¿Qué es la Neutralidad de la Red? Peligros y potencialidades

Martín Gendler[1]

Resumen

El presente artículo busca analizar el concepto de "Neutralidad de la Red" en torno a sus características, su aplicabilidad, sus potencialidades y riesgos teniendo en cuenta tanto su funcionalidad en la estructura de Internet, como en el proceso de constitución y desenvolvimiento del actual Capitalismo Informacional o Cognitivo. Para ello se realiza un análisis del concepto-principio buscando analizar sus implicancias en función de las prácticas cotidianas de los usuarios, de la búsqueda de rentabilidad de las diversas empresas, como de los Estados en pos de garantizar o no su aplicabilidad. Asimismo se intenta ir más allá de lo que atañe meramente al ámbito comercial, como los asuntos referidos a la Vigilancia en Internet vinculados con el concepto.
La relevancia del presente artículo está en analizar, describir y problematizar uno de los aspectos fundamentales de la vida social contemporánea.

Palabras Clave: Neutralidad de la red – capitalismo informacional – vigilancia en la red

Abstract

This article seeks to analyze the concept of "Net Neutrality" about its features, its applicability, potential and risks considering its functionality in the structure of the Internet, as in the

[1] Lic. en Sociología y docente de la Facultad de Ciencias Sociales de la UBA. Es miembro del equipo del Programa de Investigaciones sobre la Sociedad de la Información del Instituto Gino Germani donde investiga sobre cultura digital, movimientos sociales, juegos online y seguridad informática. Correo electrónico: martin.gendler@gmail.com

process of formation and development of the Informational or cognitive capitalism today. For this, we realize an analysis of the concept looking for its implications in the daily practices of users, the search for profitability serch of the various companies and the states towards ensuring or not their applicability. Also is trying to go beyond merely what concerns the commercial arena, such as issues related to Internet surveillance linked with the concept. The relevance of this article is to analyze, describe and problematize one of the fundamental aspects of contemporary social life.

Key Words: Net neutrality - informational capitalism - network surveillance

1. 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 resquebrajarse en torno a nuevos modos y formas en la producción. El desarrollo global de las tecnologías digitales y su penetración en las todas las esferas de la vida social trae aparejado el surgimiento de un nuevo modo de producir de forma capitalista, lo que diversas corrientes del pensamiento han llamado "capitalismo informacional" (Castells, 2001) y otras "capitalismo cognitivo" (Boutang, 2004; Rullani, 2004) 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 cual 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 cuales 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 el concepto de "Neutralidad de la Red" para profundizar en sus características, su aplicabilidad, sus potencialidades y riesgos teniendo en cuenta tanto su **funcionalidad** en la estructura de Internet como en el proceso de constitución y desenvolvimiento del actual Capitalismo Informacional o Cognitivo. Principalmente se buscará problematizar el principio de Neutralidad de la Red intentando ir más allá de lo que atañe meramente al ámbito de lo comercial teniendo en especial consideración los asuntos referidos a la Vigilancia en Internet vinculados con el concepto.
Para ello, nuestra metodología consta de:
a) Se analiza la arquitectura de Internet para comprender la estructura del tránsito de los datos y los procesos y actores involucrados.
b) Se realiza un recorrido por diversas definiciones teóricas del concepto/principio de

Neutralidad de la Red para comprender su origen, sus potencialidades y limitaciones como también las distintas visiones y posiciones sobre el mismo.
c) Se analiza en profundidad tanto la problemática económica como la respectiva al control y vigilancia.
d) Se aborda y problematiza el papel de las Empresas y del Estado. Respecto al rol de este último, se realiza un breve análisis de contenido del Marco Civil de Internet de Brasil[2].
e) Finalmente, se trabaja respecto a la Neutralidad de la Red en dispositivos móviles y del emprendimiento Internet.org, haciendo foco en la comprensión de sus potencialidades y riesgos tanto presentes como futuros.

2. 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,** el cual

> "(…) 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)

Esto configura que en la actualidad predomine el **modo de desarrollo informacional.** Cabe destacar que el modo de desarrollo penetra el conjunto de estructuras, instituciones y relaciones sociales, permeándolas. 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.

Este, define su cambio al producir un nuevo tipo de mercancías, los llamados Bienes Informacionales[3] 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, 2010: 3).

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

[2] El cuál ha sido elogiado como "una Ley bisagra en la problemática de la neutralidad de la red" por diversos estudios.
[3] De ahora en más, los llamaremos "BI".

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:

Podemos destacar una forma de **Apropiación Excluyente** del valor de cambio de los BI. Es la forma clásica a través de la cual el usuario debe pagar para utilizar el bien ya sea adquiriéndolo en tiendas, ya sea comprándolo vía Web, etc. En este caso es donde vemos los cercamientos artificiales impuestos al conocimiento para asignarle un valor de cambio al bien e impedir o limitar la replicabilidad con costo tendiente a cero.[4]

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— o monopolistas 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.

Ante esto, Zukerfeld (2010) nos habla de que durante el capitalismo industrial, la legislación se encontraba abocada a legislar la propiedad física mientras que las patentes eran la cara legisladora de la información industrial:

> "Con la excepción de una modificación de 1897 entre 1790 y 1976, esto es, durante todo el capitalismo industrial, **no hubo ninguna legislación penal vinculada con ninguno de los derechos de propiedad intelectual**… lo novedoso es que a partir de la llegada del capitalismo cognitivo, las legislaciones penales se incrementan década tras década... El conocimiento en general y una forma muy particular, la información digital, asumen una centralidad productiva antes desconocida. Ésta, frágil ante la reproducción ilegal, ha de ser custodiada por las armas jurídicas más poderosas…**Esto simboliza el núcleo duro de la fundación legal del capitalismo cognitivo**." (Zukerfeld, 2010: 19)

Sin embargo, existe otro medio de apropiación, denominado "**Apropiación Incluyente**" (Zukerfeld 2011) mayoritariamente utilizada por la Web 2.0 donde se aprovechan los conocimientos "doblemente libres" (dado que los usuarios son libres de acceder a ellos, compartir, estudiarlos, etc. pero a su vez son "libres" de recibir un pago por producirlos) en torno de garantizar la gratuidad del acceso a diferencia de la Apropiación Excluyente, pero sin

[4] El caso del cierre de Megaupload por el FBI junto a los juicios, persecución y bloqueos a nivel mundial a The Pirate Bay destaca la actualidad de este modo de apropiación y de la avanzada de la Propiedad Intelectual.

embargo se vuelve **mercantil la participación de los usuarios** en esa plataforma ya que se genera un plusvalor donde antes no lo había. De este modo, se obtiene una serie de ingresos monetarios tanto vía publicidad generalizada y/o personalizada, como a través de la producción impaga de los usuarios.

Este tipo de apropiación no busca generar valor y plusvalía a base cercar y fomentar el valor de cambio de los BI, sino que por el contrario garantiza su acceso libre y gratuito pero pone su foco en volver mercantiles las acciones, interacciones, producciones, contenidos y demás relaciones generadas o compartidas al interior de las plataformas 2.0.

3. ¿Por dónde viajan los BITS? Una breve mirada sobre la infraestructura de la Red

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 dónde 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. Y en última instancia, ese algún lado refiere a una serie de artefactos sumamente costosos que sólo pueden ser instalados, mantenidos y renovados con enormes sumas de capital. De manera sencilla, podemos decir que la infraestructura incluye ante todo cables submarinos y satélites para transmitir Información digital de manera intercontinental. Pero, naturalmente, incluye también los tendidos de fibra óptica que llevan la información dentro de los continentes." (Zukerfeld, 2014:28).

Siguiendo al autor, un hecho sumamente perturbador de esta capa/nivel es que estos tendidos de cables submarinos y los satélites se encuentran en manos de un oligopolio compuesto por pocas empresas.

A su vez, yendo al nivel del hardware podemos encontrar allí a los proveedores de servicio de Internet (ISP por sus siglas en inglés), es decir, las empresas responsables de que el tráfico de BITS llegue desde la capa de infraestructura a cada terminal digital (PC, wifi) vía el módem o router que brinda la compañía al contratante del servicio. A su vez, en este nivel se pueden encontrar los dispositivos digitales que reciben el tráfico de información (PC, notebook,

netbook, tablet, dispositivo móvil, etc.) y a su vez los servidores físicos de las principales compañías brindadoras de servicio (Google, Facebook, Microsoft, etc.). De este modo se puede apreciar un nivel oligopolizado tanto en estos servicios como en las compañías ISP[5], salvo en lo que respecta al dispositivo personal que recibirá el tráfico de datos.

A su vez, encontramos en el nivel del software justamente la programación y los protocolos (principalmente el TCP/IP) que permiten tanto el viaje a destino de estos BITS como su recepción.

Siguiendo a Cortes Castillo (2013), podemos ver que la Red, principalmente los niveles de infraestructura y hardware, está definida por el principio de estratificación donde cada capa de la red tiene funciones diferentes y separadas de otra y donde cada una sirve a la de más arriba y ésta a la siguiente. Esto permite al autor indicar la existencia de cuatro capas de la Red[6] que

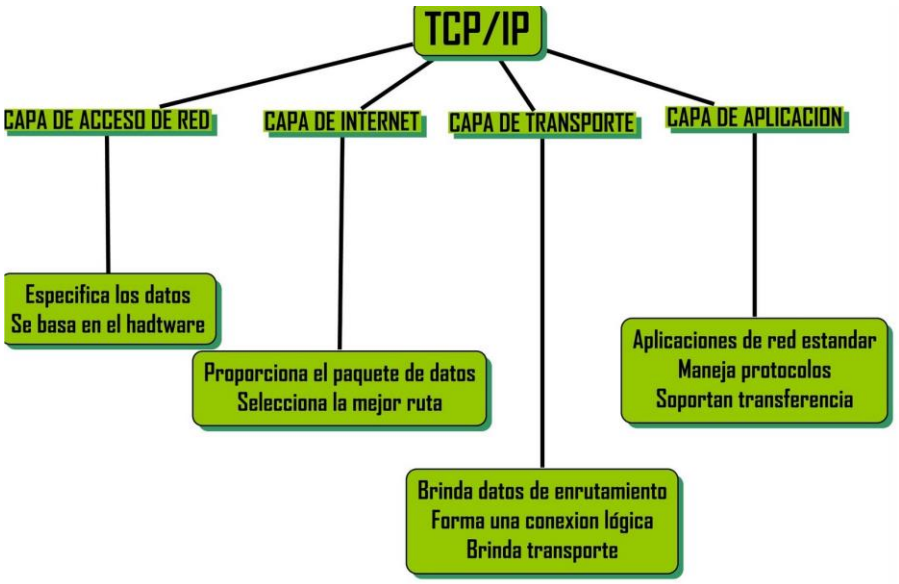
"para llevar a cabo su misión, cada capa usa los servicios de la que le precede. La capa más baja es la de '**enlace**', que contiene los protocolos responsable del transporte de paquetes a través de una red física (por ejemplo, la de una oficina o universidad); le sigue la capa **Internet**, que permite transportar paquetes a través de un conjunto de redes interconectadas, sin importar en dónde esté cada dispositivo; en seguida está la capa de **transporte**, que reparte los paquetes desde y hacia las aplicaciones de los dispositivos finales; por último, está la capa de **aplicaciones**, que contiene una serie de protocolos que permiten la comunicación entre las partes (correo electrónico, world wide web, redes de pares, video)." (Cortes Castillo, 2013: 5)

Siguiendo al autor, también encontramos el principio "extremo a extremo" que es el que asigna las funciones a cada capa. Este principio, si bien se estructura en vertical, tiene una funcionalidad horizontal, siendo los dispositivos que se conectan a la red (los extremos) los que ejecutan las funciones más elaboradas de la red y no los enrutadores o los computadores que transmiten los datos.

[5] Que reparten el mercado entre un número limitado de empresas, que si bien el usuario es "libre" de optar por la que desee siempre deberá serlo dentro de las que brinden su servicio en su zona.

[6] Que podemos verlos como trasversales a los 5 niveles descriptos por Zukerfeld (2014)

Gráfico Nro 1
Principio de estratificación: capas

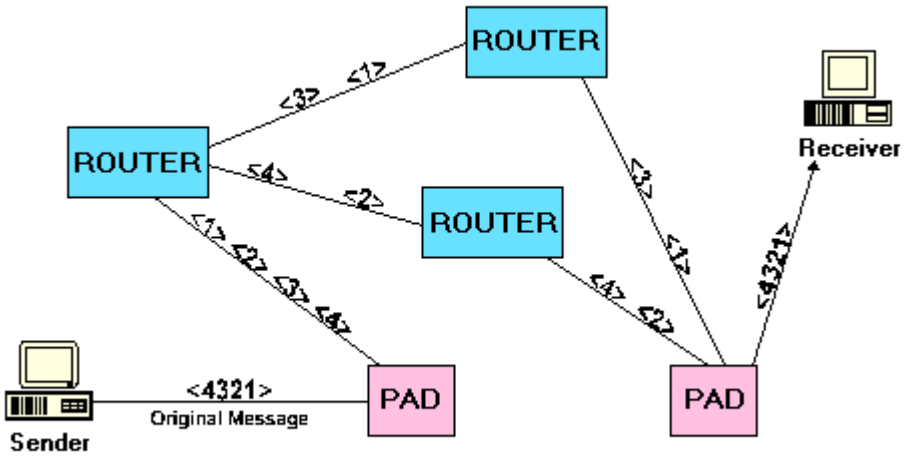


Fuente: http://dulcesalgado510.blogspot.com.ar/2010/09/capas-de-modelo-osi-y-tcpip-y-sus.html

Esto se complementa con el método que emplea Internet para transmitir los datos, conocido como la 'conmutación de paquetes de datos' o ***packet switching***. Siguiendo al autor,

"La conmutación de paquetes 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 rearman en su estado original y se vuelven asequibles para el usuario. Cada paquete contiene una parte de los datos enviados e información sobre el destino y las instrucciones para rearmarse allí (mediante los protocolos TCP/IP). Lo único que la red debe hacer –a través de los enrutadores– es transportar esos paquetes; éstos contienen la demás información. No obstante, los protocolos del envío de paquetes no garantizan un resultado; se trata de un sistema de 'mejor esfuerzo' " (Cortes Castillo, 2013:6).

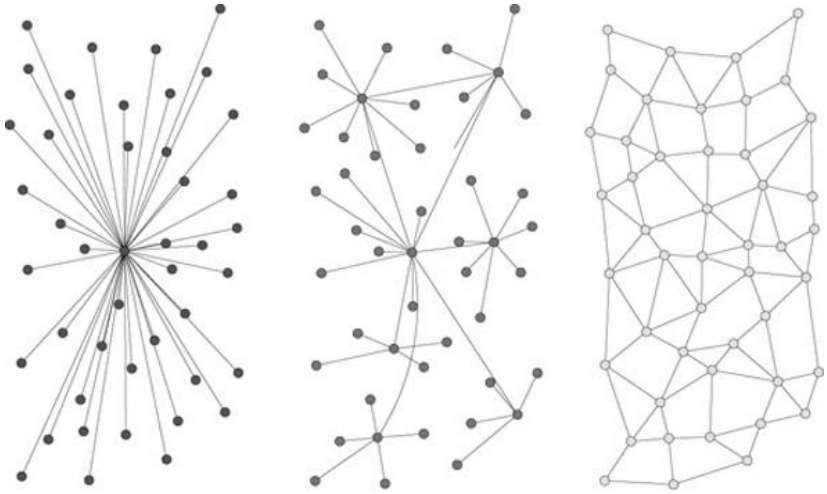
Gráfico Nro 2
Packet switching



Fuente: Netguru http://www.netguru.net/ntc/NTCC4.htm

Cabe destacar que la Red tiene una topología "distribuida" (Alcántara, 2011), es decir, un diseño de "malla" al estar todos los nodos interconectados. De esta manera se impide que un solo nodo central pueda limitar o prohibir el transporte de determinada información, se garantiza que ante la destrucción o mal funcionamiento de un Nodo el sistema continúe funcionando y a su vez garantiza la conmutación de paquetes de datos al brindar diversos canales por los cuáles la información puede ser transportada sin que uno sea distinto o más efectivo que otro necesariamente.
En la siguiente imagen podemos apreciar diversas tipologías de Red. La primera corresponde a la llamada "**Red centralizada**" (un único Nodo central), la segunda "**Red descentralizada**" (varios Nodos centrales) y la tercera es la "**Red Distribuida**" a la que corresponde la topología de Internet.

Gráfico Nro 3
Topologías de red



Fuente: Alcántara, 2011: 27

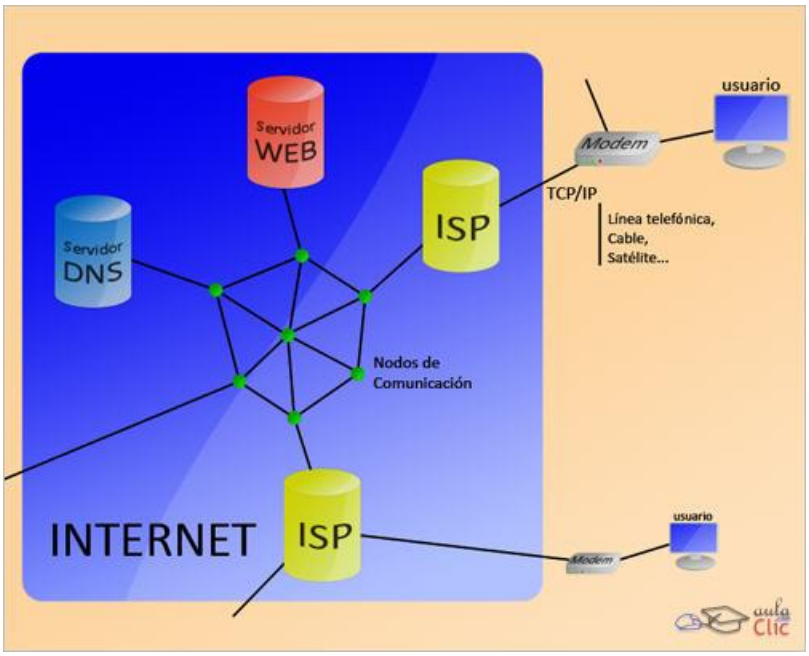
Cada vez que un usuario realiza una acción en Internet a través de un dispositivo digital, esta sale de su dispositivo, pasa por un ISP, viaja en miles de fracciones a través de la red de infraestructura hasta el servidor destino, previa relación con el servidor DNS [7]. Según la acción ejecutada, el servidor destino genera una respuesta, la cual 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 en la noticia del triunfo de River Plate) que obtendrá una respuesta por parte del servidor destino (en este caso el diario online "Olé"), que 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 cual generará como respuesta una retransmisión de esa acción enviándola (fraccionada nuevamente) a través de la red de infraestructura al ISP del usuario B, el que la

[7] Sistema de nombres de dominio o **DNS** (por sus siglas en Inglés) es un sistema de nomenclaturas cuya función más importante, es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. Es decir que el servidor DNS traduce una dirección escrita por el usuario (por ejemplo www.google.com) en código binario que le permita guiar a los datos hacia el servidor destino (Google).

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.

Gráfico Nro 3

Tráfico de datos



Fuente: AulaClick http://www.aulaclic.es/internet/t_1_1.htm

Podemos considerar que la respuesta del servidor destino es una **re-transmisión** ya que esta se codifica y reconvierte en un formato determinado (y no en 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 retransmisión.

4. ¿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 cual no debe discriminarse según origen, uso o aplicación, limitándose los prestadores del servicio (las ISP) 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 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. Es por esto que Ruiz Gómez (2013) plantea al principio de neutralidad de la red como producto y a su vez heredero de la "Internet libre primitiva", de sus fundamentos y valores.

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.

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 (Cortés Castillo, 2013; Ruiz Gómez, 2014; Fernández, 2014) 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. Siguiendo a Fernández (2014)

> "se identifican como elementos correlativos al principio convocante, garantizar cuatro libertades (FCC, 2005) a los usuarios finales: para conectar dispositivos, ejecutar aplicaciones, recibir los paquetes de contenidos que desee y obtener información relevante sobre el Plan de Servicios

contratado. Así, se puede inferir que el concepto se encuentra atravesado por dos compromisos de no discriminación diferentes: el del servicio universal –relacionado con el acceso igualitario a todos los individuos– y otro de servicio público de transporte –o common carriage, que contempla el trato igualitario de todos los contenidos que circulan por la web, sin diferenciarlos por sus costos, peso, tipo u origen."(Fernández, 2014: 71).

Esto debemos comprenderlo en clave de los diversos procesos generados, principalmente tras la sanción de la *Digital Millenium Copyright Act* (DMCA) en 1998[8], 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. principalmente con el auge de las redes peer to peer (P2P) como Napster, Kazaa, Ares y el siempre presente The Pirate Bay, entre otros.

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 recrudecimiento 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:

I. Bloqueo de páginas y aplicaciones "peligrosas" o violadoras de los derechos de autor (descargas, torrents, páginas de movimientos sociales, aplicaciones P2P, etc.): Recordemos que el ISP es la puerta de entrada y salida del dispositivo digital en la relación "acción-respuesta" de los BITS y por ende puede 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.

II. 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 ejemplo 2 GB) como es el actual caso de los servicios de telefonía móvil, o una tarifa base que requiera un pago extra para poder acceder a determinados servicios. De esta manera, 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.).

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

Una variante de esto es manteniendo la tarifa plana pero cobrando un extra por acceder "más rápidamente" a diversos contenidos (como por ejemplo Netflix[9]), ya que de igual forma se produce una discriminación en el trato de los paquetes de datos. Si bien estos intentos y acciones de los ISP encontraron una fuerte resistencia por parte de diversos movimientos sociales y Organizaciones no goburnamentales (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[10], al recrudecer 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, deliberadamente, 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". 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[11], por lo que el argumento además de engañoso, es nulo. Siguiendo a Alcántara (2011):

> "los ISP han buscado la aprobación de leyes que permitan el filtrado de las conexiones de los usuarios, de forma que se puedan tarifar por separado diferentes servicios de Internet como si requirieran y consumieran algo diferente, como si Internet estuviese en peligro de extinción. De este modo, se pretende tratar los bits de diferente manera según la información que contengan, haciéndonos creer que los bits no son sólo bits y que una determinada conexión (VoIP, o vídeo en streaming) les cuesta más que otras

[9] Empresa que efectivamente llegó a concretar un acuerdo de este tipo con el ISP norteamericano Comcast. http://www.xataka.com/analisis/el-acuerdo-de-netflix-con-comcast-vulnera-la-neutralidad-de-la-red

[10] Un caso ejemplar es el de Colombia en su Plan Nacional de Desarrollo de 2011: "En este sentido, deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de estos. Los prestadores del servicio de Internet podrán hacer ofertas según las necesidades de los segmentos de mercado o de sus usuarios de acuerdo con sus perfiles de uso y consumo, lo cual no se entenderá como discriminación." (Cortés Castillo, 2013)

[11] Si bien varias de estas participan del tendido de fibra óptica junto a varios Estados Nacionales, técnicamente no tienen implicación en lo que respecta al nivel de infraestructura.

> (como navegar la web)(…) estas corporaciones han dedicado no pocos esfuerzos tanto a hacer saber su posición ante el gobierno como a lanzar campañas masivas en contra de la neutralidad de la Red, cuyo objetivo final era aparecer como víctimas incomprendidas– y así ganar fuerza de cara a la negociación de un hipotético proyecto de ley que derogue la neutralidad de la Red"(Alcántara, 2011: 59).

De este modo, se busca obtener una reglamentación favorable en pos de incorporar los servicios limitados al igual que sucede en la actualidad con la telefonía móvil con enormes ganancias para las empresas y un pobre margen de utilización por parte de los usuarios.

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

Siguiendo a Matsushita (2014) el autor ubica al principio de neutralidad de la red dentro del ámbito de los derechos humanos relacionados con la libertad de expresión y de brindar y recibir informaciones e ideas, consagrado en el artículo 19 de la Declaración de Derechos Humanos de 1948:

> "La defensa en pro del principio de neutralidad de red es también en pro de la oportunidad de emancipación, individual, colectiva y considerada igualmente entre todos los del globo, con la finalidad de dignificar al hombre y todos los hombres, en un espíritu de fraternidad... Decimos esto, pues la oportunidad de emancipación individual y colectiva es inmediata gracias a la difusión constante y permanente de información y conocimiento, permitida y producida a través de las plataformas de comunicación, mayoritariamente de Internet." (Matsushita, 2014: 16).

Por su parte, Fernández (2014) recorre los diversos puntos del debate entre neutralidad, no discriminación, el accionar y poder de las ISP para torcer el debate a su favor y las regulaciones de los diversos Estados acerca de la problemática. Siguiendo a la autora se puede apreciar 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 concentración y centralización de la propiedad o de los insumos necesarios para prestar el servicio." (Fernández, 2014: 78).

Focalizado específicamente en la innovación, Ruiz Gómez (2013) contempla el crecimiento de las "necesidades de Internet" al calor del avance y penetración tecnológica y si bien señala que este crecimiento del uso, desarrollo y complejidad que tiene en la actualidad la red de redes se ha debido en gran parte al modelo de neutralidad y libre intercambio sostenido hasta el momento, ve con cautela el hecho de que a más complejidad de las TICS, se necesita un mayor desarrollo e inversión en la infraestructura. Por ende el autor parece coincidir con el discurso y argumentos de las ISP al pedir que se aplique una regulación a ciertos contenidos, para garantizar los "incentivos para la innovación en infraestructura" pero siempre y cuando se mantenga un "modelo de mercado competitivo".

> "Es cierto que las necesidades de Internet por parte de las TIC son cada vez mayores y esto hace que el incremento de intercambio de datos haya crecido de manera exponencial en los últimos años y las previsiones son que este intercambio, lejos de reducirse, va a seguir incrementándose. Esto genera que las redes se encuentren cada vez más saturadas y no existe ningún incentivo para que los consumidores y las empresas generadoras de contenidos traten de optimizar el tamaño de estos contenidos" (Ruiz Gómez, 2013: 17)

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 del modelo de Apropiación Excluyente y como eso puede afectar el accionar cotidiano de los usuarios y la potencialidad democratizadora de Internet.

Si bien este enfoque "económico-comercial" es interesante y necesario a tener en cuenta, la Neutralidad de la Red conlleva otras problemáticas a analizar que son escasamente trabajadas e igualmente (o aún más) perturbadoras: la vigilancia, el control y la seguridad informática.

5. Vigilancia, control, seguridad informática y otras yerbas

La posibilidad de los ISP de discriminar el acceso a los contenidos, favoreciendo a unos y prohibiendo y/o estrangulando a otros, deja en evidencia que, de esta manera, se puede acceder a todos los datos que circulan por la Red. En esto reside la relación entre neutralidad de la red y vigilancia. Es decir, al ser la puerta de entrada y salida de nuestros dispositivos digitales en relación con la red de infraestructura, los ISP tienen la posibilidad de saber desde qué dirección fue enviada, a qué hora, utilizando qué navegador y qué 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 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 la privacidad. Podemos pensar a estos datos como el "¿quién?" "¿cuándo?" "¿dónde?" y "¿para quién?" de la interacción en Internet. El abogado argentino distingue estos datos de tráfico de los "**datos de contenido**" que justamente brindan el contenido de esa acción-respuesta, es decir el ¿Qué? y el ¿por qué?. 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 están constituidos por el asunto, el contenido y el posible archivo adjunto que se pudieren enviar ambos usuarios.

Al tener la capacidad el ISP de discriminar contenidos y de potenciar o prohibir el acceso del usuario a los mismos, está 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 cual puede ser solicitado por el Estado, por empresas de marketing o publicidad online, por organizaciones delictivas o por cualquier interesado en obtenerlos.

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 omisión al no tener ninguna normativa al respecto permitiendo el libre accionar (y por ende la libre venta de estos datos) por parte de los ISP.

El acceso a los datos de contenido no es tan sencillo para las ISP como en el caso de los datos de tráfico, pero sin embargo no es imposible obtenerlos. En su accionar en Internet muchas veces el usuario accede o busca acceder a sitios que no se encuentran encriptados[12] por lo que no es necesario para las ISP utilizar un software de desencriptación, sino que reciben sencillamente ambos tipos de datos, si lo desean[13]. En el caso de páginas o aplicaciones encriptadas, muchas de ellas se encriptan con un código propio de la aplicación

[12] **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 3/9/2015

[13] 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.

(Bancos, Facebook, Google, etc.) por lo que la ISP no podrá acceder a los datos de contenido salvo una solicitud a la página/aplicación 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 parecería lograr 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 Facebook[14].

Lo perturbador del tema es que esta violación a la privacidad **se hace con consentimiento del usuario**, dado que es menester su aceptación para poder utilizar el servicio brindado por la página/aplicación determinada lo que lo vuelve totalmente legal.

Sumado a esto no podemos dejar de mencionar los datos proporcionados tanto por Wikileaks en 2010[15] como recientemente por Snowden[16] 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 requiriéndosela a:

a) los servidores/aplicaciones[17]

b) a los ISP[18], las cuáles brindarían una copia exacta de los datos de tráfico y (si pueden) contenido

[14] "Tus acciones y la información que proporcionas:
Recopilamos **el contenido y otros datos** que proporcionas cuando usas nuestros Servicios, por ejemplo, al abrir una cuenta, al crear o compartir contenido, y al enviar mensajes o al comunicarte con otras personas. La información puede corresponder a datos incluidos en el contenido que proporcionas o relacionados con este, como el lugar donde se tomó una foto o la fecha de creación de un archivo. También recopilamos información sobre el modo en que usas los Servicios, por ejemplo, el tipo de contenido que ves o con el que interactúas, o la frecuencia y la duración de tus actividades" https://www.facebook.com/about/privacy/ Consultado el 3/9/2015

[15] http://www.telegrafo.com.ec/noticias/informacion-general/item/wikileaks-revela-una-red-de-92-empresas-de-espionaje-mundial.html Consultado el 3/9/2015

[16] Edward Snowden es un consultor tecnológico que antiguamente trabajó en la Agencia Central de Inteligencia (CIA) y en la Nacional Segurity Agency (NSA) dentro de los programas de espionaje internacional Prism y XKeyscore, entre otros. En Junio de 2013 reveló diversos documentos de estas agencias y programas acerca del espionaje en Internet. Ha sido acusado de diversos cargos y actualmente se encuentra exiliado.

[17] Facebook, Twitter, Dropbox, Microsoft, Yahoo, Google, etc. http://www.rpp.com.pe/2014-10-13-snowden-insta-a-internautas-a-no-utilizar-facebook-google-y-dropbox-noticia_733375.html Consultado el 3/9/2015

c) directamente "pinchando" los cables submarinos[19] para recopilar esta información d) distribuyendo una serie de programaciones como malware[20], virus, gusanos, troyanos, backdoors[21], 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 funcional [22]que luego retransmita la información que normalmente el usuario no compartiría por Internet.

6. 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:

> "Los ataques del Estado a Internet pretenden aumentar significativamente el control social. 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. Obviamente, 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 aprueba con la tranquilidad de saber que el

[18] https://barbaricarius.wordpress.com/2013/08/13/asi-espia-la-nsa-el-trafico-de-internet/ Consultado el 3/9/2015

[19] Los cuáles recordemos son propiedad de 3 empresas oligopólicas, no casualmente estadounidenses y europas. http://www.bbc.co.uk/mundo/noticias/2013/10/131031_eeuu_nsa_espionaje_tecnicas_az Consultado el 3/9/2015

[20] 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.infospyware.com/articulos/que-son-los-malwares/ Consultado el 3/9/2015

[21] 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.

[22] Los cuáles en la mayoría de los casos ingresan en conjunto con los paquetes de información recibidos.

> 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).

Vemos así como lejos de "asegurar el bienestar de la población" 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.

Esto podemos verlo en el caso de Brasil, el cual fue uno de los principales blancos del espionaje de la NSA revelado por Snowden. Revelada esta información, este país rápidamente otorgó prioridad máxima a la sanción de su Marco Civil de Internet[23] que promueve como objetivo la regularización de la neutralidad de la red en función (y supuestamente beneficio) de la seguridad informática de sus ciudadanos y de los órganos estatales.

Si bien este Marco-ley asegura la no discriminación de contenidos en cuanto a lo comercial y establece la universalidad de conexión sin discriminación zonal, 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 el deber de mantener los registros de conexión, bajo secreto, en un ambiente controlado y seguro, **durante el plazo de un año**, según el reglamento.
> § 2º 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.
> § 3º **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.**
> § 4º El proveedor responsable de la custodia de los registros **deberá mantener el secreto** en relación a la solicitud prevista en § 2º, 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 § 3º.
> **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.
> § 1º 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

[23] http://www.telam.com.ar/notas/201404/60476-brasil-aprobo-el-marco-civil-de-internet.html Consultado el 3/9/2015

> hechos específicos en un tiempo determinado.
> § 2º 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 §§ 3º y 4º del **Art. 13.**[24]

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 territorio brasileño guarden los datos de tráfico por un plazo de tiempo (que puede ser ampliado), sino que el Estado brasileño 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" para 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. Es decir, el Estado se mete en el juego del almacenamiento 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

[24] http://blog.congresointeractivo.org/traduccion-al-castellano-del-marco-civil-de-internet-de-brasil/ Consultado el 3/9/2015

información materializada en BITS, además de garantizarse un método de seguridad efectivo ante posibles acciones y manifestaciones coordinadas en la web.[25]

De esta manera, a pesar de ser la problemática de los contenidos, su potencialidad o su estrangulamiento el debate hegemónico sobre la neutralidad de la red, este **queda minimizado** frente a la peligrosidad de la violación de la privacidad de los usuarios por parte de las corporaciones y de los Estados Nacionales, también efectuado violando la neutralidad de la red y también siendo plenamente funcional al actual modo de desarrollo informacional del capitalismo. No solo cobrando un extra para potenciar cierta información o prohibiendo su transmisión, el capitalismo logra generar plusvalor y mantener el orden social imperante, sino también mediante el registro, el control y la utilización de estos BITS.

7. Dispositivos móviles: paraíso de la discriminación y el control

Vale hacer una pequeña mención al papel de la telefonía móvil. Para estos dispositivos la peligrosidad tanto de que los ISP discriminen y estrangulen el tráfico de información como el registro y almacenamiento de datos de tráfico y de control no solo es potencial sino que es un hecho en la actualidad.

Siguiendo a Alcántara (2011) el servicio de Internet en el ámbito de la telefonía móvil ya consiste en una clara violación a la Neutralidad de la Red al brindarse servicios de paquetes de datos limitados (2GB por ejemplo), al ofrecerse conexión ilimitada y veloz a las redes sociales por un valor diario (imposibilitando acceder por medio de este pago a otros sitios/aplicaciones) y al tener estos teléfonos que vincularse con un sistema de email para que su sistema operativo funcione óptimamente[26]. A su vez, cada aplicación que el usuario desee ejecutar desde su dispositivo trae unas cláusulas de instalación que claramente violan la privacidad del sujeto[27] impidiendo su funcionamiento de no "aceptar" estas esas condiciones. Sumado a esto, la utilización del email desde el dispositivo móvil contiene una débil o incluso nula encriptación, fácilmente violable por la ISP propia, o por las que puedan conectarse ocasionalmente o incluso por la compañía de telefonía móvil que le brinde conexión de datos vía 3G o 4G-LTE.

[25] El que este Marco haya sido sancionado previamente a la Copa Mundial de Fútbol efectuada en Brasil, (tras haberse desarrollado manifestaciones coordinadas a través de la red previas al mismo) y que se hayan desenvuelto diversos mecanismos de contención de estas manifestaciones durante el evento **no es casualidad.**

[26] Gmail en el caso de Android, Icoud en el caso de Apple, Hotmail en el caso de Windows Phone.

[27] Avisando que para que esa aplicación se ejecute, la misma requerirá acceso a "cámara, video y capturas, bibliotecas de fotos y música, base de datos, contactos".

Teniendo en cuenta la tendencia de los dispositivos móviles hacia el ámbito móvil, estos son hechos más que importantes respecto a la cuestión de la neutralidad de la red y el futuro de Internet.

8. Internet.org: la culminación de la Apropiación Incluyente de la neutralidad de la red

Si bien hasta ahora hemos trabajado principalmente con métodos de violación de la neutralidad de la red mayormente vinculados con la Apropiación Excluyente, las redes sociales operan con una lógica distinta, basándose principalmente en la Apropiación Incluyente de los datos y acciones de los usuarios. 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 cual 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 completamente el principio de neutralidad de la red al no solo discriminar salvajemente los flujos de datos, sino al 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.

Cabe destacar que este modelo aún está en desarrollo y su aplicabilidad varía dependiendo del arreglo con los distintos Estados y compañías. En algunos países, como por ejemplo Colombia, Internet.org se introduce en la problemática en convenio con empresas líderes en telefonía celular. De este modo, Internet.org pasa a ser una "aplicación gratuita para los clientes" habilitando un número de aplicaciones y páginas sin costo adicional para los usuarios pre-pagos[28], es decir aquellos que cargan crédito por medio de tarjetas o carga virtual y por

[28] Entre ellas podemos encontrar: **Facebook Lite** (versión ligera de la red social), **Wikipedia** , **Messenger Facebook** (chat de la red social), **Accuweather** (estado del tiempo), **UN Women** (consejos para mujeres emprendedoras), **GirlEffect** (sitio de consejos ara las mujeres), **MAMA** (sitio de consejos para mujeres madres), **UNICEF Para la vida** (consejos para prevenir enfermedades y protección de niños), **UNICEF Tus derechos** (sitio oficial de Unicef), **MITULA** (Clasificados), **INSTITUTO COLOMBIANO PARA LA EVALUACIÓN DE LA EDUCACIÓN** (Sitio Colombiano de apoyo a la educación ICFES), **SU DINERO** (consejos para manejo del dinero), **TAMBERO** (app de apoyo a los agricultores),

este motivo no suelen acceder a Internet desde sus teléfonos móviles ya que esta actividad podría consumir todo el crédito que han cargado.
De este modo, se garantiza un acceso gratuito pero limitado a un número de aplicaciones y páginas seleccionadas (y no otras), donde su navegación implica no solo la concentración de la actividad de estos usuarios en estas páginas, sino el hecho de aceptar voluntariamente que las empresas, organizaciones y el Estado desarrolladores de estas webs y apps accedan a su tráfico de datos e información personal.

Si bien este es el modelo actual en Colombia por encontrarse en fase de pruebas, la intención manifiesta de Internet.org, como también de emprendimientos similares de otras empresas, como el Proyecto Loon de Google[29], es el de permitir el acceso de modo gratuito, bajo la consigna de que los usuarios utilicen únicamente esas webs y aplicaciones seleccionadas a cambio de permitir el acceso a su registro de actividades y datos privados y solicitando un pago adicional si se desea acceder a otros contenidos (los cuáles no se aclara si tendrán que aceptar la misma política de privacidad o no).

Por eso, cabe destacar que es sumamente preocupante que varios Estados[30] hayan aceptado aplicar esta iniciativa como método de inclusión digital, lo que podría reemplazar a otras estrategias más inclusivas. 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 o que incluso si pagan por acceder a otros contenidos o redes también se incluya la misma política de privacidad de brindar acceso voluntario a sus datos y registro de actividades.

9. 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.
Hemos realizado un recorrido a través de la infraestructura de Internet para comprender el modo de transmisión y transporte de información materializada en BITS, así como el rol

1DOC3 (consultas medicas gratis), **AGRONET** (sitio Colombiano de apoyo a la agricultura), **REPARACIÓN INTEGRAL A LAS VÍCTIMAS** (página Colombiana para los victimas de la violencia), **24 SYMBOLS** (libros gratis) http://www.ungeekencolombia.com/el-lado-oscuro-de-internet-org/ Consultado el 3/9/2015

[29] http://www.google.com/loon/ Consultado el 3/9/2015

[30] 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 3/9/2015

central de las ISP y de las páginas de contenidos y aplicaciones en este tráfico de datos y por ende sus peligros y posibilidades de acción.

Luego, hemos analizado diversas definiciones teóricas del principio/concepto de Neutralidad de la Red, observando como múltiples autores y debates se focalizan en su problemática 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.

Hemos explicado cómo estas prácticas por parte de las ISP, y permitidas por los Estados Nacionales por su reglamentación o su omisión, ponen en jaque al principio de Neutralidad de la Red y a los postulados de libre acceso, democratización y potencialidad que esta esgrime y hereda del "espíritu primigenio" de Internet. De este modo, podemos apreciar que pese a ser fuertemente oligopolizados los niveles de Infraestructura y el Hardware (Zukerfeld, 2014), la Neutralidad de la Red sobrevive y se desenvuelve gracias al carácter descentralizado del packet switching y su principio de "mejor esfuerzo", y por ende es principalmente en la capa de enlace (Cortes Castillo, 2013), donde las ISP y los Estados intentan y pueden actuar.

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, incluso pese a reglamentar el debate económico a favor de los usuarios como es en el caso de Brasil. 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 de los usuarios, siendo funcionales al modelo capitalista imperante de un modo más encubierto y naturalizador.

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 ella 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.

Cabe destacar que este panorama de violación al principio de Neutralidad de la Red por parte de empresas y Estados remite tanto a la modalidad de Apropiación Incluyente como Excluyente sin que una priorice sobre la otra. En cuanto a la Apropiación Incluyente, el acceso gratuito a sus páginas, aplicaciones y contenidos conlleva en sí la aceptación voluntaria de la

discriminación y el registro de sus datos, producciones y actividades, culminando en los proyectos de Internet gratuita (Internet.org y Loon) los cuáles se constituyen bajo la lógica del rastreo y almacenamiento de los datos de los usuarios que desean utilizarlos y que a su vez discriminan sus datos al permitirles acceder a ciertos contenidos (seleccionados de forma totalmente intencional a base de tratos y alianzas con empresas y Estados) y no otros. En cuanto a la Apropiación Excluyente, los cercamientos artificiales se ponen en manifiesto en el bloqueo o estrangulación del flujo de datos, por parte de las ISP en conjunción con las empresas "propietarias" de esta información en ciertas circunstancias determinadas, o en el cobro de servicios adicionales tanto en lo que respecta a acceso como a velocidad, discriminando los datos, información y bienes informacionales cuyo valor y replicabilidad en principio es la misma (tendiente a cero), generando de este modo un plusvalor donde antes no lo había.

Podemos apreciar de esta forma como las leyes e iniciativas de la Propiedad Intelectual ingresan a la problemática al constituir el marco regulatorio acerca de **que** se debe discriminar para "preservar los intereses comerciales de las empresas", sumando a esto un claro ejercicio ideológico sobre los usuarios acerca de la propiedad y la gratuidad de las acciones y accesos en Internet.

De este modo, vemos que la Neutralidad de la Red, la cual se estableció como un principio rector de los primeros tiempos de Internet donde la centralidad estaba dada por el intercambio libre, seguro y veloz de datos e información bajo un ideal de su potencial emancipador (Matsushita, 2014), hoy día se encuentra fuertemente amenazada por la misma dinámica de apropiación del actual modelo capitalista. Esto hemos podido analizarlo al ver la dinámica de acción tanto de Empresas como de Estados en pos de favorecer ambos modelos de apropiación, los cuáles implican en si mismos la violación del principio para generar ganancias, ya sea con el cercamiento a la libre difusión de información en sus múltiples formas o con la violación de la intimidad de esos datos (y de sus usuarios) para su uso comercial o represivo.

Sin embargo, aunque este panorama parece ser totalmente oscuro, cabe destacar que siempre a un poder le corresponde un contra poder.

Siguiendo a Assange (2013) la solución frente a la vigilancia constante puede estar en nuevos y más efectivos métodos de encriptamiento de los datos, que no solo codifiquen y vuelvan difícil de acceder a los datos de contenido, sino incluso a los datos de tráfico.

En la actualidad existen múltiples aplicaciones, programas[31], softwares de licenciamiento libre, redes privadas virtuales que reemplacen a los ISP, entre muchas otras opciones capaces de ofrecer una encriptación mayormente segura y capaces de incrementar la seguridad en los intercambios de información.

[31] Tor, PeerBlock, Ghosty, entre muchos otros

Estos programas y aplicaciones son el fruto del trabajo de diversos grupos, movimientos y agrupaciones cuyo accionar busca confrontar con el modelo de capitalismo imperante brindando diversas alternativas a los usuarios para intentar potenciar su experiencia en la red de modo seguro de acuerdo con los valores e ideales "primigenios" de Internet.

Si bien el principal problema que enfrentan estos grupos es la falta de información sobre ellos (desconocimiento) o la desconfianza acerca de la utilización de las aplicaciones creadas por ellos, **ya que justamente, la información/conocimiento es el principal elemento en juego de esta sociedad**, podemos afirmar que su mera existencia y continuo desarrollo es ya un signo de que no todo está dicho.

La Neutralidad de la Red se erige como un **campo de batalla** entre los que la defienden al sostenerla como pilar de los valores "primigenios" de Internet y quienes promueven su violación y hasta desaparición en pos de fomentar su modelo de ganancia y control. Es así como esta problemática pasa a tomar en nuestros días un carácter de gran visibilidad[32] en torno a pensar las potencialidades de que este principio persista pese al contexto y acciones adversas y pueda en el futuro ser un importante punto de referencia para construir "otra Internet posible", distinta del modelo propiciado por el capitalismo imperante.

De este modo y teniendo en cuenta tanto al poder como al contra-poder, podemos apreciar que la batalla por la Neutralidad de la Red y la configuración acerca no solo de qué Internet será posible, sino principalmente, **de que sociedad será posible** solo acaba de comenzar.

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 Consultado el 3/9/2015

ASSANGE, J (2013) "Criptopunks: la libertad y el futuro de Internet". Marea Editorial, Madrid.

BOUTANG, Y (2004) "Riqueza, propiedad, libertad y renta en el capitalismo cognitivo" en AA. VV. Capitalismo cognitivo, propiedad intelectual, y creación colectiva, Madrid: Traficantes de sueños.

[32] Esta visibilidad no solo se da por las diversas posiciones y por las leyes y regulaciones de los Estados Nación, sino también por el debate acerca de si la Neutralidad de la Red puede considerarse un Bien Público y por tanto protegido de toda discriminación explícita http://geeksroom.com/2015/02/la-fcc-declaro-a-internet-como-bien-publico-asegurando-la-neutralidad-de-la-red-netneutrality/92252/ Consultado el 3/9/2015

CAFASSI, E (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
FERNÁNDEZ, P (2014) "NEUTRALIDAD DE LA RED: TENSIONES PARA PENSAR LA REGULACIÓN DE INTERNET" Revista Questión, 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 (2005) "Crítica de la información", Buenos Aires, Amorrortu Editores.
MATSUSHITA, T (2014) "El derecho, la sociedad de la información y el principio de la neutralidad de red: consideraciones sobre el mercado y el acceso a la información" Revista de Derecho, Comunicaciones y Nuevas Tecnologías Número 11. Facultad de Derecho, Universidad de los Andes. Disponible en http://dialnet.unirioja.es/servlet/articulo?codigo=4759634
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, E (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, M (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, M (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, M (2014) "Todo lo que usted quiso saber sobre Internet pero nunca se atrevió a googlear." Revista Hipertextos, 2(1), pp. 64-103.