

VIII Jornadas de Jóvenes Investigadores
Instituto de Investigaciones Gino Germani
Universidad de Buenos Aires
4, 5 y 6 de Noviembre de 2015

Martín Ariel Gendler

FSOC-UBA-IIGG // Licenciado en Sociología

martin.gendler@gmail.com

Eje 11. Estado, instituciones y políticas públicas.

El Estado y la neutralidad de la red: inclusión y control

Palabras clave: Neutralidad de la red – Estado – legislación – inclusión digital

Investigación en curso

Introducción

En la década de 1970 se comienzan a vislumbrar diversos cambios político-económico-sociales en las distintas sociedades de nuestro tiempo.

El modelo de producción industrial solventado en su articulación con el Estado de Bienestar comienza a desquebrajarse en torno a nuevos modos y formas en la producción. El desarrollo global de la tecnología y su penetración en las todas las esferas de la vida social trae aparejado el surgimiento de un nuevo modo de producir capitalistamente, lo que diversas corrientes del pensamiento han llamado “capitalismo informacional” (Castells, 2001) y otras “capitalismo cognitivo” (Boutang, 1999; Rullani, 2000) que comprende un cambio en el *modo de desarrollo* (Castells, 1995) dentro del capitalismo al pasar a ser el conocimiento/información el principal insumo de la producción de bienes por sobre la materia y energía lo que conlleva a diversos sectores a replantear las legislaciones y estrategias de acumulación vigentes. A su vez, comienza a gestarse un proceso de reconfiguración de los lazos sociales y de solidaridad

que imperan en los diversos colectivos humanos, generando un *proceso de cambio* en las relaciones sociales “típicas” del capitalismo industrial.

Dentro de estos procesos, la información materializada en bits (Cafassi, 1998) implica la construcción y desarrollo de una estructura de transporte que le permita desplazarse de modo seguro y veloz a todos los puntos del planeta, la cuál ha ido creciendo en tamaño y efectividad de transporte desde su planteo como una forma de comunicación descentralizada ante posibles ataques soviéticos en EEUU. Conforme la llamada “red de redes”, Internet, ha ido penetrando en las diversas estructuras productivas nacionales y en la vida cotidiana y se ha vuelto un factor fundamental en el nuevo paradigma capitalista informacional/cognitivo, se han erigido diversos niveles (Zukerfeld, 2014) que permiten el funcionamiento de su estructura y el transporte de información, las cuáles crecen en tamaño y complejidad constantemente.

En una sociedad donde el conocimiento e información se han convertido en el principal insumo productivo y social (Lash, 2005), diversos intereses, prácticas y luchas son creados y puestos en juego en torno a su transporte, propiedad, creación, copia, legislación, accesibilidad y descarga.

El presente artículo tiene como **objetivo** analizar la relación entre el principio de “Neutralidad de la Red” y los Estados Nacionales dentro del proceso de constitución y desenvolvimiento del actual Capitalismo. Para ello, además de realizar un análisis de las implicancias del concepto, se recorre y analiza la postura y el accionar del Estado respecto a la neutralidad de la red en Argentina, Brasil y Chile, teniendo en especial consideración los efectos y consecuencias generados por la acción u omisión del principio, tanto en las problemáticas respectivas a lo comercial, a la inclusión digital como a la vigilancia y el control.

Para ello, nuestra metodología consta de realizar un recorrido crítico por diversas definiciones teóricas del concepto y también realizar una lectura detallada de las leyes mencionadas.

Contexto de posibilidad: Capitalismo informacional/cognitivo y apropiación

Desde la década de 1970 se empiezan a entrever profundos cambios en el modo de producción capitalista, donde la revolución de la tecnología de la información ha sido fundamental para llevar a cabo un proceso de reestructuración del sistema capitalista signado por los **cambios en su modo de desarrollo**, los cuales “*son los dispositivos tecnológicos mediante los cuales el trabajo actúa sobre la materia para generar el producto, determinando en definitiva la cuantía y calidad del excedente. Cada modo de desarrollo se define por el elemento que es fundamental para fomentar la productividad en el proceso de*

producción” (Castells, 1995: 32) configurando que en nuestra época actual predomine el **modo de desarrollo informacional**. El modo de desarrollo penetra el conjunto de estructuras, instituciones y relaciones sociales, permeándolas.¹

Este, define su cambio al producir un nuevo tipo de mercancías, los llamados Bienes Informacionales² que son *“Bienes obtenidos en procesos cuya función de producción está signada por un importante peso relativo de los gastos (en capital o trabajo). En todos los casos se trata de bienes en cuya producción los costos de las materias y de la energía son despreciables frente a los de los conocimientos involucrados.”* (Zukerfeld, 2010a: 3). Esto no elimina la producción de bienes industriales sino que ésta **queda relegada o subsumida** ante la nueva producción informacional.

Los BI primarios (Zukerfeld, 2010) compuestos puramente de información digital, tienen su materialidad en los Bits que los componen. Siguiendo el planteo de Cafassi (1998) no solamente los BI tienen materialidad, sino que cuentan con una característica particular que pone en jaque el sistema de valorización tradicional capitalista dado que los bits son fácilmente replicables sin pérdida de calidad o contenido con un costo tendiente a 0, lo que modifica de modo radical la tradicional valorización capitalista al ya no poder obtener un valor de cambio por cada réplica de producto producido (como era el caso de la producción en serie industrial).

Por lo tanto, se emplean una multiplicidad de estrategias para volver redituables estos bienes fácilmente replicables y así asegurar su valoración y la obtención de ganancia.

Siguiendo a Rullani (2004): *“El valor de cambio del conocimiento está entonces enteramente ligado a la capacidad práctica de limitar su difusión libre, es decir, de limitar con medios jurídicos —patentes, derechos de autor, licencias, contratos—la posibilidad de copiar, de imitar, de «reinventar», de aprender conocimientos de otros. En otros términos: el valor del conocimiento no es el fruto de su escasez —natural—, sino que se desprende únicamente de limitaciones estables, institucionalmente o de hecho, del acceso al conocimiento”* (Rullani, 2004: 4). Es decir, que el valor del conocimiento y por ende de los BI estará atado a una serie de restricciones artificiales que limiten su difusión o asignen valor a su replicabilidad.

¿Por donde viajan los BITS? Una breve mirada sobre la infraestructura de la Red

¹ Esto no significa automáticamente el fin de la producción agraria o el cierre de las industrias, pero sí significa una reestructuración de sus estructuras, instituciones y relaciones sociales adaptándose al nuevo modo de desarrollo.

² De ahora en más, los llamaremos “BI”.

Como podemos apreciar, la información y el conocimiento materializado en BITS cumplen un **papel fundamental** en la producción y organización del capitalismo actual.

Pero ¿por donde circulan estos BITS? ¿Cómo llegan a cada hogar, a cada teléfono móvil, a cada empresa, al Estado? ¿Quién nos permite y brinda el acceso a los diversos contenidos y páginas web? Siguiendo a Zukerfeld (2014) podemos apreciar que la estructura de Internet está compuesta actualmente por 5 niveles: infraestructura, hardware, software, contenidos y red social. El nivel de la infraestructura *“es el más básico y el que suele olvidarse con mayor facilidad. No es difícil notar que los flujos de información digital circulan por algún lado. De manera sencilla, podemos decir que la infraestructura incluye ante todo Cables submarinos y satélites para transmitir Información Digital de manera intercontinental... Incluye también los tendidos de fibra óptica que llevan la información dentro de los continentes.”* (Zukerfeld, 2014:28).

Siguiendo a Cortes Castillo (2013), dentro de las capas de la Red encontramos el método que emplea Internet para transmitir los datos, conocido como la ‘conmutación de paquetes de datos’ o **packet switching**. Siguiendo al autor, *“implica que todos los datos –sin importar su contenido o características– se parcelan en el punto de origen y se transmiten por la red en cualquier orden y por rutas distintas hasta llegar al destino final. Solo allí se rearmen en su estado original y se vuelven asequibles para el usuario.”* (Cortes Castillo, 2013:6).

Cada vez que un usuario realiza una acción en Internet a través de un dispositivo digital, esta sale de su dispositivo, pasa por un ISP, viaja en miles de fracciones a través de la red de infraestructura hasta el servidor destino. Según la acción ejecutada, el servidor destino genera una respuesta, la cuál puede volver al usuario original o ser retransmitida a otro/s usuario/s según cuál sea la acción deseada. Vemos así por ejemplo que un usuario que ingresa a un diario online y desea conocer los resultados de su equipo de fútbol favorito generará una acción (por ejemplo un clic) que obtendrá una respuesta por parte del servidor destino (en este caso el Diario online) el cuál enviará la información, fragmentada a través de la red de infraestructura hasta el ISP del usuario y de allí a su dispositivo digital. En cambio, en el caso de un diálogo sincrónico en el Chat de alguna aplicación, la acción saldrá del dispositivo del usuario A, pasará por su ISP, se fraccionará en miles de partes y viajará por la red de infraestructura hasta el servidor destino, el cuál generará como respuesta una re-transmisión de esa acción enviándola (fraccionada nuevamente) a través de la red de infraestructura al ISP del usuario B, el cuál la transmitirá al dispositivo digital de éste. Si el usuario B desea responder al usuario A, luego de tipear lo que desea escribir y apretar “enter”, se generará el

mismo proceso pero al revés.³ Vemos así el importante papel que cumplen los prestadores del servicio de Internet (ISP) y los servidores destino en el proceso de circulación de los datos y BITS.

¿Neutralidad de la Red?

Si bien diversos autores discrepan en el origen o el surgimiento de este concepto/principio, lo que queda en claro es que la **neutralidad de la red** es un principio que establece que todos los contenidos que circulan por Internet deben recibir tratos igualitarios, manteniéndose las redes abiertas a la libre circulación de información, la cuál no debe discriminarse según origen, uso o aplicación, limitándose los prestadores del servicio a garantizar el acceso y la conexión entre los usuarios y no establecer restricciones sobre los contenidos que circulan.(Wu, 2003).

Es decir, que la neutralidad de la red es un principio que busca garantizar la circulación continua y fluida de BITS entre los diversos usuarios y servidores destino mediadores sin que haya diversos obstáculos en su camino.⁴

Siguiendo a Miranda y Carboni (2011): *“El término neutralidad de la red tiene sus orígenes en el Informe Bangemann realizado por los países de la Unión Europea a comienzos de la década del 90. El mismo planteaba regular las redes en pos de garantizar interconexión e interoperabilidad bajo las premisas de la nueva economía basada en las políticas de liberalización del mercado para promover la competencia y la inversión privada. Por su parte, Estados Unidos analizó dicho informe y elaboró el suyo propio conocido como Green Paper que introduce el concepto de neutralidad de la red para aludir a la relación entre la arquitectura de las redes y su marco regulatorio.”* (Miranda y Carboni, 2011: 6). Debemos tener en cuenta que este primer planteamiento se realizó pocos años después de la caída del Muro de Berlín en plena configuración del neoliberalismo y del nuevo sistema de negocios del capitalismo informacional o cognitivo. Bajo esos procesos, la necesidad de una red confiable y veloz para el intercambio de información era de suma importancia, principalmente por la escasa penetración de Internet en la población mundial en aquella época.

³ Consideramos que la respuesta del servidor destino es una **re-transmisión** ya que esta se codifica y reconvierte en un formato determinado (y no otro) antes de llegar al usuario B. Los membretes de un email de gmail (emisor, destinatario, asunto, firma, etc) o el nombre y el avatar de usuario en Facebook son un buen ejemplo de esta re-transmisión.

⁴ Es por esto que Ruiz Gómez (2013) lo plantea como producto y a su vez heredero de la “Internet libre primitiva”, de sus fundamentos y valores.

Conforme esta penetración fue aumentando exponencialmente, se fue constituyendo poco a poco un enorme mercado y se fueron obteniendo ganancias astronómicas por intermedio de la Red, poco a poco esta libertad fue siendo cada vez vista con peores ojos por parte de los diversos gobiernos y de las empresas capitalistas.

Diversos autores coinciden en que fue el académico norteamericano Tim Wu quien plantearía originalmente el principio en 2003 observando 4 peligros a la neutralidad de la red: 1) Bloqueo de aplicaciones, 2) Tendencia a la monopolización de los ISP con perjuicio de los clientes, 3) Priorización de determinados servicios, proveedores, aplicaciones o contenidos, según acuerdos comerciales, 4) Falta de transparencia. Ante estas amenazas, se plantearía una serie de libertades rectoras del principio intentando encontrar la forma de mantenerlo intacto.

Esto debemos comprenderlo en clave de los diversos procesos generados, principalmente tras la sanción de la *Digital Millenium Copyright Act* (DMCA) en 1998⁵, la instalación de la política de Seguridad Nacional y lucha antiterrorista en los países centrales tras los atentados del 11 de septiembre de 2001 y de la avanzada de la Propiedad Intelectual en torno a criminalizar los diversos intercambios de información, videos, música, etc. Es decir que, conforme la expansión de la penetración de las tecnologías digitales, el modelo original de neutralidad de la red anti-discriminatorio pasaría a ser visto como una amenaza por los principales centros del capital informacional o cognitivo, intentando, por medio de un encrudecimiento en la legislación, imponer los cercamientos artificiales (Rullani, 2004) propios de la Apropiación Excluyente que destacábamos anteriormente.

Por un lado las empresas proveedoras del servicio, los ISP comenzaron a plantear la batalla desde dos frentes:

1) Bloqueo de páginas y aplicaciones “peligrosas” o violadoras de los derechos de autor (descargas, torrents, páginas de movimientos sociales, aplicaciones P2P, etc.): El ISP es la puerta de entrada y salida del dispositivo digital en la relación “acción-respuesta” de los BITS y por ende pueden regular, estrangular o directamente cortar de cuajo el flujo de BITS dirigido o proveniente de una aplicación o página web considerada como “indeseable”. Por este medio se viola la neutralidad de la red al discriminar una serie de datos por sobre otros.

2) Cancelar la Tarifa Plana y brindar conexión “Premium”

Tarifa Plana se refiere al servicio donde por un costo fijo mensual, el ISP permite el acceso ilimitado a todos los contenidos de la web sin discriminar a unos por sobre otros. Eliminando esta tarifa plana, se pasa a cobrar o bien por un “paquete de datos mensuales limitados” (por

⁵ La cuál establecía criminalidades penales para la evasión o violación de los sistemas electrónicos de protección del copyright (Gendler, 2013).

ejemplo 2 GB), o una tarifa base que requiera un pago extra para poder acceder a determinados servicios. Así, los ISP lograrían emular al servicio de cable televisivo permitiendo el acceso a diversos contenidos “básicos” y cobrando un extra para acceder a los más populares (como Facebook, Twitter, Youtube, Wikipedia, etc). Si bien estos intentos y acciones de los ISP encontraron una fuerte resistencia por parte de diversos movimientos sociales y ONG, Alcántara (2011) sostiene que en este debate las ISP cuentan con ventaja por **acción u omisión** de los Estados Nacionales.

Acción al sancionar leyes a favor de la discriminación y cobro de servicios y paquetes de información por parte de las ISP, al encrudecer las leyes penando el libre compartir y sobre todo el uso de P2P o al habilitar a las ISP a ir recortando la velocidad de Internet de los usuarios que utilicen estos servicios que “atentan” contra la Propiedad Intelectual.

Omisión al no reglamentar un marco normativo sobre estas problemáticas permitiendo a las ISP hacer y deshacer a gusto y conveniencia de sus negocios.

A su vez, las ISP argumentan que, con el desarrollo de las tecnologías digitales, cada vez son más usuarios los que utilizan una mayor velocidad para descargas de paquetes de datos, lo que genera una “congestión de las redes” ocasionando problemas de conexión y de velocidad en horarios pico. Es por esto que incitan a que el Estado autorice el cobro diferencial de contenidos para, con ese dinero extra, “poder seguir innovando en la infraestructura”.⁶

Ahora bien, ¿que implicancias tiene este avance excluyente de las ISP sobre el principio de Neutralidad de la Red?

Fernández (2014) indica como la alteración de la neutralidad puede poner en peligro no solo la libertad de expresión y de circulación de la información, sino también el espíritu “primigenio” de Internet, y podría llegar a trabar la innovación de nuevas aplicaciones y servicios al pasar a estar estos segmentados en los usuarios que puedan pagarlos. *“Parte de la discusión se centra en si el respeto a las mencionadas libertades debe dejarse al juego de la libre competencia entre los operadores o si es precisa una intervención legislativa o regulatoria para establecer deberes específicos de neutralidad, y si resultan suficientes en este sentido las previsiones incluidas en los distintos dispositivos legales aprobados a tal fin por los países descriptos... En consecuencia, se torna fundamental la intervención de los Estados y los organismos supranacionales a la hora de encarar políticas públicas que actúen en favor de garantizar los derechos digitales de los ciudadanos, en detrimento de la*

⁶ Como hemos visto, no solo los datos se transfieren de manera fragmentada por los múltiples canales y nodos de la red sobre el principio de “mejor esfuerzo” impidiendo su congestionamiento, sino que la infraestructura es un nivel de la red totalmente ajeno a los ISP, por lo que el argumento además de engañoso, es nulo.

concentración y centralización de la propiedad o de los insumos necesarios para prestar el servicio.” (Fernández, 2014: 78).

Podemos ver hasta aquí como los derechos humanos, la libertad individual, el libre tráfico de información materializada en BITS, la innovación, y el ataque contra el espíritu primigenio de Internet dominan estos planteamientos acerca de la Neutralidad de la Red focalizando en la problemática de cómo estas acciones favorecen a los diversos cercamientos artificiales y como eso puede afectar el accionar cotidiano de los usuarios y la potencialidad democratizadora de Internet. Con esto queremos expresar que si bien este enfoque económico es interesante y necesario a tener en cuenta, la Neutralidad de la Red conlleva otras problemáticas a analizar: la Vigilancia, el control y la seguridad informática.

Vigilancia, control, seguridad informática y otras verbas

La relación entre neutralidad de la red y la Vigilancia se da por el hecho de que las ISP pueden discriminar contenidos al ser la puerta de entrada y salida de nuestros dispositivos digitales. De este modo, los ISP tienen la posibilidad de saber desde que dirección fue enviada, a que hora, utilizando que navegador y que aplicación (facebook, twitter, gmail, etc) cuál es el destino, entre otros.

Esto es lo que Fernández Delpech (2004) llama “**datos de tráfico**”, es decir los registros superficiales de la “acción-respuesta” que de todos modos permiten dar cuenta de un gran número de datos respecto a la acción del usuario/empresa/estado en la red y por tanto constituyen una fuerte violación a su privacidad. El abogado argentino distingue estos datos de tráfico de los “**datos de contenido**” que justamente brindan el contenido de esa acción-respuesta⁷. Las ISP están en conocimiento constante de los destinatarios de las acciones, por ende en conocimiento de sus datos de tráfico. Esto les permite en muchas ocasiones almacenarlos y crear un historial de cada usuario acerca de sus acciones en la red, el cuál puede ser solicitado por el Estado, por empresas de marketing o publicidad online, por organizaciones delictivas o por cualquier interesado. En muchos casos el Estado es cómplice de este almacenamiento, como mencionamos anteriormente, por Acción al reglamentar la obligatoriedad de este almacenamiento en leyes, decretos o disposiciones oficiales o por

⁷ Para dar un ejemplo sencillo, podemos ver en un email enviado por el usuario A desde su PC hogareña desde su cuenta de gmail a otro usuario. Los datos de tráfico serían su número de IP, las 18.15hs, desde Buenos Aires (Argentina), hacia el Usuario B que utiliza también una cuenta de gmail. Si este genera una respuesta, el ISP obtendrá a su vez los mismos datos pero referidos al Usuario B (su IP, 18.30hs, Madrid, con objetivo Usuario A). Los datos de contenido serían el asunto, el contenido y el posible archivo adjunto que se pudieren enviar ambos usuarios.

Omisión al no tener normativa al respecto permitiendo el libre accionar (y por ende la libre venta y uso de estos datos) por parte de los ISP. En su accionar en Internet muchas veces el usuario accede o busca acceder a sitios que no se encuentran encriptados⁸ por lo que no es necesario para las ISP utilizar un software de desencriptación, sino que recibe sencillamente ambos tipos de datos, si lo desea⁹. En el caso de páginas o aplicaciones encriptadas, muchas de ellas se encriptan con un código propio de la aplicación (Bancos, Facebook, Google, etc) por lo que la ISP no podrá acceder a los datos de contenido salvo una solicitud para que se los brinde.

Aquí vemos también que las ISP no son los únicos actores involucrados en la violación de la privacidad. Recordemos que la información materializada en BITS en Internet viaja por el principio de Conmutación de Datos que primero los comprime en “paquetes de datos” y luego los fragmenta para su envío a través de la infraestructura. Si bien esto puede parecer que lograría la inviolabilidad del contenido, estos datos se vuelven a juntar en un servidor/aplicación objetivo que es el que brinda la respuesta (al usuario A o retransmitiéndola al Usuario B). Por ende, este servidor/aplicación tiene acceso tanto a los datos de tráfico como de contenido ya que debe generar una respuesta a esos datos o retransmitirlos, por lo que puede a su vez almacenarlos y luego utilizarlos o venderlos según sea su intención. Esto es claro con solo observar una pequeña parte de la política de privacidad de Facebook¹⁰.

Sumado a esto no podemos dejar de mencionar los datos proporcionados tanto por Wikileaks en 2010 como recientemente por Snowden a fines de 2013 respecto al accionar de las agencias de seguridad nacionales (principalmente la NSA y la CIA estadounidenses y varias agencias europeas vía el programa PRISM y otros) en lo que refiere a esta problemática de la violación de la privacidad. Ambas fuentes señalan una vigilancia constante por parte de estas agencias en lo que respecta tanto a datos de tráfico como de contenido. Por un lado esta información la consiguen vía requiriéndosela a: 1) los servidores/aplicaciones (Facebook, Twitter, Dropbox, Microsoft, Google, etc), 2) a los ISP, las cuáles brindarían una copia exacta de los datos de

⁸ Encriptar es una manera de codificar la información para protegerla frente a terceros. Por lo tanto la encriptación informática sería la codificación la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red. Es por medio de la encriptación informática como se codifican los datos. Solamente a través de un software de descodificación que conoce el autor de estos documentos encriptados es como se puede volver a decodificar la información. Fuente: <http://www.larevistainformatica.com/que-es-encriptacion-informatica.htm> Consultado el 17/8/2015

⁹ Los datos de tráfico siempre son recibidos por el ISP. En cambio para recibir los datos de contenido debe haber un deseo y un accionar para ello.

¹⁰ <https://www.facebook.com/about/privacy/> Consultado el 17/8/2015

tráfico y (si pueden) contenido, 3) directamente “pinchando” los cables submarinos para recopilar esta información, 4) distribuyendo malware¹¹, virus, gusanos, troyanos, backdoors¹², entre muchos otros para garantizar un acceso total a la información.

Si bien algunos de estos modos y formas de violar la privacidad y obtener datos parecieren no tener relación con la neutralidad de la red debemos destacar que efectivamente **tienen relación y mucha**. No solo se obtienen datos por medio de las ISP o de los servidores/aplicaciones con los que el usuario está en contacto, sino que estos se obtienen tanto en la misma infraestructura oligopolizada que les da transporte como al introducir estos malwares al dispositivo. Y para que todo esto pueda ser posible claramente **la información materializada en BITS es discriminada, visualizada y seleccionada** en su transporte, tanto para requerirla los organismos de seguridad como para utilizarla para introducir malware funcional¹³ que luego retransmita la información que normalmente el usuario no compartiría por Internet.

El Estado como actor en la problemática

Como hemos visto, el Estado pasa a ser un actor privilegiado en la problemática de la neutralidad de la red por acción o por omisión.

Siguiendo a Alcántara (2011) en múltiples ocasiones el Estado se alía con las ISP y los servidores/aplicaciones para recolectar los datos de tráfico y contenido: *“El progresivo endurecimiento de la legislación sobre propiedad intelectual ha sido el paraguas bajo el cual se han introducido sistemas de monitorización intensiva de la actividad de los usuarios en Internet... aquí los Estados se encuentran con el apoyo incondicional de las grandes corporaciones, aliados de éstos en esta batalla concreta. Ambos sectores ven en Internet una amenaza y deciden aliarse para quitarle todo el potencial que posee.[Así] Se presiona al Estado para desarrollar leyes que les favorezcan, leyes que el estado desarrolla y sabiendo que el éxito de estos sectores es también su éxito: la misma ley que permite controlar el flujo de contenidos permite disciplinar a la población”* (Alcántara, 2011: 52-53).

¹¹ El Malware es una aplicación informática maliciosa diseñada tanto para ser difícil de detectar como para registrar acciones del dispositivo infectado. Suele utilizarse para obtener datos para publicidad o venta de información. <https://www.infospware.com/articulos/que-son-los-malwares/> Consultado el 17/8/2015

¹² Este es un tipo de malware cuya función es abrir las “puertas traseras” del software de nuestros dispositivos permitiendo así la extracción de la información guardada en el dispositivo, incluso aquella que no es compartida en Internet.

¹³ Los cuáles en la mayoría de los casos ingresan en conjunto con los paquetes de información recibidos.

Esta tensión y alianza de los Estados nacionales con las ISP y los servidores/aplicaciones podemos apreciarla al analizar tres de los marcos regulativos que han surgido en los últimos años en nuestra región: el Marco Civil de Internet de Brasil, la Ley Argentina Digital y la Ley 20.453 “de neutralidad de la red” de Chile.

Chile

El primero en reglamentarse fue el de Chile en el año 2010, fruto de la conjunción entre el pedido de organizaciones de la sociedad civil (principalmente NeutralidadSI! y ONG Cívico) y el interés de varios diputados interesados para reglamentar una Ley de Defensa al Consumidor en Internet. El Proyecto fue presentado a principios de 2007 y tras tres años de duros debates, modificaciones y reiteradas acciones de las organizaciones sociales¹⁴ fue aprobado en 2010 con inmensa mayoría parlamentaria¹⁵.

Si bien esta ley fue el primer proyecto a nivel mundial en consagrar la Neutralidad de la Red, cuenta con varios puntos de duda que debemos analizar brevemente.

Si bien la Ley expresa la **prohibición** de que los proveedores interfieran o bloqueen contenidos y servicios *legales* utilizados por los usuarios y a su vez fija la obligación de brindar información sobre el servicio contratado, vemos que, siguiendo a Lara (2010), **la definición de “que es” un proveedor de Internet excluye al Estado Chileno** quien también brinda conexión tanto en asociación con algunas ISP como principalmente en ministerios y espacios públicos. De esta manera el Estado Chileno quedaría legalmente exento de estos puntos del marco normativo. A su vez, el Artículo 24 H en su sección “a” establece que “No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho a usar contenidos y redes”, dejando abierta la posibilidad de intervención en la medida en que ésta no sea considerada arbitraria, es decir, **cuando se considere que hay uno o varios motivos** que permitan violar de esta manera la neutralidad de la red, por ejemplo cuando esos contenidos sean considerados como *ilegales* por las diversas normativas y concepciones. Lara a su vez critica el hecho de que **no esté especificado** en el cuerpo de la ley cuando estaría justificada o autorizada la intervención, pudieron argumentar la misma desde un amplio arco de motivos y de consideraciones de contenidos de carácter no legal. De esta forma, por ejemplo, una convocatoria a la manifestación a favor de la educación pública puede ser doblemente intervenida, tanto por el Estado Chileno (que reiteramos, se encuentra exento de

¹⁴ Entre ellas saturar las casillas de e-mail de los diversos diputados, exigiendo su tratamiento.

¹⁵ Para acceder a la Ley: <http://www.leychile.cl/Navegar?idNorma=1016570>

poder bloquear, discriminar y/o limitar el contenido en las redes que suministra), como también por los mismos ISP que pueden considerar que hay un motivo para intervenir (“la seguridad nacional”) o que una convocatoria no informada previamente a las autoridades es un *contenido ilegal* y por tanto la Ley les permite discriminar y trabajar con esos datos.

Brasil

En cuanto a Brasil y su destacado “Marco Civil de Internet”, su proyecto data de 2009 cuando la *Secretaria de Assuntos Legislativos do Ministério da Justiça* junto con el *Centro de Tecnologia e Sociedade da Escola de Direito* de la Fundación Getúlio Vargas en Río de Janeiro, lanzaron el 29 de octubre la primera fase de un proceso colaborativo para la construcción de un marco regulatorio de Internet en Brasil. El proyecto pronto pasó a una segunda fase en 2010 donde se habilitó un espacio Wiki para que los diversos usuarios colaboraran en su creación. Finalizado su tiempo estimado, el proyecto fue enviado al poder legislativo en 2011, aplazándose en 2012 su tratamiento de *modo indefinido* principalmente por presiones de los multimedios brasileros, entre ellos el poderoso “O Globo”. Sin embargo, tras las revelaciones de Edward Snowden en 2013 acerca del espionaje de la NSA a Brasil, principalmente a su presidenta Dilma Roussef, ésta decretó la “**urgencia constitucional**” por la cuál debía tratarse este proyecto de Ley teniendo prioridad por sobre todos los demás. Tras una serie de debates y cambios, finalmente se aprobó el 23 de abril de 2014.

Analizándolo brevemente, podemos ver que este Marco cuenta con una serie de definiciones precisas que no dejan lugar a segundas interpretaciones (a diferencia de lo que ocurría con la Ley Chilena). A su vez, sus artículos 3, 4, 5 y 24 consagran la privacidad de los usuarios y sus datos personales, reglamenta el *derecho de acceso* a Internet y del acceso a la información, promueve la innovación y la difusión de nuevas tecnologías, optimización de las redes de infraestructura, desarrollo de programas de capacitación de Internet y prestación de servicios al ciudadano por parte del Estado y de los privados. Estas diversas disposiciones se orientan dentro de un marco más amplio de políticas de Inclusión Digital, definidas por la Cumbre Mundial de la Sociedad de la Información (2003) como el “*conjunto de políticas públicas relacionadas con la construcción, administración, expansión, ofrecimiento de contenidos y desarrollo de capacidades locales en las redes digitales públicas, en cada país y en la región*” las cuales tienen una larga trayectoria en la región. En cuanto a la Neutralidad de la Red, su artículo 9 lo consagra, y al hacer extensible la disposición al “responsable de la transmisión, conmutación o ruteo” incluye también al Estado Nacional y a los Estados

Federales al igual que las ISP (a diferencia de Chile). De este modo, El Marco Civil de Internet reglamenta de forma consistente lo referente a la problemática hegemónica a favor de los usuarios.

Ahora bien, sus artículos 13 y 15 son sugerentes en cuanto al **control**:

Art. 13. En la provisión de conectividad a Internet, cabe al administrador del sistema autónomo respectivo le deber de mantener los registros de conexión, bajo secreto, en un ambiente controlado y seguro, **durante el plazo de un año**, según el reglamento.

§ 2° La autoridad policial o administrativa o el Ministerio Público podrá requerir cautelarmente que los registros sean guardados durante un plazo superior al previsto en este artículo.

§ 3° **la autoridad solicitante tendrá el plazo de sesenta días, contados a partir de la solicitud, para ingresar, con el pedido de autorización judicial, a los registros previstos en este artículo.**

§ 4° El proveedor responsable de la custodia de los registros **deberá mantener el secreto** en relación a la solicitud prevista en § 2°, que perderá su eficacia en caso de que el pedido de autorización judicial no sea aceptada o no haya sido ejecutada en el plazo previsto en § 3°.

Art 15. El proveedor de aplicaciones de Internet constituido en forma de persona jurídica, que ejerza esa actividad en forma organizada, profesionalmente y con fines económicos, **deberá mantener los respectivos registros de acceso a aplicaciones de internet**, en secreto, en ambiente controlado y de seguridad, **por el plazo de seis meses**, en los términos del reglamento.

§ 1° Orden judicial podrá obligar, por tiempo determinado, a los proveedores de aplicaciones de Internet, que no estén sujetos a lo dispuesto en el artículo a guardar registros de acceso a aplicaciones de Internet, siendo que se tratan de registros relativos a hechos específicos en un tiempo determinado.

§ 2° La autoridad policial o administrativa o el Ministerio Público podrán solicitar cautelarmente a cualquier proveedor de aplicaciones de Internet que los registros de acceso a aplicaciones de Internet sean guardados, **inclusive por plazo superior al previsto en el artículo**, observando lo dispuesto en §§ 3° y 4° del **Art. 13.**¹⁶

Vemos así como por intermedio de estos dos artículos no solo se dispone la **obligatoriedad** de que los ISP y los proveedores de aplicaciones (Google, Facebook, etc.) que operen en el

¹⁶ <http://blog.congresoactivo.org/traduccion-al-castellano-del-marco-civil-de-internet-de-brasil/>

territorio brasilero guarden los datos de tráfico por un plazo de tiempo (que puede ser ampliado), sino que el Estado brasilero tiene la potestad de solicitar los mismos y **esa solicitud se mantendrá en el más profundo de los secretos.**

Respecto a los datos de contenido:

Art. 19. Con el objetivo de asegurar la libertad de expresión e impedir la censura, el proveedor de aplicaciones de Internet solamente podrá ser responsabilizado por daños que surjan del contenido generado por terceros si, después de una orden judicial específica, **no toma las previsiones para**, en el ámbito de los límites técnicos de su servicio y dentro del plazo asignado, **hacer disponible el contenido especificado como infringiente**, exceptuando las disposiciones legales que se opongan

§ 1º La orden judicial de que trata este artículo deberá contener, bajo pena de nulidad, **identificación clara y específica del contenido** especificado como infringiente, que permita la localización inequívoca del material.

Vemos aquí como las ISP y los servidores/aplicaciones tienen la obligación de suministrar datos de contenido si las autoridades estatales lo requirieran so pena de multas o de ser responsabilizados como “cómplices” de posibles violaciones a la propiedad intelectual. Lo que queremos explicitar con esto es que, si bien un Estado puede ser víctima de la vigilancia por parte de otros (recordemos que los organismos estatales utilizan la red de Internet al igual que los usuarios civiles, es decir, con ISP, cables submarinos pinchados, etc.) e incluso puede reglamentar un Marco-Ley “progresista” en términos de garantizar la neutralidad de la red en términos de los contenidos comerciales, de todos modos reglamenta diversas medidas de claro control y violación de la privacidad de los usuarios. Respecto a esto, **no solo no prohíbe el registro de datos** por parte de las ISP y servidores/aplicaciones, **sino que lo hace obligatorio** y reglamenta su acceso a estos datos de modo discreto y constante.

Argentina

En cuanto a Argentina, la Ley “Argentina Digital” es un caso diferente al analizado en Chile y/o Brasil al no ser una ley que nazca de alguna organización o fundación de la sociedad civil, sino que surge como un proyecto de reemplazo de la antes vigente Ley de Telecomunicaciones 19.798, sancionada en 1972 durante la dictadura de Lanusse.

En su página web, puede apreciarse su argumentación “*Impulsamos esta Ley con el objetivo de generar un salto tecnológico en las comunicaciones de la Argentina, que garantice la*

*soberanía tecnológica y productiva para el desarrollo de nuestra nación*¹⁷. Si bien diversas agrupaciones de la sociedad civil celebraron el tratamiento de un nuevo marco regulatorio que incluya a la telefonía móvil y a Internet, sus críticas se focalizaron principalmente en los presurosos tiempos de aprobación del proyecto (Diciembre de 2014) y en diversos puntos de sus disposiciones.

Analizándola brevemente, podemos ver que, al igual que en el Marco de Brasil, esta Ley ratifica en diversos puntos el rol del Estado en cuanto a políticas de Inclusión Digital al expresar como objeto el “garantizar el derecho humano a las comunicaciones y a las telecomunicaciones”, “promover el rol del Estado como planificador”, y fomentar “la competencia y generación de empleo”. De este modo, se crea una nueva autoridad de aplicación, la AFTIC a la que se le brindan atribuciones para regular tarifas de interconexión, la velocidad mínima de conexión, el establecimiento de zonas de promoción e incentivos para el despliegue de infraestructura.

La AFTIC a su vez cuenta con presupuesto propio (cerca a los 15 millones de pesos), absorbe a la Secom y la Comisión Nacional de Comunicaciones y quedan bajo su órbita la empresa Arsat (de gran capital accionario estatal), el programa Argentina Conectada y el Correo Oficial de la República Argentina convirtiéndose de cierta forma en “juez y parte” de las telecomunicaciones argentinas al ser la autoridad que reglamenta, regula y sanciona y al tener en su órbita empresas como Arsat que es responsable de la TDA y de la Red Federal de Fibra Óptica (entre varios otros).

A su vez, el directorio de la AFTIC si bien está reglamentado que esté integrado por un director y presidente designados por el Ejecutivo, tres propuestos por una comisión bicameral especializada y tres representantes parlamentarios (mayoría, 2da minoría y 3ra minoría, un representante de las provincias y un director propuesto por el Consejo Federal de las Tecnologías de Telecomunicaciones y Digitalización (Artículo 84), el mismo artículo dispone que esos miembros serán nombrados por el Poder Ejecutivo sin previa consulta al poder legislativo, judicial u organizaciones de la sociedad civil, lo que asegura en cierto modo una selección favorable al gobierno de turno.

Respecto a la Neutralidad de la Red, son centrales sus artículos 56 y 57:

“ARTÍCULO 56. — *Neutralidad de red.* Se garantiza a cada usuario el derecho a acceder, utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, servicio o protocolo a través

¹⁷ <http://www.argentinadigital.gob.ar/> Consultado el 17/8/2015

de Internet sin ningún tipo de restricción, discriminación, distinción, bloqueo, interferencia, entorpecimiento o degradación.

ARTÍCULO 57. — *Neutralidad de red. Prohibiciones.* Los prestadores de Servicios de TIC no podrán:

- a) Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario.
- b) Fijar el precio de acceso a Internet en virtud de los contenidos, servicios, protocolos o aplicaciones que vayan a ser utilizados u ofrecidos a través de los respectivos contratos.
- c) Limitar arbitrariamente el derecho de un usuario a utilizar cualquier hardware o software para acceder a Internet, siempre que los mismos no dañen o perjudiquen la red.”

Vemos así que, al igual que en Chile y en Brasil, la problemática económica de la Neutralidad de la Red queda legislada de modo de asegurar la no discriminación de los BITS con un fin económico. Sin embargo, y siguiendo a Chaparro (2014), en lo relativo al control, vigilancia y privacidad de los datos la Ley es más “*una simple formulación de intenciones, [donde] la capacidad de fijar todas las políticas de telecomunicaciones queda en manos de la autoridad de aplicación.*” (Chaparro, 2014: 3).

Vemos así que respecto a la privacidad, solo el artículo 5 es claro¹⁸, refiriéndose a la “inviolabilidad de las comunicaciones” pero haciendo referencia principalmente a las comunicaciones de emails, correo o mensajes emitidos por otros mecanismos (cuyos datos de tráfico y contenido pueden ser requeridos por un “juez competente”, sin mayor explicación de los procedimientos para ello).

Otra muestra de que la ley queda mayormente en una “formulación de intenciones” refiere a la confidencialidad de los datos y BITS emitidos por los usuarios, los cuáles solo son señalados en el Artículo 62, inciso “F” al referirse a que los licenciatarios de Servicios de TIC deben “Garantizar a los usuarios la confidencialidad de los mensajes transmitidos y el secreto de las comunicaciones” sin especificar los modos y formas en los cuáles se debe operar para garantizar esto y las sanciones que pueden surgir de no cumplirlo. Cabe destacar que nuevamente el foco está puesto en las comunicaciones y no refiere a las **producciones** de los usuarios y su circulación, las cuales brillan por su ausencia en todo el marco regulatorio.

¹⁸ Es el único artículo que contiene la palabra “privacidad” en todo el documento.

Finalmente, y siguiendo a Chaparro (2014), podemos ver que en el artículo 65 se explicita que *“podrá disponerse el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basadas en los siguientes supuestos:*

a) Afectación del funcionamiento de los servicios de Seguridad Nacional, Defensa Civil y de Emergencias.”

Vemos así que no solo se conserva el término “Seguridad Nacional” de la vieja Ley promulgada en dictadura, sino que se deja cierta carta blanca al interferir en los flujos de datos y en su posterior sanción sin que esté especificado que considera la Ley como un asunto de “seguridad nacional” lo suficientemente importante para violar la Neutralidad de la Red y la privacidad de los datos consagrados previamente en el mismo documento.

Vemos así como en estas tres leyes, si bien se reglamenta la problemática económica de la Neutralidad de la Red comprendida dentro del marco de las políticas de inclusión digital de los diversos países¹⁹, lejos de “asegurar el bienestar de la población” como pretendía Fernández (2014), no hay que olvidar que el Estado no deja de ser el “capitalista colectivo” como esgrimía Engels y por tanto busca mantener en su accionar (u omisión) las relaciones sociales capitalistas y por tanto al modo de desarrollo actual (informacional), incluso cuando estas implican incrementar exponencialmente el control y la vigilancia de su población.

Es decir, podemos apreciar como **el Estado reglamenta y se mete en el juego del almacenamiento y supervisión de datos y por ende en la discriminación, control, uso, etc. de los mismos, ocupando(o recuperando) cierto lugar de privilegio en lo que respecta al modo de desarrollo informacional por intermedio del control y uso de la información materializada en BITS**, además de garantizarse un método de seguridad efectivo ante posibles acciones y manifestaciones coordinadas en la web.²⁰

De este modo a pesar de ser la problemática económica el debate hegemónico sobre la neutralidad de la red, este debate en cierto aspecto **queda minimizado** frente a la peligrosidad de la violación de privacidad de los usuarios por parte de las corporaciones y de los Estados Nacionales, también efectuado violando la neutralidad de la red y siendo plenamente funcional al actual modo de desarrollo del capitalismo. No solo cobrando un extra para potenciar cierta información o prohibiendo la transmisión de la misma el capitalismo logra

¹⁹ Las cuáles no dejan de tener una fuerte influencia de los lineamientos de la CEPAL y del G8 (Di Palma, 2015)

²⁰ Un ejemplo fueron las detenciones “preventivas” y la planificación para contrarrestar las movilizaciones durante el Mundial de Fútbol de Brasil en 2014, luego de sancionar el Marco Civil de Internet.

generar plusvalor y mantener el orden social imperante, sino también mediante el registro, el control y la utilización de estos BITS.

Internet.org: la culminación de la Apropiación de la Neutralidad de la Red

Como dijimos anteriormente, a diferencia de las violaciones efectuadas por las ISP o el Estado, las redes sociales obtienen los datos de tráfico y contenido de forma legal y sobre todo **voluntaria**.

Bajo este modelo de apropiación incluyente, la red social Facebook en alianza con varias compañías telefónicas ha creado en 2014 y perfeccionado en 2015 su plataforma **Internet.org**, la cuál permite acceder de modo gratuito a Internet, con una gran velocidad de conexión, ofreciendo solo algunas aplicaciones para su uso (Facebook, Twitter, Wikipedia) y bloqueando el resto de la red salvo un pago adicional. De este modo se violaría el principio de neutralidad de la red al discriminar salvajemente los flujos de datos, con el problema de ser voluntaria la aceptación de esta discriminación para poder utilizar la plataforma. Esta plataforma obtendrá, también voluntariamente, todos los datos de tráfico y contenido referidos a todas los servidores/aplicaciones con los que quiera interactuar el usuario y no solo las propias, con lo que a su vez pueden ser un excelente método de concentración de datos para la vigilancia de los Estados.

Por eso, cabe destacar que es sumamente preocupante que varios Estados²¹ han aceptado aplicar esta iniciativa como método de inclusión digital, lo que podría reemplazar a otras estrategias. De este modo, la potencialidad democratizadora de la red se vería restringida solo a los usuarios capaces de pagar por más servicios, incluso llegando al riesgo de naturalizar entre los nuevos usuarios el que solo existan ciertos servidores/aplicaciones ignorando toda la gama restante.

Conclusiones y reflexiones abiertas

En el presente artículo hemos hecho un recorrido por las diversas implicancias y problemáticas que abarca el principio de la Neutralidad de la Red. Luego de recorrer el funcionamiento de la red, hemos podido observar su problemática

²¹ Hasta el momento Kenia, Tanzania, Indonesia, Colombia y Guatemala <http://www.eltiempo.com/tecnosfera/novedades-tecnologia/alianza-de-tigo-y-facebook-para-llevar-internetorg-a-8-millones-de-usuarios-en-colombia/15092296> Consultado el 17/8/2015

económica referida a la discriminación, el potenciamiento y/o la estrangulación de ciertos datos y accesos a determinadas páginas o informaciones, en función de implementar en la utilización de Internet los cercamientos artificiales funcionales al modelo de apropiación excluyente del capitalismo informacional/cognitivo.

También hemos analizado como la Neutralidad de la Red también conlleva una fuerte problemática relativa al control y la vigilancia tanto por parte de las empresas que componen la Red como de agencias de información internacionales y Estados Nacionales, efectuándose acciones de control sobre la información materializada en BITS y sobre la misma población en pos del mantenimiento de las relaciones sociales capitalistas contemporáneas.

Asimismo, hemos analizado una violación a la Neutralidad de la Red por intermedio de la apropiación incluyente esgrimida por las aplicaciones líderes de la web 2.0 que discriminan datos y favorecen el registro el control social, con el consentimiento los usuarios, siendo funcionales al modelo capitalista imperante de un modo más encubierto y naturalizador.

Al realizar un breve análisis de los marcos regulatorios de Brasil, Argentina y Chile hemos podido apreciar que si bien se reglamenta mayormente la problemática económica a favor de la Neutralidad y de sus usuarios, se dejan múltiples **puntos grises** (Chile y Argentina), se designan autoridades con potencialidad de resolución, control y sanción que son tanto **jueces como partes** del asunto (Argentina) o se reglamenta la obligatoriedad del almacenamiento de los datos y el hecho de que el **Estado pueda requerirlos cuando desee de modo secreto** (Brasil). Como señalamos anteriormente, si bien la Neutralidad de la Red se inscribe dentro del marco de políticas tendientes a generar Inclusión Digital y una experiencia favorable para los diversos usuarios, el hecho de que estas leyes reglamenten (por acción u omisión) directa o indirectamente los mecanismos necesarios para que los BITS puedan ser discriminados, utilizados y/o almacenados nos habla de esta estrategia de los Estados Nación de pasar a (o volver a) ocupar un rol fundamental en las relaciones capitalistas actuales por intermedio del manejo de la información.

En el capitalismo informacional/cognitivo el principal insumo del modo de desarrollo es la información/conocimiento y por ende **es la que se encuentra en juego constantemente**. El poder reglamentar, controlar y disponer a voluntad de la misma permite mantener funcional, estable y productivo esta nueva configuración capitalista frente a la amenaza inherente de los BITS que dan soporte material a la información/conocimiento por su costo de replicabilidad tendiente a cero, y es por eso que las empresas y los Estados despliegan toda la gama de estrategias y acciones anteriormente mencionadas.

Quedará para futuras investigaciones el analizar en mayor profundidad estos marcos regulatorios (tanto individual como comparativamente) y otros de la región y a nivel mundial, como también relevar y analizar diversas acciones y estrategias de los grupos y movimientos de la sociedad civil que se oponen a las diversas violaciones de la Neutralidad de la Red en sus aristas económica y de control/vigilancia.

Bibliografía

- **ALCÁNTARA, J** (2011) “La Neutralidad de la Red y por qué es una pésima idea acabar con ella” Biblioteca de las Indias, Sociedad Cooperativa del Arte de las Cosas. E-book disponible en <http://www.versvs.net/wp-content/libros/la-neutralidad-de-la-red/jose-alcantara-la-neutralidad-de-la-red.pdf>
- **ASSANGE, J** (2013) “Criptopunks: la libertad y el futuro de Internet”. Marea Editorial, Madrid
- **BOUTANG, Yean** (2004) “Riqueza, propiedad, libertad y renta en el capitalismo cognitivo” en AA. VV. Capitalismo cognitivo, propiedad intelectual, y creación colectiva, Madrid: Traficantes de sueños.
- **CAFASSI, Emilio** (1998), Bits moléculas y mercancías (breves anotaciones sobre los cambios en el submundo de las mercancías digitalizadas), Universidad Nacional de Quilmes, Bs. As, 1998.
- **CASTELLS, M** (1995) “La ciudad informacional”. Madrid: Alianza
- **CASTELLS, M** (2001) “La era de la Información. Volumen I –(prólogo, capítulos 1 a 5)” Edición de Hipersociología, 2011
- **CORTES CASTILLO, C** (2013) “La neutralidad de la red: la tensión entre la no discriminación y la gestión” Documento del Centro de Estudios de Libertad de expresión y acceso a la información (CELES). Disponible en <http://www.palermo.edu/cele/pdf/PaperNeutralidadFinal.pdf>
- **CHAPARRO, E** (2014) “Argentina Digital: una oportunidad perdida” Publicación de la Fundación Vía Libre, disponible en <http://www.vialibre.org.ar/2014/12/16/argentina-digital-una-oportunidad-perdida/>
Consultado el 17/8/2015
- **DI PALMA, C** (2015) “En Tic confío, visibilidad y vigilancia, Proyecto de Ley Argentina digital ¡Y dale con el acceso!” Ponencia presentada en las VI Jornadas Debates Actuales de la Teoría Política Contemporánea. Buenos Aires
- **FERNÁNDEZ, P** (2014) “NEUTRALIDAD DE LA RED: TENSIONES PARA PENSAR LA REGULACIÓN DE INTERNET” Revista *Question*, Vol 1, Número 42. Disponible en <http://perio.unlp.edu.ar/ojs/index.php/question/article/view/2131>
- **FERNÁNDEZ DELPECH, H** (2004) “la conservación de los datos de tráfico en la lucha contra la delincuencia informática”. Biblioteca Jurídica Virtual del instituto de

investigaciones jurídicas de la UNAM, México DF. Disponible en <http://biblio.juridicas.unam.mx/libros/6/2940/20.pdf>

- **GENDLER, M** (2013) “Movimientos sociales en la Sociedad Red: el caso del movimiento y Partido Pirata sueco” Ponencia presentada en las VII Jornadas de Jóvenes investigadores. Instituto Gino Germani disponible en http://jornadasjovenesiigg.sociales.uba.ar/files/2013/10/eje3_gendler.pdf
- **LASH, S** (2007) “Crítica de la información”, Buenos Aires, Amorrortu Editores.
- **LARA, C** (2010) “Las dudas del proyecto de ley sobre neutralidad en la red” Publicación de la ONG Derechos Digitales, disponible en <https://www.derechosdigitales.org/1855/las-dudas-de-la-ley-sobre-neutralidad-en-la-red/> Consultado el 17/8/2015
- **MIRANDA, C y CARBONI, O** (2011) “Neutralidad de la red, un debate pendiente en Argentina” Revista Oficios Terrestres Número 28. Facultad de Periodismo y Comunicación Social. Universidad Nacional de La Plata. Disponible en <http://perio.unlp.edu.ar/ojs/index.php/oficiosterrestres/article/view/1587/1428>
- **RUIZ GÓMEZ, L** (2013) “Neutralidad de la red y desarrollo de las TIC” Revista Universitaria Europea Número 20. Enero-Junio 2014. ISSN: 1139-5796. Disponible en <http://dialnet.unirioja.es/servlet/articulo?codigo=4860450>
- **RULLANI, Enzo**, (2004) El capitalismo cognitivo, ¿un déjà-vu? en AA. VV., *Capitalismo cognitivo, propiedad intelectual, y creación colectiva*, Madrid, Traficantes de sueños, 2004 (versión digital en Hipersociología)
- **WU, T.** (2003), “Network neutrality, broadband discrimination”, *Journal of Telecommunications and High Technology Law*, Colorado, Vol. 1, N.º 2, pp.: 141-179.
- **ZUKERFELD, Mariano** (2010), “La expansión de la Propiedad Intelectual: una visión de conjunto” en Mónica Casalet (compiladora) El papel de las Ciencias Sociales en la construcción de la Sociedad del Conocimiento: Aportes de los participantes al Summer School de EULAKS. EULAKS, Flacso México, México DF, 2010
- **ZUKERFELD, Mariano** (2011), Más allá de la Propiedad Intelectual: Los Conocimientos Doblemente Libres, la Apropiación Incluyente y la Computación en la Nube en de Capitalismo y Conocimiento: Materialismo Cognitivo, Propiedad Intelectual y Capitalismo Informacional, Tesis Doctoral, FLACSO, 2011.
- **ZUKERFELD, Mariano** (2014) “Todo lo que usted quiso saber sobre Internet pero nunca se atrevió a googlear.” Revista Hipertextos, 2(1), pp. 64-103.