REVCOM
REVISTA CIENTÍFICA DE LA REDCOM
RedCOM
ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 120

El péndulo entre la libertad de información y la seguridad: caso "Deep Web"

Francisco Piccini

UNIVERSIDAD DE BUENOS AIRES

pancho_piccini@hotmail.com

Resumen

El artículo aborda la pendulación entre libre circulación de la información y la privacidad vs. la seguridad y el control, que se produce por los fuertes intereses que intervienen en ambos polos. Frente al caso de la *Deep Web,* por su ambigüedad intrínseca, la posición de la sociedad civil que es ajena a ella levanta las banderas de uno y otro lado. Relacionar esta pendulación con la *Deep Web* y los espacios de internet permite que los Estados nacionales y su legislación actualicen su rol de soberanos sobre las sociedades que representan.
Las posiciones más duras de este conflicto, en orden de jerarquía, están encarnadas en las potencias mundiales y los motores de búsquedas y navegadores más populares. A nivel de la sociedad civil, además de los que navegan por la superficie, encontramos los que utilizan la *Deep Web* como herramienta de información y comunicación segura y los que la utilizan para delinquir.

Palabras clave: internet, Deep Web, privacidad, seguridad

Introducción

En el presente trabajo analizamos las tensiones y debates sobre seguridad en internet. El movimiento pendular entre libre circulación de los sujetos y de la información, por un lado, y la seguridad y el control, por otro, es moneda corriente, y serán utilizados de ahora en adelante como marco amplio de indagación. En particular, se problematizará el fenómeno *Deep Web* como caso límite para ver hasta dónde los actores y los discursos que éstos sostienen son arrastrados, matizados o radicalizados, en pos de sus objetivos. Las preguntas que se proponemos abordar son: ¿Es la *Deep Web* un espacio estrictamente delictivo pero libre, y como tal fundamentalmente opuesto a la *internet superficial*? ¿Qué sucede con la libertad de

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 121

expresión cuando la sociedad civil levanta la bandera de la seguridad en la red? ¿Qué rol le toca cumplir a los Estados nacionales frente a las potencias mundiales políticas y económicas en relación a un espacio virtual que no admite fronteras? Estamos entendiendo, a partir de las preguntas que, como dice Manuel Castells, aún cuando los actores que traiga a colación este conflicto sean diversos, internet, a fin de cuentas, "sufre, como todo lo demás, la presión implacable de dos fuentes fundamentales de dominación que todavía planean sobre nuestra existencia: el capital y el Estado". (2009:164)

A partir de una revisión bibliográfica se introducirán los antecedentes que informan esta pendulación. Se describirá la arquitectura de internet y las posibilidades de navegación que orienta en relación a la *Deep Web*. Esto ayudará a tener una caracterización técnica y amplia de este fenómeno. Nos detendremos en el conflicto de intereses entre la *Deep Web* y los buscadores e indexadores de internet, conflicto que habilita un terreno de posicionamientos permanentemente conflictivo, sobre todo para la sociedad civil, que es aquella que encarna la balanza siempre inclinada entre seguridad y privacidad. La *Deep Web,* a partir de un perfil técnico aparentemente neutral, tomara matices de ambigüedad cuando se articule con uno y otro lado de la balanza.

Siempre en el marco general de la balanza inclinada entre privacidad/libertad de expresión e información y seguridad/control, vale entender que todo conflicto implica relaciones de poder. Serán ilustradas la vigilancia y la censura que pueden encarnar los navegadores y buscadores online, presentando nuevos modelos de control social, cuando de intereses encontrados entre la privacidad y la seguridad se trata. Ahondar en este sub conflicto del trabajo es útil para que, apoyándonos en entrevistas a actores relevantes del campo, podamos construir una mirada más sistemática sobre las posiciones y las contradicciones de la sociedad civil frente al binomio par seguridad/control y privacidad/libre circulación.

Se identificarán dos posiciones que se pueden tomar respecto a los fenómenos de internet, y cuáles son las contradicciones en que incurre la sociedad civil al asumir una posición u otra. Por un lado, la libre circulación de la información en las redes, la no vigilancia de los sujetos en internet y, seguidamente, la privacidad, son valores que los *hackers*, numerosos investigadores y organismos que abogan por los derechos a la libertad de expresión en internet se apropian, pero principalmente la sociedad civil lo hace. Por otro lado, las tomas de posiciones que se refieren a la seguridad en internet, y por lo tanto al control, son asumidas por los organismos de gobiernos de las potencias mundiales, acompañadas por las grandes empresas multimediáticas (como Google), pero también por la sociedad civil, cuando se ve

escandalizada frente a los delitos que pueden cometerse a través de las redes. Como si fuera una balanza, cuando se habla de la libre circulación de información y la privacidad, el discurso de la seguridad encuentra una contraparte de peso, y viceversa. Se producen divisiones verticales en los actores de la sociedad civil con repercusiones de grados diversos.

Escenario vertiginoso y actores en conflicto

En el presente trabajo analizamos las tensiones y debates sobre seguridad en internet. Cierto es también que habrá otros subtemas que estarán pivoteando junto a este, aunque se tocarán de soslayo: la restricción a la circulación de información online, la educación en nuevas tecnologías de la información y las zonas grises, posibilidades y probabilidades de una efectiva gobernanza de internet. En término del cuadrante que propone Lawrence Lessig (1998), donde el mercado, las normas culturales, las leyes y la arquitectura son las formas de regular una tecnología de la información y la comunicación, en este caso el análisis comenzará apoyándose sobre las regulaciones por arquitectura que construyeron internet y aquellas programaciones de software que dieron lugar a la *posibilidad técnica del anonimato,* para luego poder afrontar, una vez desarrollado el núcleo del conflicto que desata la *Deep Web* y las posiciones pendulares*,* las normas culturales que adoptó la sociedad de internautas respecto al uso del contenido web, y que obligan a pensar los intersticios de la relación donde debería trabajarse para equilibrar la balanza.

En 2005 se tenía un estimado de 1.000 millones de usuarios de internet a nivel global (Kurbalija y Gelbstein, 2005), y según el último reporte de Internet Society (2014), para 2015 se proyectan 3.000 millones. Teniendo en cuenta que la población mundial para 2013 ronda los 7.000 millones de personas (Centro de Noticias ONU, 2013), esto nos plantea que más de un tercio de la población mundial circula en internet. Esta concentración mundial de la población, encuentra en internet un ámbito colectivo de comunicación y circulación de información y comunicaciones, ha traído consigo la evolución espontánea de la regulación y la gestión de internet (Abbate, 1999; Castells, 2001 en Castells, 2009).

Pero esas 3.000 millones de personas que circulan por internet, ¿por dónde circulan? Puede ser una pregunta extraña a primera vista, pero este trabajo tiene por objetivo tomar un fenómeno particular del ciberespacio y observar cómo las tensiones entre la vigilancia y el control social chocan y rebotan cuando la circulación de información online y la privacidad son banderas que la sociedad civil elige levantar frente a estos poderes. El fenómeno en cuestión es **la *Deep Web.* Bajo este nombre se conoce a aquellas páginas web o contenidos online**

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 123

que no serían accesibles a través de los buscadores y/o navegadores más utilizados por los internautas.

Durante el desarrollo de este trabajo, se intentará ver qué rol cumple y podría cumplir la *Deep Web* en un entorno donde actores tan poderosos como el capital y los gobiernos ponen especial interés en que internet sea un lugar seguro y por lo tanto controlado, siendo esto pre-condición para hacer de la red de redes un lugar económicamente rentable y políticamente útil. A través de los discursos que entre una y otra parte sostienen para legitimar posiciones, con los cuales se puede pensar en un binomio complejo entre seguridad y control *vs.* privacidad, libre acceso y circulación de la información, a través de estos discursos, repetimos, se verá que el plano de batalla, porque así es la internet, tiene posiciones globales y actores fundamentales a nivel mundial. Hay una red de influencias a nivel mundial que circula por las venas de internet. Pero como tal, también se verá que a medida que las posiciones se van endureciendo, el lugar de debate pasa a ser regional o llanamente local, y los Estados nacionales tienen la posibilidad de erigirse entonces en los nuevos *guardianes de internet*, como los llama Tomás Maldonado en *Crítica de la Razón Informática* (1998). Internet "sufre, como todo lo demás, la presión implacable de dos fuentes fundamentales de dominación que todavía planean sobre nuestra existencia: el capital y el Estado" (Castells, 2009:164).

¿Pero la *Deep Web* es un único actor? ¿Qué comprenden "el capital y los gobiernos"? Los actores que se presentan en el escenario de este trabajo son muy variados, y pueden ser institucionalmente gigantes o pequeños actores capilares perdidos en las redes de internet. En jerarquía, a la cabeza de este bloque está Estados Unidos y las instituciones que ha fundado (algunas *ad hoc)* para regular o controlar los espacios donde circula información en internet, como la CIA y el Departamento de Defensa de Estados Unidos. Las potencias económicas son las más interesadas en regular lo que sucede por las carreteras de internet, no sólo para hacerlo económicamente rentable sino apoyándose en el discurso de la seguridad a nivel mundial. En su mismo nivel de importancia para este trabajo, están los llamados "guardianes de internet": las empresas que desarrollan los motores de búsqueda como Google, Yahoo o Bing, o los navegadores populares como Google Chrome, Mozilla Firefox o Internet Explorer. Estos actores son los encargados de *construir* para la mayor parte de los internautas una determinada realidad social informática, ya que, para la mayor parte de aquellos, a través de sus algoritmos y sus índices la información tiene su *socialización primaria* (Berger y Luckmann, 1978).

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 124

A nivel de la sociedad civil, encontramos que la *Deep Web* segmenta verticalmente a la sociedad de acuerdo a sus intereses y los convierte en actores conscientes y no de la lucha por la libre circulación de información online y la privacidad. Por un lado encontramos a aquellas personas que utilizan efectivamente las herramientas que ofrece la *Deep Web* creando dominios, portales o foros de chat o comercialización por fuera del circuito de información *visible.* Complementarios en este análisis, está siempre latente el ataque de *crackers.* Por *crackers* se entiende a los individuos que pululan en la *Deep Web* y cuya actividad consiste en robos de identidad, de datos bancarios, de IP, entre otros. Su único fin es cometer actos que, desde el punto de vista de los gobiernos y la sociedad civil que se mueven por la *superficie de internet*, son llanamente delictivos[1]. Detrás de todo esto, quizás expectante, se encuentra el resto de la sociedad civil que no circula por la *Deep Web* sino por la *internet superficial*, utilizándola para su vida cotidiana, trabajo, comunicación y divertimento. Este actor es importante por las banderas que levanta a favor de la privacidad de sus datos, pero sin reconocer el partido que se juega, siendo que cualquier lado de la balanza que se incline le traerá tantos favores como derrotas.

La posibilidad técnica del anonimato

Lo esencial que hay que tener en cuenta para entender las problemáticas que desata la *Deep Web* es la posibilidad técnica de anonimato, ofrecida por los softwares que permiten acceder a ella[2]. Pero vayamos al principio.

Jovan Kurbalija explica claramente la arquitectura técnica básica:

> El principal estándar de internet que especifica la manera en que se trasladan datos es el protocolo para el control de transporte/protocolo de internet (TCP/IP), el cual se basa en tres principios: conmutación de paquetes, redes punto a punto y robustez. La red entre uno y otro punto terminal es neutral y no evita el desarrollo y la creatividad en los mismos. Esto significa que las aplicaciones que corren en internet pueden ser diseñadas en los bordes de la red sin requerir permisos por parte de los operadores y otras partes. (2005: 42)

1 Esta posición de la sociedad civil está justificada en el Anexo, donde se agregan casos en los cuales la participación de organizaciones de la sociedad civil fue clave para la promulgación o revocamiento de leyes referentes a la pornografía online, la privacidad y los delitos informáticos.

2 A los fines de este trabajo, remarcar la diferencia entre el hecho de que el anonimato sea una posibilidad técnica de un software específico que *además* permite acceder a la *Deep Web* no hace a la cuestión, siempre y cuando las dos características sean ofrecidas por un mismo actor. En este caso, con el navegador Tor. En un navegante que solamente curiosea por la *Deep Web,* es claro que el anonimato le es irrelevante.

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 125

Estos números IP son como documentos de identidad únicos que posee cada dispositivo que se conecta a internet. El desarrollador de este protocolo fue la IETF (Fuerza de Tareas de Ingeniería para Internet), siendo fundamental en los orígenes de internet -y hoy- para garantizar la conmutación de paquetes entre dispositivos, para lo cual previamente debió imponerse su uso. Es claro entonces que esta arquitectura pilar de internet no fue diseñada pensando en la seguridad, sino en la libre circulación de información y todo el potencial que este conllevaba. En este contexto es que tiene su origen la ética *hacker. "*La misma arquitectura se convirtió más adelante en el cimiento para el desarrollo de la creatividad y la libertad de expresión en internet" (Kurbalija, 2005: 16).

Sin embargo, cuando internet tuvo la explosión que tuvo, con crecimientos exponenciales, la seguridad apareció como tema de agenda. Kurbalija sostiene que por este crecimiento de la población de internautas fue que se crearon soluciones *ad hoc* como los cortafuegos, el antivirus y el software de codificación, pero que un tratamiento de raíz del problema de la seguridad implicaría hacer cambios sustanciales en el estándar TCP/IP.

Al entrar a la *Deep Web* se aprovechan las posibilidades técnicas que ofrecen algunos navegadores de ocultar esa dirección IP propia. El ejemplo clásico, siendo el software más usado para acceder al mundo subterráneo de internet, es el navegador Tor. Con este navegador se es técnicamente un anónimo capaz de producir mensajes. Esto revela que, si con este navegador es posible acceder a contenido con diferentes codificaciones y enrutamientos que se encuentran en la *Deep Web*, es porque del lado de los navegadores y buscadores tradicionales hay una decisión voluntaria de no ofrecer esos contenidos como parte de la realidad virtual que construyen -y esta decisión, como tal, es política.

La ambigüedad técnica de la *Deep Web* y las luchas de poder que inclinan la balanza

En este apartado, se ahondará ampliamente en el conflicto que desata el uso de la *Deep Web* que hacen los *crackers* y aquellos usuarios que no la utilizan para delinquir, y cómo estos usos resultan por igual castigados cuando los actores a cargo de la seguridad deciden entrar en acción. Hay que tener en cuenta, en este sentido, la condición fundamentalmente ambigua de la *Deep Web,* según la perspectiva y el actor que la mire, lo que fundamenta que la balanza esté continuamente inclinada de acuerdo a las coyunturas en conflicto.

Hay actores de la sociedad civil, capilarmente distribuidos en la red social, que tienen intenciones delictivas y otros con una ética basada en la cultura del compartir; hay empresas proveedoras de internet; hay gigantescas multinacionales cuyo negocio atraviesa la circulación

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 126

de información online y fuertes presencias gubernamentales que, en muchos casos aliadas a las gigantes multinacionales, persiguen el fin de hacer de internet una comunión de intereses corporativos. Ahora bien, ¿cuáles son los conflictos que reúnen a estos actores? ¿Por qué una persona que tipea en su buscador favorito la información que solicita está relacionada con un *cracker* y con la designación de IPs hecha por la IETF? Las preguntas que guiarán la argumentación de este trabajo giran en torno al binomio complejo antes dicho: por un lado los gobiernos de las potencias mundiales y los «guardianes de la internet», detentores de la seguridad y poderosas empresas que ofrecen un servicio de búsqueda de contenido online; por otro lado, la protección de la privacidad con la que se embandera la sociedad civil y la lucha por la libre circulación y recepción de información online de los difusores y portadores de la información reñida con los intereses globales. El principal hincapié será hecho sobre el papel de la sociedad civil que circula por la superficie de internet, y cómo el discurso que sostienen hace crujir los fundamentos de uno y otro lado, siendo entonces un actor vital por su pendulación.

Se ha dicho que la *Deep Web* son aquellas páginas web o contenidos online que no serían accesibles a través de los buscadores y/o navegadores más utilizados por los internautas. Sin embargo, hay portales y sitios web que llevan esta posición –y tienen motivos para ello- a un extremo. No serían sólo ese guardián frente al castillo que cuando se le solicita el ingreso se limita a decir que no. Directamente *esconden su castillo.* No sólo hay un cifrado. También utilizan diferentes estrategias para *eludir* el alcance de indexación y enrutamiento de los motores de búsqueda tradicionales (Google, Yahoo, Bing): diseñan sus URLs con formatos que son incompatibles con el diseño de los navegadores más usados; se multiplican con *sitios espejos*; o directamente sus documentos están redactados en formatos no indexables.[3] En estos sitios, a esta posibilidad de no ser indexado que dio imaginación a la metáfora de superficie-profundidad de internet, se los conoce como *Deep Web.* En tanto tal, podemos ver que la *Deep Web*, como afirma Christian Borghello, constituye “una *herramienta* como cualquier otra que puede ser utilizada para el bien, para el mal o para todos los grises que hay en el medio”[4]. Es una herramienta de la arquitectura de internet.

“¿Pero no me perjudica que los buscadores no indexen contenidos que podrían serme útiles?”, podría preguntarse la sociedad civil que vive su vida cotidiana en la *superficie* de

3 Se refiere a eludir los estándares de contenidos y aplicaciones de los que da cuenta Kurbalija (2005).

4 Entrevista a Christian Borghello, director de Segu-Info y co-fundador de ODILA, realizada por el autor en mayo de 2015.

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 127

internet. Sin embargo, a pesar de la ingenuidad, esta pregunta pone sobre la mesa dos cuestiones cruciales: la cuestión del ¿por qué? de la *Deep Web,* y la otra referente al ¿qué?

Los límites de la balanza sobre la seguridad y el control

En primer lugar, la *Deep Web* es una zona muy conflictiva de internet, y desde el punto de vista de los organismos de gobierno, ilegal. En ella se pueden encontrar servicios financieros (cuentas de PayPal robadas, tarjetas de crédito clonadas, falsificación de billetes), servicios comerciales (explotación sexual, mercado negro, armas y munición, asesinos a sueldo, documentación falsa y drogas), archivos clasificados de gobiernos y diplomáticos (caso Wikileaks), una inmensa biblioteca gratuita de archivos digitales, servicios de *hosting* y almacenamiento irrestricto, entre otros. Como se puede observar, las actividades nombradas pueden fácilmente ser tratadas desde la ilegalidad si uno lo mira desde la perspectiva de un gobierno X y desde la moral pública de la sociedad civil. Son claros los intereses de "no salir a la superficie" de muchas de estas actividades. Pero si se mira con atención se verá que en el conjunto de esas actividades, hay algunos conceptos que crujen.

No se discutirá los intereses de los *guardianes de internet* en acabar con el robo de cuentas bancarias, tarjetas, la lucha contra la pedofilia, la explotación sexual o el mercado negro, porque la solución de estas problemáticas son apoyadas también por la sociedad civil[5]. Pero cuando se habla de circulación de información la balanza de la seguridad encuentra una contraparte de peso, y se producen divisiones verticales en los actores de la sociedad civil con repercusiones de grados diversos. Se nombró Wikileaks por ser un caso famoso y de alcances mundiales, y que ejemplifica claramente qué sería una información "confidencial" de repercusiones mundiales y locales, pero dentro de este contrapeso también se incluye a diversos medios de comunicación, a los gobiernos que utilizan el espionaje como defensa/ataque frente a otros espionajes y a actores de la sociedad civil que apoyan la cultura del compartir.

Los límites de la balanza sobre la privacidad y la libre circulación de información

Esta posibilidad técnica del anonimato en la *Deep Web* les proporciona a los actores antes nombrados las posibilidades de hacerlo sin consecuencias dolorosas. Es decir,

5 En el *Anexo de enlaces* se encuentran notas periodísticas que dan cuenta de debates sobre leyes en los que la participación de la sociedad civil fue relevante, sea para su promulgación o para su revocamiento.

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 128

considerando el caso hasta acá, la libertad de expresión y de circulación de información estaría garantizada, porque, como bien dice Castells, lo único que podrían hacer los gobiernos frente a esto es *perseguir* (2009: 161), y nada más. Pero entre las personas que reciben la información en internet, y aquellas que la trabajan y difunden, hay actores que son los encargados de mover la información desde los difusores hasta los ciudadanos a pie: los intermediarios son los navegadores y los buscadores.

Según StatCounter (2015), uno de los dos productores de estadísticas actualizadas sobre usos y costumbres de internet a nivel mundial, en la actualidad Google Chrome sería el navegador más usado a nivel mundial (49,24% a mayo del 2015), seguido muy atrás por Internet Explorer y Mozilla Firefox. En cuanto a motores de búsqueda, las empresas radicadas en Sillicon Valley siguen siendo las más utilizadas por los usuarios de internet, aunque la presencia del gigante chino Baidu también influye.

Como dice Castells (2009) cuando habla de la «googlearquía», los motores de búsqueda en línea se configuran de tal forma que necesitan la participación tácita, aunque no necesariamente consciente, del usuario final. Es decir, la capacidad de indexar o no indexar que tiene Google con sus *web crawlers*[6] y la probabilidad de que los ciudadanos puedan acceder a información valiosa que circula por fuera de la *internet superficial* es un ciclo que se realimenta a sí mismo. Esto puede –y funciona- como un cuello de botella que favorece a los gobiernos que intenten tanto ofrecer seguridad como controlar lo que una sociedad busca, sabe, conoce a través de las redes. Christian Borghello lo plantea en estos términos:

> Está la política que ellos [Google] están obligados a cumplir, que si esa información que ellos indexaron no cumple con todos los requisitos legales y de «limpieza» que deberían tener, la sacan del índice, o no te la muestran en realidad: está pero no te la van a mostrar. No va a estar indexada, pero ellos la van a tener[7].

Sin embargo, como dice Lessig (1998), "las comprensiones o expectativas acerca de cómo uno debe comportarse, expectativas impuestas mediante las comprensiones o expectativas de casi los miembros de una comunidad" –en este caso, la digital-, construye un *sentido común digital* al que respondemos, un hábito profundamente arraigado de nuestro comportamiento en la web, y tiene especial importancia a la hora de hablar de seguridad, privacidad y libre acceso a la información. ¿Cómo se llegó a la situación donde casi la mitad de los internautas usa un único navegador, el Google Chrome? ¿Qué sostiene a www.google.com

6 Para ver más sobre los *web crawlers,* visítese http://www.robotstxt.org/.

7 Entrevista a Christian Borghello realizada por el autor en mayo de 2015.

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 129

como el principal motor de búsqueda hoy 2015? ¿Estamos hablando sólo de una situación monopólica agresiva de Google que coorta a usar su buscador?

Se podría nombrar muchísimos servicios que permitirían abrir nuevos y más amplios canales para la circulación de información, y que tienen una política menos cerrada que los softwares tradicionales, sea por el anonimato o por la construcción de la realidad que hacen: DuckDuckGo, Tor u Orbot son algunos casos. Estos servicios, en el marco de la balanza que estructura este trabajo, están imprimiendo su peso del lado de la privacidad y de la libertad de expresión y obtención de información en internet. ¿Por qué? Porque quien no puede saber la identidad de un internauta no puede crear algoritmos en base a su comportamiento en internet, y por lo tanto no puede *plegarse* sobre el usuario, creando determinado circuito de información que se cierra sobre sí mismo.

Esto es muy diferente respecto a lo que sucede con los buscadores tradicionales, como Google, Yahoo, y otros. Estos buscadores, cuanto más continuamente son usados, más cerrados sobre sí mismos se vuelven, y por contrapartida, menos abierto a información que no esté en relación con el contenido anteriormente buscado. ¿Entonces la solución sería dejar de usarlos? En nuestro recorrido, la balanza representada en un lado por la libertad y la privacidad y en otro por la seguridad y el control aquí empieza a trabajar sobre cuestiones más finas. La solución no es dejar de usarlos, o al menos no es tan simple como podría decirse, porque Google es cultural, al punto de que en muchos diccionarios se ha asumido como sinónimo de "buscar en la web". Pero antes que cultural, fue una sistematización de un uso, de un sentido común y una costumbre que finalmente derivó en una aceptación sin cuestionamientos (Hayek, 1980, citado en Maldonado, 1998: 45).

Aún existiendo las herramientas que permitirían al gran sector de sociedad civil que navega actualmente por la *superficie de* internet utilizar servicios que privilegien su privacidad y su libertad de acceso a la información, y por lo tanto detener el movimiento pendular de la balanza, esto no sucede por sí mismo.

Cierto es que la sociedad civil, la "opinión pública", nunca se ha expresado a favor o en contra del uso de estas herramientas de búsqueda, ni de ningún navegador, ni parecidos. Para sostener esto me baso en que no hay legislaciones, proyectos de ley, presiones de representantes políticos o movimientos de organizaciones no gubernamentales que exijan una puesta sobre la mesa de lo que conlleva usar un determinado motor de búsqueda u otro. En 2015 la Unión Europea ha intimado a Google por favorecer a través de su buscador productos propios de la misma empresa, acusándosela de «posición dominante». Google, a través de su

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 130

vicepresidente Amit Singhal, se defendió con una obviedad: "Aunque Google quizás sea la herramienta de búsqueda más usada, *la gente ahora puede encontrar y acceder a la información de numerosas formas*, y las alegaciones de daño a los consumidores y competidores están muy lejos de la realidad" (2015).

¿Pero está dispuesta la sociedad civil a abandonar usos y costumbres que riñen con su libre acceso a la información, en pos de defender su derecho a la privacidad y a no ser observado y controlado mediante la información? ¿Es la *Deep Web* y la posibilidad técnica del anonimato el núcleo duro de la libertad en internet, y por lo tanto hacia el que deberíamos trabajar? ¿Es un hábito digital profundamente arraigado el límite de la balanza?

El fin del sueño *Deep Web* y la sociedad civil

Anteriormente dijimos que la posibilidad técnica del anonimato en la *Deep Web* encarnaría, entonces, la libertad de expresión y de circulación de información estaría garantizada. Según Castells (2009), la preocupación fundamental de la mayoría de los gobiernos es establecer normas para controlar internet y encontrar mecanismos para ejercer este control según la ley y el orden. Pero sostiene que hay motivos serios para dudar de la eficacia de los controles cuando van dirigidos a la comunidad de usuarios en general. Si nos guiáramos por esta idea, podríamos efectivamente pensar a la *Deep Web* como encarnando la *neutralidad informacional de la red,* donde ningún contenido sería discriminado, incluso aquellos patentemente conflictivos, como el contenido pedófilo. Christian Borghello refuta este planteo:

> Creo que la *Deep Web* es una forma de publicar o de exponer cosas que normalmente la gente no expondría en un medio público, por pudor, por miedo o por equis motivo. No lo vería como *neutralidad* en la red. Yo creo que ser *neutral* en la red significa que todos tenemos acceso a lo mismo, al mismo ancho de banda, al mismo tipo de información, y *eso en la Deep Web no pasa*. Supuestamente, si vos estás en la Deep Web y entraste por Tor, sos anónimo. No es tan así. Estás un poco más oculto, pero no estás anónimo. Todo depende de qué tan *objetivo* te transformás. ¿Qué significa esto? Si vos sos un *high profile*¸ que está siendo investigado por narcotráfico, por pedofilia, por una causa importante, y te transformaste en un *blanco*, tarde o temprano te van a encontrar[8].

Entonces la larga cita de Borghello refuta la *posibilidad del anonimato.* En términos de Maldonado (1998), podríamos decir que existe la *probabilidad* de pasar anónimamente por la

8 Entrevista a Christian Borghello realizada por el autor en mayo de 2015.

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 131

Deep Web y tener una actividad más o menos dinámica. Pero la posibilidad efectiva de que esto se sostenga es baja cuando la información que se dinamiza te convierte en un «*high profile».* La *Deep Web,* más que mostrarnos las posibilidades y ventajas de las nuevas tecnologías de la información en asegurarnos los ideales de libre circulación y privacidad, nos revela sus limitaciones. Antes que asegurar, gracias a su posibilidad técnica nacida de la arquitectura de internet, un espacio de circulación de información y libertad en internet, nos señala los límites.

En esta orilla a la que hemos hecho llegar a la *Deep Web*, el discurso de la sociedad civil asume dos caras contradictorias. Cuando defiende su derecho a la privacidad, y como caso reciente tenemos a las discusiones en torno a *Pyraweb,* Marcelo Temperini sostiene que la sociedad civil "actúa como si sus derechos no entraran en colisión con otros".

> Creo que la información la tenemos que tener para combatir cualquier tipo de delito. Para mí es necesario para intentar avanzar en agarrar a los delincuentes. En *Pyraweb* se argumentó que los criminales más peligrosos utilizan herramientas de anonimización o cifrado, imposibilitando que sean fácilmente encontrados. La realidad es que la mayoría de los delincuentes no saben tanto. Y es gente que se la puede encontrar. Lo que hay de fondo en esa ley es defender las libertades de internet asociando que tener determinados datos significa vigilancia masiva.[9]

Al mismo tiempo que se entiende que intensificar la búsqueda y recopilación de información tiene como contrapartida el resquebrajamiento de la esfera privada, también se observa que este accionar se apoya en el argumento de que esta búsqueda proporcionará mayor seguridad a los ciudadanos. Las banderas de la sociedad civil están en todos lados, y por lo tanto en ninguno. ¿Con qué posibilidades y probabilidades cuenta la sociedad civil, y con qué herramientas, para asumir su contradicción y superarla?

El rol del Estado y la necesidad de políticas digitales

Marcelo Temperini plantea que "en la Sociedad de la Información, cuanto más seguridad tenés, cuanto más seguro es un sistema, más le vas quitando del otro lado: menos acceso, menos transparencia. Es un tema que yo creo que no tiene una solución. Tiene *momentos*. El

9 Entrevista a Marcelo Temperini, director del sitio El Derecho Informático, fundador de Asegurarte y co-fundador del Observatorio de Delitos Informáticos de Latinoamerica, realizada por el autor en junio de 2015.

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 132

tema es entonces ¿qué privilegiamos?"[10]. No estaría lejos de la verdad decir que defender a los ciudadanos implica, en algún punto, atacar a otros actores, es decir, tener una seguridad ofensiva. Temperini cree que en Argentina esa idea aún no está clara para los gobiernos, lo cual posicionaría al país en la balanza de la protección de datos privados, a contracorriente de lo que sucede a nivel mundial con las potencias.

Es claro también que si se alentara a un cambio de hábitos y apropiación en el uso de determinados softwares, éste debería ser un cambio *total*. Lo difícil no es investigar sobre posibilidades a nivel software para apoyar ese cambio de hábitos, sino si realmente va a ser usado ese software. Si se empieza a usar *Tor* para conservar el anonimato, es un despropósito usar www.google.com o el mismo Facebook. No sólo porque hay que cambiarse de sistema y acostumbrarse a un nuevo rendimiento del sistema operativo debido a lo que cuesta el cifrado, y en el transcurso abandonar protocolos, e incluso averiguar si nuestro proveedor de internet usa nuestros datos o no. Hay que preguntar antes ¿cuántas personas están dispuestas a dar este paso? ¿Cuántas personas dan el paso de verdaderamente averiguar que sucede con sus datos online?

> Argentina tiene una ley de protección de datos personales hace 15 años, ¿y cuánta gente conoce esa ley? ¿Cuántas empresas cumplen con las 25.326? ¿Cuánta gente hace un *habeas data* para darse de baja en alguna base de datos en la que figura sin su consentimiento? Esa es la hipocresía. Es una ley cuyo objetivo es proteger la privacidad, y hay un montón de disposiciones y hay un montón de herramientas para defenderse si realmente interesa la privacidad. Si yo explicara todo eso, ¿la gente se defendería? A la gente no le importa.[11]

Se podría agregar, como argumenta Temperini, que la noción de privacidad que ellos comparten es muy similar a las condiciones de privacidad que ofrecen los buscadores, navegadores y redes sociales mayormente usadas, y este nuevo paradigma versa sobre la idea de que la información personal es, en principio, pública.

¿Pero quién puede educar a una sociedad civil en sus derechos y responsabilidades? Resumamos: la *Deep Web* y otros servicios que abren nuevos y más amplios canales para la circulación de información, y que tienen una política menos cerrada que los softwares tradicionales, son los que obligan a la sociedad civil a hacer peso sobre el binomio privacidad/libertad de circulación de información. Pero debido a la condición fundamentalmente

10 Entrevista a Marcelo Temperini realizada por el autor en junio de 2015.

11 Entrevista a Marcelo Temperini realizada por el autor en junio de 2015.

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 133

ambigua de la *Deep Web*, utilizada también como un espacio para cometer delitos penales, los poderes de las potencias mundiales, junto a las grandes empresas radicadas en Sillicon Valley, entran en acción. Y este entrar en acción es ciego a los grises que presenta la *Deep Web*: este poder arrasa con delitos pero también con derechos. La sociedad civil apoya primero, pero después recula.

Debe prestarse atención entonces a que el verdadero partido pasa a jugarse al nivel de los Estados nacionales como los únicos que pueden tener soberanía ejercer protección sobre las sociedades que, aún cuando internet no contemple fronteras, están articuladas dentro de naciones diferentes. Además, los Estados nacionales se presentan como los únicos que pueden, vía legislación, llamar a un miramiento sobre lo que sucede en los espacios virtuales, y ponerse a la par de las grandes multinacionales y las potencias. Pero el trabajo del Estado como defensor de una soberanía que comprende a sus ciudadanos, no puede limitar el trabajo de defensa a una situación externa. La defensa interna también debe ser comprendida en esa regulación, que sería una regulación con los recaudos que señala Temperini[12]: si el Estado nacional decide observar, recopilar y almacenar los datos de sus ciudadanos para combatir delitos informáticos como la pedofilia, el tráfico ilegal, pasando por el *phishing* y el robo de identidades, ¿dónde quedarían esos datos? ¿En una dependencia del Estado o en un privado? ¿Qué situaciones ameritarían que esos datos sean revelados para una investigación? ¿Tienen todos los datos la misma relevancia? Y una más crucial: si el Estado se embarca en esta empresa, ¿no estaría tomando el problema por su final, cuando debería comenzar por verificar cuál es el Estado actual de los datos de sus ciudadanos en el mundo de internet, algo así como relevar el *estado del arte de la información personal pública?*

Como dijo Castells (2009), Internet sufre la presión implacable de dos fuentes fundamentales de dominación: el capital y el Estado, ambos como actores globales, pensando en que las grandes potencias no limitan sus redes de influencias a sus límites geográficos. Por lo tanto, es importante remarcar el rol de la sociedad civil como actor de peso, que cuenta con características específicas que le otorgan una importancia crucial en la inclinación de la balanza control *vs*. privacidad y libertad de expresión, principalmente por su carácter pendular en este binomio complejo. Si levantar la bandera por la defensa de los datos privados le trae tantos beneficios como problemas, significa que el trabajo a realizar, dentro del marco de posibilidades que dibujan las relaciones de poder e influencia a nivel mundial, es fundamentalmente educativo.

12 Entrevista a Marcelo Temperini realizada por el autor en junio de 2015.

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 134

También hay un gran trabajo por hacer en términos de *desmitificación.* Asumir una tarea educativa por parte de los Estados nacionales para conducir a sus ciudadanos hacia una concientización de la política de los espacios de internet, y dar cuenta que existen herramientas con un potencial legítimo para defenderse, como puede ser la ley 26.032 sobre la libertad de expresión en internet o la 26.388 sobre tipificación de delitos informáticos. Los principios "deben ser claramente establecidos a nivel políticas y no tácitamente asumidos a nivel técnico". (Kurbalija, 2005).

BIBLIOGRAFÍA

Singhal, A. [2015, 15 de abril], *The Search for Harm* [Documento en línea], Blog Oficial de Google. Disponible en: http://bit.ly/1FtVg6M. [Recuperado 2015, 17 de junio].

Assagne, J. (2014), *When Google Met Wikileaks*, London: OR Books.

Becerra, M. (2000), *De la divergencia a la convergencia en la sociedad informacional: fortalezas y debilidades de un proceso social inconcluso",* en Zer n° 8, Facultad de Ciencias Sociales y de Comunicación, Universidad del País Vasco, Bilbao.

Berger, P. y Luckmann T. (1978), *La construcción social de la realidad,* Buenos Aires: Amorrortu.

Castells, M. (2009), Regular la libertad: cuando la caperucita Internet encuentra a los lobos feroces corporativos (pp. 161-176), en *Comunicación y Poder*, Madrid: Alianza Editorial.

Castells, M. (s.f.), *Hackers, crackers, seguridad y libertad*, Lección inaugural del curso académico 2001-2002 [En línea], Universidad Oberta de Catalunya. Disponible en: http://bit.ly/1RcvyKI [Recuperado 2015, junio 15]

Centro de Noticias ONU (2013, 13 de junio), La población mundial crecerá en mil millones en la próxima década [En línea], español. Disponible en: http://bit.ly/1H66ZzH. [2015, 16 de junio].

Internet Society (2014, junio), *Global Internet Report 2014*. Disponible en: http://bit.ly/VI8BKg [Recuperado 2015, 14 de junio].

Katz, C. (1998), *El enredo de las redes* [Documento en línea]. Disponible en: http://bit.ly/1GrxdGv [Recuperado 2015, 20 de junio].

Keane, J. (2015) *Why Google is a political matter? A conversation with Julian Assange* [Entrevista en línea], publicado en The Monthly. Disponible en: http://bit.ly/1Rcvc71 [Recuperado 2015, 16 de junio].

Kurbalija, J. y Gelbsetein E. (2005) La canasta de infraestructura y organización, en *Gobernanza de Internet. Asuntos, actores y brechas,* DiploFoundation y la Sociedad para el Conocimiento Mundial, Malta.

Agencia France-Press (2015, 4 de abril), La acusación de Europa contra Google, en 5 puntos. [En línea], La Nación. Disponible en: http://bit.ly/1IR4i2v [Recuperado 2015, 12 de junio].

ISSN 2451-7836 | Año 1, #2, junio de 2016 | **Contribuciones** | Pág. 135

Lessig, L. (1998), "Las leyes del ciberespacio", conferencia Taiwan Net '98. Disponible en: http://bit.ly/1dMhMBO

Maldonado, T. (1998), *Crítica de la Razón Informática,* Barcelona: Paidós.

Pew Research Center (2015, marzo), *Internet Seen as Positive Influence on Education but Negative on Morality in Emerging and Developing Nations* [Documento en línea]. Disponible en: http://pewrsr.ch/1C0TsVU. [Recuperado en 2015, 20 de junio]

Statscounter [En línea]. Consultado en: http://gs.statcounter.com/ [Recuperado 2015, 14 de junio]

ANEXO DE ENLACES

- Sobre la ley Pyraweb y los actores involucrados: http://bit.ly/1Txo6hi.
- Nota en diario Perfil (16/11/2013) sobre la sanción de ley de Grooming en Argentina y los debates que alentó: http://bit.ly/1JWTMKf.
- Ley 26.388 sobre tipificación de delitos informáticos en Argentina. Se trata, según los expertos, de una reforma al Código Penal: http://bit.ly/U6ZyAE.
- Nota en Medium, portal de la ONG Tedic, sobre Pyraweb: http://bit.ly/1IR4Khc.
- La llamada ley Cheheade, en Perú. Para ver el proyecto de ley: http://bit.ly/1QForPX. Para leer sobre el debate en la ONG Derechos Digitales: http://bit.ly/1J5TqRd.
- Proyecto de ley sobre cibercafés en Chile: http://bit.ly/1MOtKq6
- Ley impulsada en Argentina por la senadora Sandra Giménez: http://bit.ly/1kWiWrx

Artículo recibido el 19-11-2015 | Aceptado el 23-05-2016 | Publicado 13-06-2016