
- Reportes periódicos de parte de los operadores, indicando el uso y tratamiento de la información personal.
- Auditorías continuas de parte de los entes gubernamentales a los operadores de red y servicios.

Referencias bibliográficas

[1] Oficina Asesora de Planeación y Estudios Sectoriales., "Boletín Trimestral de las TIC, cifras cuarto Trimestre de 2013.," Bogotá, República de Colombia, 2014.

[2] B. SWANSON, "The Coming Exaflood," The Wall Street Journal, 2007. [Online]. Available: http://online.wsj.com/news/articles/SB11692582051 2582318.

[3] Unión Internacional de Telecomunicaciones UIT, Requisitos para la inspección detallada de paquetes en las redes de la próxima generación, Recomendación UIT-T Y.2770. Ginebra, Suiza, 2012, p. 32.

[4] Asamblea Nacional Constituyente, Articulo 15, CONSTITUCION POLITICA DE COLOMBIA 1991. Colombia, 1991.

[5] Congreso de Colombia, Ley estatutaria 1581 de 2012. Colombia, 2012.

[6] Ministerio de las Tecnologías de Información y las comunicaciones., Decreto 1704 de 2012. Bogotá, Colombia, 2012, p. 3.

[7] Congreso de Colombia, Interceptación de datos informáticos, Artículo 269c, Ley 599 de 2000. Colombia, 2000.

[8] Revista Dinero, "Sus derechos en el Habeas Data," Revista Dinero, Bogotá D.C, Colombia, Feb-2013.

[9] "Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones," 2013. [Online]. Available: https://es.necessaryandproportionate.org/text.

[10] La Constitución de los Estados Unidos de América 1787. [Online]. Available: http://www.archives.gov/espanol/constitucion.html

[11] FCC, Rules & Regulations for Title 47. ELECTRONIC CODE OF FEDERAL REGULATIONS, 2006.

[12] Electronic Frontier Foundation, "Public Unredacted Klein Declaration," 2006. [Online]. Available: https://www.eff.org/node/55051

[13] Electronic Frontier Foundation, "How the NSA's Domestic Spying Program Works", 2013. [Online]. Available: https://www.eff.org/nsa-spying/how-it-works

[14] J. Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," Forrester Research, 2013. [Online]. Available: http://blogs.forrester.com

[15] "Überwachungsskandal: NSA speicherte mehr als 300 Berichte über Merkel," http://www.spiegel.de/, 2014.

[16] Office of the Privacy Commissioner related to PIPEDA, "Legal information related to PIPEDA," www.priv.gc.ca, 2013. [Online]. Available: https://www.priv.gc.ca/leg_c/interpretations_02_e.asp.

[17] Review of the Internet traffic management practices of Internet service providers http://www.priv.gc.ca/, 2009. [Online]. Available:

http://www.priv.gc.ca/information/research-recherche/sub/sub_crtc_090728_e.asp

[18] ccTDLs, Country code top-level domain, https://www.icann.org. [Online]. Available: https://www.icann.org/resources/pages/cctlds-19-2012-02-25-en

[19] Grace Ayres, ICANN's Multi-Stakeholder Model, https://www.icann.org. [Online]. Available: http://www.icann.org/en/help/ombudsman/icann-multi-stakeholder-model-14apr08-en.pdf