**VIGILANCIA DE LA RED: ¿QUÉ SIGNIFICA MONITOREAR Y DETECTAR CONTENIDOS EN INTERNET?[1]**

## Resumen

Este documento analiza el creciente interés de los gobiernos en monitorear la red.[2] En primer lugar, ofrece un marco conceptual general sobre la arquitectura de Internet. Posteriormente, analiza el concepto de control en Internet, haciendo énfasis en los intermediarios y en el uso de tecnologías como la Inspección Profunda de Paquete. Por último, plantea la tensión entre la seguridad nacional y la prevención de la violencia, y derechos como la libertad de expresión y la privacidad.

La conclusión de este documento es que el monitoreo de los contenidos en línea pone en riesgo las garantías fundamentales de los ciudadanos, y amenaza con desmontar el entorno digital abierto y pluralista que conocemos. Y se hacen, entre otras, las siguientes recomendaciones:

- **Necesidad de amplia participación y consulta:** las discusiones de proyectos de ley sobre monitoreo de contenidos en Internet que se lleven a cabo deben contar con una participación amplia, que garantice la inclusión de todos los puntos de vista y un adecuado nivel de conocimiento sobre los temas técnicos.

- **Necesidad de estudios de impacto a derechos humanos:** en relación con la recomendación anterior, sugerimos que los proyectos de ley que buscan establecer mecanismos de monitoreo de contenidos en Internet cuenten con un estudio técnico previo sobre el impacto que tendrían en materia de derechos humanos y en la arquitectura de la red. Los resultados de éste deben explicitarse en la exposición de motivos de la iniciativa.

---

[1] Este documento fue elaborado por Carlos Cortés, investigador de la 'Iniciativa por la Libertad de Expresión en Internet' (iLEI), del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo. La investigación y elaboración del documento fue supervisada y contó con los comentarios de Eduardo Bertoni, director del CELE.
Carlos Cortés es abogado de la Universidad de Los Andes, Colombia. Fue director de la Fundación para la Libertad de Prensa (FLIP); asesor de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, y profesor de 'Derecho de Medios' del Programa de Periodismo y Opinión Pública de la Universidad del Rosario, Colombia. Ha trabajado como periodista en medios de comunicación colombianos como Semana y La Silla Vacía. Actualmente es candidato a magíster en 'Gobernanza de Medios' del London School of Economics, Londres, Reino Unido. carloscortescastillo@gmail.com

[2] En buena medida, decidimos estudiar este tema luego de conocer la existencia de algunos proyecto de ley argentinos que buscan establecer mecanismos de detección o monitoreo de contenidos en Internet. Se trata de los proyecto de ley 728 de 2012 y 1892 de 2012. No obstante, la relevancia del tema –y, por ende, del documento– tiene un indudable alcance regional.

- **Necesidad de transparencia e información de los PSI y OSL:** los Proveedores de Servicios de Internet y los Operadores de Servicios en Línea deben informarles a sus usuarios cómo y en qué condiciones monitorean sus contenidos. Esta obligación incluye el uso de tecnologías como la Inspección Profunda de Paquete.

- **Transparencia e información de los gobiernos:** los gobiernos deben hacer explícitas las políticas de vigilancia y monitoreo de Internet, bien sea en desarrollo de leyes existentes o de decisiones administrativas. Específicamente, deben ser transparentes con las obligaciones que imponen a los intermediarios.

- **Necesidad de delimitar el uso de herramientas de monitoreo:** las autoridades judiciales y de inteligencia pueden contar con herramientas legales para monitorear la actividad en línea de los ciudadanos. Sin embargo, éstas deben estar sujetas a las mismas restricciones que se aplican en otros temas, como la protección de datos y la interceptación de comunicaciones.

- **Necesidad de ampliar el debate con los usuarios:** las organizaciones de la sociedad civil que trabajan en estos temas deben hacer un esfuerzos por acercar a los usuarios a este debate. Esto incluye la formación en herramientas legales y derechos humanos aplicadas a Internet.

## 1. Introducción

La primera persona en usar el término 'ciberespacio' para referirse a Internet fue John Perry Barlow, en 1996: *"Gobiernos del Mundo Industrial, ustedes, gigantes cansados de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, les pido a ustedes, del pasado, que nos dejen en paz. No son bienvenidos entre nosotros. No tienen soberanía donde nos reunimos"*.[3] Su declaración era un rechazo a la intromisión de los Estados en la naciente red, y se convertiría en el manifiesto libertario de los años siguientes. Los 'ciberlibertarios' –como eran conocidos– exigían un Internet autónomo, alejado de las instituciones políticas y legales del mundo real.[4]

Vistas en retrospectiva, las palabras de Barlow fueron proféticas, tanto por la visión que tenía de un entorno digital revolucionario –un auténtico ciberespacio–, como por el temor que albergaba de una intervención estatal. Y es este último punto el que convirtió su manifiesto en una utopía: hoy en día, y de manera creciente, todo tipo de normas regulan actividades en Internet, desde las transacciones comerciales hasta el acceso a material pornográfico. Esto sin mencionar el pulso por la regulación de la infraestructura de la red, o los debates sobre las instituciones internacional que deben hacerse cargo de su gobernanza.

Aunque Internet es un territorio en disputa, los Estados reivindican su soberanía sobre la fracción de cables, tubos y señales que pasa por sus fronteras. Y en ese propósito, una de las obsesiones de los Estados es controlar los contenidos a los que acceden sus ciudadanos. El ejemplo más célebre es el de China, que cuenta con un cortafuegos (o *firewall)* tan impresionante como su legendaria muralla. Entre el Internet que conocemos en Occidente y al que acceden en China, se interpone un sofisticado sistema de filtros y bloqueo de contenidos. Algo similar sucede en Irán, donde varios servidores intermediarios (o *proxys*) monitorean los datos que transmiten los usuarios.[5]

La explicación usual que oímos frente a estas iniciativas es que se trata de una estrategia de censura oficial: esos gobiernos ocultan información que, de conocerse, minaría las bases de su propia legitimidad y autoridad. En esencia, es un atentado contra la democracia. No obstante, el caso de estos países no sirve para explicar todas las intervenciones de los gobiernos en Internet. En muchos otros escenarios, los Estados defienden principios que las constituciones consagran y los ciudadanos exigen.

El ejemplo más reciente lo tenemos en Argentina. Un proyecto de ley presentado en el Congreso[6] propone la creación del Observatorio de Redes Sociales, de Correos Electrónicos y Mensajes de Texto, que busca *"detectar, combatir y denunciar"* expresiones de acoso, discriminación y violencia en Internet. En el

[3] Barlow, J.P. A Declaration of Independence of Cyberspace. Disponible en: https://projects.eff.org/~barlow/Declaration-Final.html. Consultada el 19 de junio de 2012 [traducción informal].

[4] Cfr. Murray, A. Nodes and Gravity in Virtual Space. Legisprudence, 5 (2). 2011, pp. 195-221.

[5] Freedom House. Freedom on the Net 2011. Washington, 2011.

[6] Proyecto de ley 1892 de 2012. Tiene origen en la Cámara de Diputados. Fue publicado en el Trámite Parlamentario No. 22 el 03/04/2012. Se giró a tres comisiones: (a) Derechos humanos y garantías, (b) Comunicaciones e informática y (c) Presupuesto y hacienda.

mismo sentido de este proyecto, pero un paso más adelante, países como Alemania, Francia o Brasil han aplicado normas genéricas o específicas para prevenir la difusión en Internet de contenidos ofensivos o políticamente sensibles.

A primera vista el verbo 'detectar' que contiene el proyecto argentino parece referirse a un proceso de menor importancia. Tal vez se refiera a monitorear los contenidos que ya son públicos en la red, como foros de lectores en medios de comunicación o actualizaciones de estado en redes sociales. Tal vez sería más grave si se hablara de 'bloquear' o 'remover'. Sin embargo, ¿qué implica detectar o monitorear contenidos en Internet?, ¿cuáles son las consecuencias para los ciudadanos?

Este proyecto argentino no contempla ningún mecanismo; se limita a exigir que los prestadores de servicios de Internet y de redes sociales ubiquen en un lugar visible los datos de contacto del Observatorio. No obstante, otro proyecto de ley que conoció el CELE[7] busca obligar a los establecimientos de comercio que ofrezcan conexión a Internet a que instalen obligatoriamente programas de detección y filtrado de contenidos no aptos para menores de edad.

Más allá de cado caso en particular, estas iniciativas dejan entrever un posible desconocimiento de parte de los legisladores de la manera como funciona Internet y del impacto que puede tener una norma, más allá de su intención, en los derechos fundamentales de las personas.

El propósito de este documento es, entonces, analizar ese deseo ascendente de los gobiernos de observar la red, y explorar la tensión entre estas iniciativas y derechos como la libertad de expresión y la privacidad. Igualmente, el propósito es delinear las implicaciones de este objetivo en el ambiente digital.

Es necesario hacer varias precisiones sobre el alcance de este documento. En primer lugar, nos centraremos en el gobierno como actor principal. Muchos actores privados tienen intereses propios en que se monitoree cierto tipo de contenidos en Internet. Por ejemplo, la industria del entretenimiento viene haciendo cabildeo político y legal para que los intermediarios inspeccionen y retiren contenidos que supuestamente violan los derechos de autor. No obstante, ese enfoque no se abordará acá, ya que desbordaría el objetivo que nos proponemos. Lo anterior no implica que omitamos el papel de los proveedores de servicios de Internet, ya que son éstos los que, por su ubicación estratégica, hacen parte de la estrategia oficial de monitorear la red.

En segundo lugar, nos enfocaremos en el problema del monitoreo en Internet. La filtración y el bloqueo de contenidos están estrechamente relacionados con este tema. Sin embargo, la idea de observar la red y detectar contenidos –en los términos que sugiere el proyecto argentino mencionado– sigue la línea de una tendencia que ya se ha visto en otros países. En términos técnicos, el monitoreo o detección se lleva a cabo mediante la Inspección Profunda de Paquete o *Deep Packet Inspection*, una tecnología que permite observar (muchas veces sin que el usuario sepa) todos los contenidos que pasan por la red.

[7] Se trata del proyecto de ley 728 de 2012, 'de Protección y Promoción de los Derechos de las Niñas, Niños y Adolescentes en Internet'. Ingresó a la Dirección de Comisiones el 13/04/2012 y fue enviado a tres comisiones el 16/04/2012. Las comisiones son: (a) De sistemas, medios de comunicación y libertad de expresión; (b) De población y desarrollo humano; (c) De justicia y asuntos penales. A 10 de julio de 2012, no tiene fecha de egreso de ninguna de las tres.

En tercer lugar, este documento hace un uso extenso de analogías para explicar varios aspectos relacionados con Internet. Esta figura debe interpretarse de manera cuidadosa y, en particular en este documento, únicamente como un recurso pedagógico. Es usual que en documentos y debates públicos Internet se asimile en algunos aspectos al teléfono o la televisión. Igualmente, se toman prestados elementos de dispositivos como el DVD o el VHS, o se asemeja el funcionamiento de la red a un correo postal o una autopista. El problema consiste en que muchas veces estas analogías apuntan a negar regulaciones específicas para Internet dado que, justamente al acudir a ellas, ya existen normas aplicables. Y aunque Internet comparte semejanzas con cada uno de los ejemplos citados, ninguno lo explica completamente ni sirve como modelo para su regulación.

Por último, una advertencia que debe tenerse en cuenta durante todo el texto: para analizar cualquier tipo de política pública relacionada con Internet resulta indispensable entender antes cómo funciona ésta. La premisa parece obvia, pero se desconoce constantemente en los debates sobre este tema. Tal omisión es justificable, al menos en parte, debido al alto nivel de sofisticación y tecnicismo que rodea Internet. Construir puentes entre las ciencias sociales (el Derecho, la Ciencia Política, entre otros) y la tecnología (la Ingeniería, los Sistemas) es un objetivo vital en el fortalecimiento de esta discusión.

Para lograr ese propósito, fue necesario simplificar algunas explicaciones técnicas y omitir algunos conceptos. De otra manera, este documento no sería entendible para la mayoría del público para el cual está pensado. Un experto podrá encontrar este enfoque falto de rigor, pero lo hemos hecho de manera cuidadosa, tratando de 'traducir' el debate sin omitir sus elementos clave.

## 2. La arquitectura de la red

La característica más importante de Internet es que es una red descentralizada. En términos generales, no existen puntos de control por donde pasen todos los datos ni requisitos previos para que una persona envíe o reciba información –más allá de tener un computador conectado a la red–. A esto se suma el manejo homogéneo de todos los datos que se transmiten y la posibilidad de hacer varios intercambios a través de una misma conexión.[8] Existen tres términos técnicos que explican esta arquitectura de Internet, y que la diferencia de otros medios o sistemas de comunicación: i) el Principio de extremo a extremo o *End-to-end Principle*; ii) la conmutación de paquetes de datos o *packet switching*, y iii) el Modelo de Interconexión de Sistemas Abiertos u *Open System Interconnection*. A continuación ofrecemos una explicación breve de cada uno.

### a. El Principio de extremo a extremo (PEE)

El PEE es un principio de diseño de redes según el cual las funciones o servicios de la red deben implementarse en los extremos de ésta. En el caso de Internet, hablamos de una 'red tonta' (*dumb network*) con 'inteligencia' en los extremos. Es decir, una red que se limita a transportar los datos hacia su destino, donde se encuentran las aplicaciones y

[8] Hablamos de un manejo homogéneo en términos generales. No obstante, los Proveedores de Servicios suelen aplicar políticas de manejo de tráfico o *Traffic Management* en su redes. Este punto será abordado más adelante.

dispositivos que los interpretan.[9] Esto permite que en la red 'convivan' aplicaciones con funciones distintas de texto, voz, video o datos.

Puesto en práctica, el PEE se asemeja al funcionamiento de una autopista, con sus carreteras y caminos anexos. La autopista permite el tránsito de cualquier vehículo: no establece restricción al servicio que presta –transporte público o privado–, y es en su destino donde se diferencia –dejar a un pasajero, entregar una encomienda, etc.–.

En los primeros años de Internet, la utilidad del PEE era menos perceptible, ya que todos los computadores que usaban la red eran similares y, en general, cumplían las mismas funciones. Hoy en día la relevancia es clara: a Internet no se conectan solo los computadores de escritorio, sino también portátiles, impresoras, dispositivos móviles (tabletas, teléfonos), radios y consolas de juego, entre otros. Igualmente, el menú de aplicaciones y usos crece exponencialmente cada minuto. Cada unos de estos aparatos y aplicaciones usa la conexión de manera diferente, lo cual es posible gracias a este principio.

### b. La conmutación de paquetes de datos (*packet switching*)

Este método de comunicación –que complementa el PEE– divide y agrupa los datos que se transmiten a través de la red sin importar sus características. En otras palabras, para la red es tan 'importante' el texto de un blog como una transacción financiera. Así, en el punto de origen de la transmisión los datos se parcelan en varios paquetes y viajan por la red en cualquier orden, dependiendo de factores como el tamaño (no es lo mismo ver un video en YouTube que enviar un correo electrónico), la velocidad de la conexión y la ruta entre emisario y destinatario. En el destino final, los paquetes se rearman en su estado original (para que una voz en Skype se entienda, por ejemplo) o de la manera adecuada para que sean accesibles (que un texto sea legible).

Para armar ese rompecabezas, cada paquete contiene dos tipos de información: una parte, conocida como el 'encabezado', que permite determinar la ruta del paquete y, dependiendo del tipo, también la manera como se relaciona con los demás paquetes y las aplicaciones o programas que están involucrados (Outlook o Safari, por ejemplo). Y otra, conocida como la 'carga útil', que contiene una porción de los datos objeto de la transmisión (una fracción del texto o el video como tal).[10] Usualmente los textos técnicos hablan de la pareja de protocolos TCP/IP, que constituyen la base de esta operación de conexión y transporte.[11]

Además de los cables, los tubos y los computadores de los usuarios, este intercambio de información se logra mediante el uso de enrutadores o *routers*. El enrutador es un equipo que interpreta datos (como el que tenemos en nuestra casa, usualmente debajo del escritorio) conectado a dos o más líneas de la red cuya función es recibir paquetes de datos y enviarlos a otro enrutador, que repite la función hasta que los datos llegan a su destino. Los enrutadores están en todos los puntos de la red: en los simples, como

[9] Cfr. Van van Schewick. Internet Architecture and Innovation. MIT Press. Posición 1098 y ss [versión para Kindle].

[10] Cfr. Parsons, C. Deep Packet Inspection in Perspective: Tracing its Lineage and Surveillance Potentials. The New Transparency Project, Working Paper 1. The Surveillance Project. Disponible en http://qspace.library.queensu.ca/handle/1974/1939. Consultada el 19 de junio de 2012.

[11] Sin embargo, no son los únicos protocolos.

la casa o la oficina, o en sitios críticos, como las instalaciones de los Prestadores de Servicios de Internet (PSI), agencias de gobierno, o núcleos de conexión que constituyen la espina dorsal de la red. Básicamente, entre un cable y otro siempre hay un enrutador.

Siguiendo con la analogía anterior, la autopista –como la conmutación de paquetes en la red– alberga por igual buses, carros o camionetas. Dependiendo del peso y el tráfico, los autos toman una u otra ruta, y llegan a su destino gracias a la información que proporcionan las señales de tránsito a lo largo del camino –los enrutadores–. [12]

La conmutación de paquetes de datos permite que una red sea más eficiente y se utilice simultáneamente para transmitir todo tipo de información. Este método se diferencia de la conmutación de circuitos, donde la red establece un canal exclusivo entre dos extremos para que intercambien datos.

El ejemplo clásico de este último es la telefonía análoga que tuvimos hasta hace poco: cuando dos personas hablaban por teléfono se establecía un canal de comunicación exclusivo para esa transmisión. Ninguna otra información podía pasar por esa ruta mientras se estaba usando.

### c. El Modelo de Interconexión de Sistemas Abiertos (*Open System Interconnection*)

El método de comunicación de paquetes se complementa con un modelo de interconexión de redes divido en capas, conocido como Modelo de Interconexión de Sistemas Abiertos (MISA). El objetivo principal de MISA es estandarizar las funciones de un sistema de comunicación desde el cable que entra a nuestra casa hasta el ícono que aparece en la pantalla del computador. El uso de las capas permite asignar funciones separadas y encadenadas de una a otra: cada capa sirve a la de más arriba y ésta, a su vez, sirve a la siguiente. Usualmente, la capa superior cumple una función más compleja que la anterior.

*"Estas capas forman una representación completa de la red, desde sus capacidades físicas (señales eléctricas enviadas a través de un cable o alambre telefónico, por ejemplo) en la capa uno, hasta las aplicaciones y servicios (correo electrónico, navegación, por ejemplo), en las capas más altas"*, explica Cooper.[13] Además de desagregar un complejo proceso y de facilitar la compatibilidad, MISA facilita la detección y manejo de errores en el sistema.

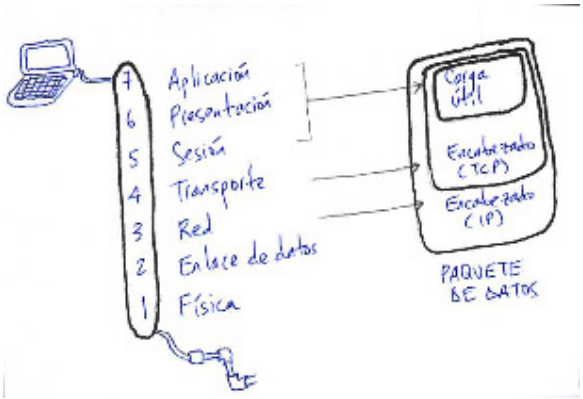


**GRÁFICO**. Capas de Misa y correspondencia con la conmutación de paquetes

Como muestra el gráfico, el encabezado y la carga útil de los paquetes de datos hacen parte de las capas más altas del

[12] Esta analogía también sirve para entender el concepto de manejo de tráfico. Los paquetes de datos viajan por diferentes direcciones, dependiendo de factores como el tamaño y el tipo. Los Prestadores de Servicios de Internet son, a la vez, los agentes de tránsito y quienes mueven el tráfico.

[13] Cooper, A. Doing de DPI Dance. Assessing the Privacy Impacto of Deep Packet Inspection. En: Privacy in America. Scarecrow Press Inc. 2011. P. 149.

modelo. El primero se relaciona con la capa de 'transporte', mientras que la segunda abarca las de 'sesión', 'presentación' y 'aplicación'. En otras palabras, la carga útil –que, recordemos, incluye la 'nuez' de la transmisión– está ubicada en las capas más altas, o profundas, del modelo. Al contrario, el encabezado está más próximo a la capa física, la más 'superficial' de éste.

Examinemos este proceso con un ejemplo. Pablo le envía un correo electrónico a María a través de Gmail: esta acción está enmarcada en la capa de 'aplicación', es decir, la más alta del modelo. El correo incluye el contenido (asunto y cuerpo del texto) y la dirección electrónica de María (maria@gmail.com): estos datos hacen parte de las capas 'aplicación', 'presentación' y 'sesión', que son las que siguen en orden descendente en el modelo y corresponden a la carga útil.

El mensaje también incluye datos sobre el orden de los paquetes y la aplicación o programa en que se ejecutan: éstos hacen parte de la capa de 'transporte' y corresponden al encabezado. Por último, el mensaje sale de una dirección IP del computador de Pablo (215.33.57.120) dirigido a otra (en este caso, cualquier dirección IP del servidor de Gmail): estas coordenadas están en el tercer nivel –'red'– del modelo, que también hace parte del encabezado. Más abajo de éste se encuentra el 'enlace de datos', que es el cable que conecta el computador a la red y, por último, la capa 'física', donde está la conexión a Internet, cualquiera que ésta sea. Cuando María reciba el correo en su cuenta, este proceso hará el recorrido inverso: de la capa 'física' llegará a la de 'aplicación', en la cual ella podrá leer el mensaje.

Para el objetivo de este documento no es necesario entender en detalle el funcionamiento de MISA. Lo importante es entender cómo se transporta la información en la red, y cómo esta última se divide según las acciones jerarquizadas que se llevan a cabo y que se organizan en niveles. Y, concretamente para entender el monitoreo de contenidos, es relevante tener claro que en la medida en que un tercero quiera saber más sobre lo que hace una persona en Internet, mayor será el grado de inmersión en las capas. Para decirlo de manera coloquial: una cosa es leer los sobres de las cartas que le llegan al vecino y otra muy distinta es abrir los sobres y leer las cartas. A esto volveremos más adelante.

## 2. El deseo oficial de controlar Internet

El Principio de Extremo a Extremo y la conmutación de paquetes de datos son el sustento técnico de lo que se conoce en el debate público como 'la neutralidad de la red' (*network neutrality*), término acuñado por el académico norteamericano Tim Wu según el cual todos los contenidos en Internet reciben el mismo trato. La combinación de la 'red tonta' con la transmisión de datos sin jerarquía alguna, explican la innovación creciente y el intercambio de información –pluralista y democrático– que hoy conocemos.[14]

No es necesario contar con una licencia para usar Internet de una manera específica (en la red, cualquiera puede ser bloguero o cantante), ni existe una única tecnología para difundir contenidos. A diferencia de la telefonía o de la televisión por cable, Internet es un sistema abierto y descentralizado. Sin embargo, estas

[14] Cfr. Wu, T. Network Neutrality, Broadband and Discrimination. 2 J. on Telecomm. & High Tech. L. 141, 2003.

características no están talladas en piedra; así como hoy en la red gozamos de innumerables puertas y ventanas, mañana podríamos tener una única entrada celosamente custodiada. Hoy nuestra interacción en la red se asemeja a jugar en un enorme patio; mañana podría parecerse más a jugar en la arenera de un parque.

Lessig considera que el usuario está sujeto a cuatro fuerzas que moldean su comportamiento en Internet: el mercado, que ofrece incentivos hacia el consumo de uno u otro producto; las normas sociales, que influyen en el comportamiento (por ejemplo, el reproche social hacia el uso de groserías en chats y redes sociales); la ley, que establece conductas punibles, y el código –la arquitectura de la red, los programas, los dispositivos–, que en últimas define el entorno digital en el que nos movemos.[15]

*"El código es ley en Internet"*, señala Lessig para subrayar el poder que el entorno digital tiene sobre el usuario. Por más que queramos, no podremos instalar Windows en un iPad o usar Facebook sin tener una cuenta registrada; por más que queramos navegar a una velocidad mayor, dependemos del servicio del proveedor de Internet.

La relación entre el código y la ley puede ser complementaria, principalmente cuando ésta última resulta insuficiente para influir en la conducta de las personas. Mientras que una ley nacional que obligue a un usuario a suministrar su verdadera identidad en Facebook o Twitter tiene altas probabilidades de fracasar, un ley que imponga la obligación a los intermediarios tendrá un impacto inmediato. En el momento en que Facebook o Twitter exijan un número de identidad válido para iniciar sesión (que, por ejemplo, verificará contra una base de datos oficial), nuestro experiencia en la red habrá sido modificada.

Ese es, precisamente, uno de los pulsos más importante que vemos en la red: un esfuerzo por incrementar el control sobre el comportamiento de los usuarios en línea. Según Lessig, se trata de *"cambios en la arquitectura de la Red que permitirán mejorar el control estatal, al facilitar la vigilancia de las conductas —o al menos su rastreo"*.[16]

Julie Cohen ofrece el término 'arquitecturas de control', que responden al anhelo humano –más tradicional y mundano de lo que se cree– de *"usar información y tecnologías de la información para manejar y estructurar el riesgo que se corre"*.[17]

Tal y como los 'ciberlibertarios' temían, los Estados terminaron por reivindicar su soberanía nacional en el ciberespacio. Si bien la gobernanza de Internet en el contexto internacional está inmersa en un debate sin resolver sobre las instituciones que deben hacerse cargo y el origen que deben tener (desde la asignación de dominios de páginas hasta las decisiones sobre infraestructura), cada país ha optado por una estrategia previsible: regular la red dentro sus fronteras. Tendemos a creer que esta tentación solo existe en regímenes dictatoriales, pero la realidad es más tozuda:

> A medida que Internet gana importancia y penetra más y más en los caminos de la vida pública, los gobiernos de Occidente están empezando a sentir –y muchos de

[15] Cfr. Lessig, L. El Código Code 2.0. Edición en Español. Traficante de Sueños 2009.

[16] Ibídem p.231.

[17] Cohen, J. Configuring the Networked Self. Yale University Press, London, p .156, 2012.

> ellos ya lo está sintiendo– una presión creciente para regularla. Parte de esta presión tendrá inevitablemente un origen ilegítimo, perjudicial y anti-democrático; mucha otra, no.[18]

Más allá del impacto que tengan, no todas las intervenciones de los gobiernos en la red son totalitarias. No es un asunto blanco o negro. El ejemplo de China, conocido por tener el cortafuegos o *firewall* más grande del mundo –que busca monitorear todo el contenido que entra y sale del país a través de Internet–, no resume el problema del control en Internet. A medida que se desarrolla la red, las zonas grises aumentan.

Los objetivos de intervención son tan amplios como las prioridades de cada país, más allá del sustento democrático que tengan. Algunos Estados de Medio Oriente, por ejemplo, consideran inaceptable que se difunda pornografía a través de Internet; otros, como Estados Unidos, priorizan la lucha contra el terrorismo, y unos más, como Alemania, quieren prevenir que ciertos discursos políticos –palabras, imágenes– exacerben el doloroso pasado. En un sentido similar, el proyecto de ley argentino (1892 de 2012), que en buena medida anima este documento, pretende *"detectar, combatir y denunciar"* expresiones de acoso, discriminación y violencia en Internet. La pregunta que se desprende es, ¿y cómo se hace?

### a. Los guardianes: la llave del control

Algunos Estados controlan el uso de Internet –de manera directa y permanente– a través de un brazo burocrático, auténticos ejércitos dedicados a monitorear la actividad en línea. Para hacerlo, emplean estrategias como la intervención en los Servidores Raíz de Nombre de Dominio, que relacionan las direcciones IP con los sitios de Internet, o en la espina dorsal de la red, que conecta los puntos críticos del tráfico de datos.

En términos prácticos, esto implica que el gobierno puede 'apagar' Internet como si fuera un interruptor de luz. En diferentes grados, y dependiendo del músculo oficial, éste es el caso de países como Arabia Saudita, China y Cuba.[19] A esto se suma el uso de la Inspección Profunda de Paquete, de la que hablaremos más adelante.

La mayoría de países opta por una estrategia acaso más sencilla y eficiente (aunque no excluyente con la anterior): acudir a los intermediarios –los Prestadores de Servicios de Internet y los Operadores de Servicios en Línea (PSI y OSL, respectivamente)– que hacen las veces de 'guardianes' (*gatekeepers*) de la red. Un guardián es un agente que ocupa una posición privilegiada, controla el acceso a un sitio o el uso de un recurso: del PSI depende nuestro acceso a Internet, y de aplicaciones y servicios como Google, Facebook, o de 'nubes' como Dropbox (todos ejemplos de OSL), depende en gran medida nuestra experiencia en línea. Tal protagonismo es útil para los gobiernos, que encuentran en estos terceros un aliado –voluntario u obligado– para sus propósitos.

El uso de estos intermediarios para aplicar la ley no es una teoría nueva. Cuando existen conductas que las normas no logran desestimular (por ejemplo, una

[18] Mozorov, E. The Net Delusion. Public Affairs Books, New York, pg 218, 2011.

[19] Cfr. Zittrain, J. y Palfrey, J. Internet Filtering: The Politics and Mechanisms of Control. En:
Acces Denied. MIT Press, 2008; y Op. Cit. Freedom House.

sanción penal para frenar la piratería en línea); cuando el Estado se encuentra en una posición desventajosa para hacerlas cumplir, y cuando hay un intermediario en una posición privilegiada para detenerlas, el uso de incentivos –legales, económicos– permite que éste último ayude a cumplir los fines que escapan a la órbita oficial.[20]

En otras palabras, en muchos casos la oferta de los gobiernos hacia estas empresas ha sido: *"o nos ayudan a detectar ciertos contenidos o ustedes también serán responsables"*. Esta estrategia ha ganado terreno en la gobernanza de Internet mediante la creación de 'puertos seguros' (*safe harbors*) para los intermediarios, con las consecuencias negativas para el uso abierto de la red y la afectación de los derechos individuales.[21]

Tanto los gobiernos como los intermediarios (de manera independiente o conjunta) se valen de sofisticados equipos y servicios ofrecidos por empresas británicas o norteamericanas, entra muchas otras, para monitorear la red.[22] En particular, el mercado está inundado de productos para hacer Inspección Profunda de Paquete.

Recientemente, cuando se conoció que el gobierno sirio usaba esta tecnología para perseguir disidentes, e incluso la habría usado para ubicar a la periodista Marie Colvin –que posteriormente murió en un bombardeo junto con un fotógrafo francés–, varias organizaciones de la sociedad civil protestaron.[23] Sin embargo, su uso es más generalizado y, como planteábamos al comienzo del capítulo, hace parte de diferentes estrategias de los gobiernos para ejercer su soberanía en Internet.

### b. La inspección: de superficial a compleja

Desde el punto de vista técnico, la manera de ejercer el control es la parte más complicada. Si tenemos claro el funcionamiento básico de Internet (expuesto antes) podemos vislumbrar lo complejo que es monitorear sus contenidos. No hay un programa o dispositivo que de manera automática detecte y retire de la red aquello que puede ser perjudicial o inconveniente; no existe un procedimiento aséptico y quirúrgico. Al contrario, es necesario desplegar tecnologías que intervienen la red, de las cuales la Inspección Profunda de Paquete o *Deep Packet Inspection* (IPP) es una de las más importantes, especialmente cuando se trata de monitorear contenidos en Internet.[24]

[20] Cfr. Kraakman, R. Gatekeepers: The Anatomy of a Third-Party Enforcement. Journal of Law, Economics and Organization, Vol 2. No 1. 1986.

[21] El 'puerto seguro' ofrece al intermediario la garantía de no ser responsable por las acciones de sus usuarios, siempre y cuando cumpla con ciertas actuaciones. Este tema se aborda parcialmente en el documento del iLEI/CELE 'La tensión entre la propiedad intelectual y el intercambio de contenidos en la red'. Disponible en: http://www.palermo.edu/cele/libertad-de-expresion/ilei-investigaciones_realizadas.html.

[22] Ver, "Selling arms and snooping technology is no way to help democracy, Cameron". Privacy International. Disponible en https://www.privacyinternational.org/opinion-pieces/selling-arms-and-snooping-technology-is-no-way-to-help-democracy-cameron. Consultada el 19 de junio de 2012.

[23] Ver, "Don't get your sources killed in Syria". Galperin, E. Comittee to Protect Journalists. Disponible en https://www.cpj.org/security/2012/05/dont-get-your-sources-in-syria-killed.php. Consultada el 19 de junio de 2012.

[24] Existen muchas otros tipos de intervención, como el filtrado de encabezados o la manipulación del Sistema de Nombres de Dominio.

Retomemos el ejemplo del capítulo anterior en el que Pablo envía un correo electrónico a María. Cada función se ubica en una capa diferente, desde la más alta (el uso de la aplicación para producir y enviar el mensaje) hasta la más baja (los cables que transportan los datos). Así, la cantidad de información disponible sobre los datos de esta transmisión dependerá de qué capas estemos observando. Por ejemplo, si observamos la capa 'red' –en el tercer nivel–, tendremos acceso a la dirección IP del computador tanto de Pedro como de María; si profundizamos un poco más, hasta la capa 'transporte' –en el cuarto nivel–, sabremos que los datos corresponden a Gmail o Google, y si llegamos hasta la 'sesión' y 'presentación' –en los últimos niveles–, sabremos qué dice el correo electrónico.

Para observar o acceder a esos datos es necesario inspeccionar los paquetes. Esto es, revisarlos mientras pasan por un punto de la red, de la misma manera como se abren o inspeccionan con un escáner las maletas en un aeropuerto. Y para hacerlo, se requieren dispositivos y programas especiales que –con diferentes grados de precisión y sofisticación– puedan hacer ese trabajo en una o varias de las capas, a través de la IPP.

El dispositivo, conocido también como 'caja negra', debe estar conectado a la red para poder observar el tráfico. Puede estar en la red de los PSI o de los OSL, en los enrutadores de las entidades públicas o en las espinas dorsales de la red. La capacidad técnica varía según el producto: un tipo de IPP puede copiar algunos de los paquetes para inspeccionarlos posteriormente o simplemente observarlos mientras transitan por la red. Lo cierto es que *"entre más cerca llega una tecnología de inspección a supervisar la capa de aplicación de la carga útil, más podrá saber esta tecnología sobre el paquete (...)"*.[25]

Según Cooper, la IPP *"es la colección, observación, análisis y/o almacenamiento de datos relacionados con una aplicación que se encuentra en Internet por encima de la capa tres"*,[26] es decir, de la capa de 'transporte' en adelante. Parsons, mientras tanto, define la IPP al ubicarla en el nivel más radical de una escala de tipos de inspección:[27]

i) Inspección Superficial de Paquete: incluye los 'cortafuegos' –o *firewalls*– que tienen sistemas operativos como Windows o Apple OS X, y que se ubican entre el cliente y la red a la que éste está conectado. El objetivo de esta inspección es limitar que cierto tipo de contenido, determinado por el usuario, llegue o abandone el equipo. Sin embargo, para hacerlo no puedo leer más allá del encabezado de los paquetes. Esto es, no puede revisar la carga útil.

ii) Inspección Media de Paquete: referida normalmente a los dispositivos ubicados entre el usuario final y la compuerta a Internet o salida al PSI (conocidos como *proxys*). Este tipo de controles son normales en entidades públicas y empresas privadas: todo el tráfico que pasa sobre la red debe cumplir con las reglas impuestas por el administrador, como bloquear el acceso a YouTube o Facebook para los empleados. En términos de inspección –explica Parsons–, este tipo de inspección puede leer la capa de 'presentación', con lo cual accede parcialmente a la carga útil de los paquetes. En otras palabras, es la antesala de la IPP.

[25] Op. Cit. Parsons, p. 3 [traducción informal].
[26] Op. Cit. Cooper, p. 145 [traducción informal].
[27] Cfr. Op. Cit. Parsons, p. 8 y ss.

iii) Inspección Profunda de Paquete (IPP): Parsons coincide con la definición de Cooper en cuanto a que los dispositivos en esta categoría tienen el potencial de mirar todo el tráfico, escoger paquetes y rearmarlos para conocer los datos objeto de la transmisión. Volviendo al ejemplo de Pedro y María, esta tecnología puede reconstruir el correo tal y como fue escrito.[28]

Existen procesos de inspección y manejo de paquetes esenciales para el funcionamiento de la red, lo cual es natural en cualquier sistema de comunicación. Cooper considera que para intermediarios como los PSI el uso de la IPP *"puede ofrecer una mayor comprensión sobre cómo están siendo usadas sus redes, permitiéndoles tomar decisiones más informadas sobre actualizaciones de la red y arquitectura de ésta"*.[29]

Si enviamos una carta por el servicio postal físico, la empresa de correos tendrá que saber cuál es la dirección de remisión y envío y, posiblemente, también el contenido general del sobre o su peso. De la misma manera, en la relación entre el emisario y el receptor en Internet hay, al menos, un tercero que tiene acceso a cierta información de la transmisión.

Adicionalmente, es innegable el incentivo económico que tienen los intermediarios para hacer esto. El uso de la IPP le ha permitido a algunos PSI discriminar el tráfico de sus usuarios con el propósito de manejar su mercado. (Volviendo a la analogía de la autopista, la IPP sirve para crear carriles rápidos, de automóviles último modelo, y lentos, de camiones y carros viejos). Así, utilizan los datos de los encabezados IP para enrutar los paquetes que envían y reciben sus suscriptores, e inspeccionan los encabezados TCP –muchas veces de manera poco transparente– para tener alguna información adicional sobre la actividad de éstos.

Por ejemplo, a un PSI le interesa saber que uno de sus usuarios descarga películas o intercambia archivos de gran tamaño en redes de pares (*peer to peer networks* o P2P). Basado en esto, puede optar por restringir la descarga en ciertos horarios o manejar el tráfico para evitar congestiones en la red. En 2010, el PSI norteamericano Comcast estuvo involucrado en, al menos, un caso de este tipo.[30] Aunque el asunto del monitoreo de contenidos como parte de una estrategia comercial y económica es muy relevante, este documento no lo desarrolla por no estar dentro del enfoque propuesto. No obstante, para muchos observadores, se trata de una estrategia que atenta contra la esencia de la neutralidad de la red.

Más allá del negocio y de los argumentos técnicos, el problema surge cuando la labor de inspección se mueve del rango de los simples encabezados de los paquetes, esenciales para prestar el servicio o garantizar la seguridad del sistema, hacia la carga útil de los mensajes; cuando combinando y sumando información, el tercero comienza a acceder a datos sensibles del usuario o a perfilarlo a partir de sus actividades en la red. Y, más relevante aún, el

[28] Existen tecnologías de encriptación de paquetes para combatir el uso de IPP. Para muchos, éste puede ser el 'antídoto' del monitoreo de contenidos. No obstante, su uso está restringido –tanto por razones técnicas como económicas– a ciertas aplicaciones y sectores.

[29] Op. Cit. Cooper, p. 140 [traducción informal].

[30] Ver, "Appeals Court Throttles FCC's Net Neutrality Authority". Wired. Disponible en: http://www.wired.com/threatlevel/2010/04/net-neutrality-throttle/. Consultada el 19 de junio de 2012.

problema surge cuando los gobiernos promueven o están al tanto del uso de estas tecnologías en detrimento (y a espaldas) de los usuarios.

## 3. El monitoreo en la balanza

Si sostenemos –como lo venimos haciendo– que resulta apresurado concluir que cualquier intención oficial de monitorear la red es sinónimo de represión, tenemos que preguntarnos, entonces, en qué medida esa intervención es legítima y ajustada a principios democráticos. Y, para hacerlo, es necesario repasar los fines que persiguen los gobiernos al ejercer su soberanía en Internet.

En general, esta intervención se sustenta en los bienes comunes de la seguridad nacional y el orden público, y en la necesidad de establecer límites a la libertad de expresión. Todos estos valores están enmarcados en garantías reconocidas tanto en constituciones nacionales como en instrumentos de derecho internacional. A continuación ofreceremos algunos ejemplos para, posteriormente, hacer una análisis crítico.

### a. La necesidad de una red segura

Tener algún tipo de acceso a la información que se intercambia en cualquier sistema de comunicación ha sido una obsesión permanente de las agencias de inteligencia y la fuerza pública en todo el mundo. Para el juez norteamericano Richard Posner, *"en una era de terrorismo global y proliferación de armas de destrucción masiva, el gobierno tiene la imperiosa necesidad de recoger, extraer, depurar y buscar vastas cantidades de información (...)"*.[31]

La necesidad de combatir el terrorismo y el crimen y, en general, de recabar pruebas judiciales, son objetivos de primer orden, aún a costa de la libertad e intimidad de los ciudadanos. Una agenda que, sin duda, ganó terreno a partir del atentado terrorista del 11 de septiembre de 2001 en Estados Unidos. En palabras de Naomi Klein, después de los ataques, *"de repente el miedo al terror era mucho mayor que el miedo a vivir en una sociedad vigilada"*.[32]

Este objetivo no es nuevo. En 1994 el Congreso norteamericano expidió la ley Calea (*Communications Assistance for Law Enforcement*), según la cual las redes de telecomunicaciones deben diseñarse para que las agencias de seguridad puedan llevar a cabo una vigilancia electrónica. La regulación estaba pensada para el teléfono –una tecnología más fácil de monitorear–, pero su aplicación se ha hecho extensiva a Internet y, particularmente, a los PSI.[33]

Hoy en día, conscientes del poder de los guardianes en Internet, el FBI está promoviendo una ley que extienda esta obligación a los OSL. Es decir, para que Facebook o Twitter, por ejemplo, tengan también una 'puerta de atrás' (*backdoor*), por donde pueda entrar el gobierno a mirar cuando sea necesario.[34]

El Reino Unido está inmerso en un debate similar. En 2009, el gobierno laborista propuso que los PSI registraran

---

[31] Posner, R. en Solove, D. Understanding Privacy. Harvard University Press, London. 2008, pg 83 [traducción informal].
[32] Klein, N. Shock Doctrine. Picador, New York. 2007, p. 382 [traducción informal].
[33] Cfr. Op. Cit. Lessig, p. 63 y ss.
[34] Ver, "FBI: We need wiretap-ready Web". CNet. Disponible en: http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/. Consultada el 19 de junio de 2012.

todas las transmisiones de datos de los usuarios de Internet mediante el uso de 'cajas negras' de IPP. Recientemente, la propuesta se retomó con el Programa de Desarrollo de las Capacidades de Comunicación (*Communications Capabilities Development Programme*), que incluye a los OSL.

Si bien el gobierno inglés ya contaba con herramientas para solicitarle a los intermediarios información de sus usuarios que tuvieran almacenada (en virtud del Acto para la Regulación de Poderes de Investigación de 2000), esta propuesta permitiría monitorear y detectar contenidos permanentemente. En el momento en que este documento se publicó, el texto definitivo del proyecto apenas comenzaba a conocerse.[35]

El antecedente inmediato de esta propuesta son los disturbios en Londres del año pasado. Como parte de la respuesta oficial, el primer ministro inglés David Cameron manifestó que su gobierno estaba explorando maneras de prohibir el uso de redes sociales cuando hubiera indicios de que serían usadas para organizar actividades criminales.[36]

En el mismo sentido, en marzo de este año el entonces presidente francés Nicolás Sarkozy propuso, como reacción a los asesinatos en Tolouse por parte de un extremista islámico, que se tramitara una ley para encarcelar a las personas que visitan constantemente sitios en Internet que *"promueven el terror"*.[37]

América Latina no es ajena a esta tendencia. En 2010 en México, el Partido de la Revolución Democrática presentó un proyecto de ley para monitorear y reglamentar el uso de redes sociales. El objetivo principal era prevenir la actividad en línea de los carteles del narcotráfico, que usan las redes sociales para intercambiar información sobre crímenes. Adicionalmente, existe la preocupación de que algunos blogs y sitios de Internet se usan para incitar a la violencia y hacer apologías del crimen organizado. Hasta el momento, no se conocen avances de la iniciativa.[38]

En este enfoque cae también uno de los proyectos de ley argentinos mencionados en la introducción (1892 de 2012), cuyo objetivo es: *"detectar, combatir y denunciar las prácticas denominadas como ciber acoso o ciberbullyng, preservar el ámbito de internet de cualquier tipo de manifestación de violencia que afecte los derechos de grupo, comunidades o personas y cualquier otra práctica de contenido y/o carácter discriminatorio"*. Añade la exposición de motivos que *"defender la libertad de las plataformas digitales es defender que todos sean igual*

[35] Ver, "Draft Communications Bill reveals Home Office's mass surveillance plans going ahead - but government remains tongue-tied about how technology will actually work". Privacy International. Disponible en: https://www.privacyinternational.org/press-releases/draft-communications-bill-reveals-home-offices-mass-surveillance-plans-going-ahead. Consultada el 19 de junio de 2012.

[36] Ver, "United Kingdom: David Cameron Considers Banning Rioters from Social Media. Index on Censorship. Disponible en http://www.indexoncensorship.org/2011/08/united-kingdom-david-cameron-considers-banning-rioters-from-social-media/. Consultada el 19 de junio de 2012.

[37] Ver, "Sarkozy propone encarcelar a quien frecuente sitios web terroristas". Infobae.com. Disponible en: http://america.infobae.com/notas/46914-Sarkozy-propone-encarcelar-a-quien-frecuente-sitios-web-terroristas---. Consultada el 19 de junio de 2012.

[38] Cfr. Ferraz, J. et al. Filtrado de contenido en América Latina: razones e impacto en la libertad de expresión. En: Hacia una Internet libre de censura. Propuestas para América Latina. Facultad de Derecho – Centro de Estudios en Libertad de Expresión y Acceso a la Información. Universidad de Palermo, 2012, p. 182 y ss.

*de libres para expresarse sin ser agredidos o discriminados"*.

Una última aproximación, tal vez menos relevante en nuestra región, se refiere al interés de algunos Estados de hacer cumplir en Internet la religión que profesan. Arabia Saudita, por ejemplo, emplea sistemas de monitoreo y filtrado para evitar el acceso a sitios que menoscaben el culto o que vayan en contra de sus preceptos.[39]

Ésta es apenas una muestra del interés de los Estados de hacer valer principios que, a primera vista, conviven en nivel de importancia con la libertad de expresión. Según Zittrain y Palfrey, para los Estados *"la libertad de expresión nunca ha sido absoluta, incluso en aquellas democracias liberales que valoran estas libertades más encarecidamente"*.[40] Y si así ha sido siempre, ¿por qué habrá de ser diferente en Internet?

### b. Privacidad, vigilancia y libertad de expresión

El monitoreo de contenidos en Internet reduce la órbita de privacidad del individuo, modifica su interacción con la red y condiciona su libertad de expresión. Esta afectación subsiste más allá de la finalidad del monitoreo o, incluso, así no exista una en particular. Tal impacto parte del supuesto de que el individuo sabe o sospecha que su actividad en línea está siendo monitoreada. Si se lleva a cabo sin su conocimiento, la situación sería aún peor, ya que no se le estaría reconociendo siquiera la titularidad de sus derechos más elementales.

El monitoreo en línea constituye una forma de vigilancia, y su penetración en la vida de las personas aumenta en la medida en que las relaciones sociales, laborales y económicas están cada vez más mediadas por el uso de Internet. Hace 20 años poco o nada podía saberse de una persona al observar su actividad en la red; hoy en día puede tenerse una radiografía exacta.

Muchos autores se refieren al impacto que la vigilancia tiene en el individuo. La observación permanente busca controlar y normalizar las conductas de la persona, que opta por actuar de conformidad con la expectativa –explícita o implícita– de quien lo observa. Consciente de que está siendo monitoreada, la persona inhibe su espontaneidad y evita cualquier clase de experimentación.[41] De hecho, volver un espacio predecible y controlable es uno de los objetivos de sistemas como los circuitos cerrados de televisión en lugares públicos (estaciones de metro, parques y calles).

El monitoreo de las actividades en línea es también una violación a la privacidad. Es posible argumentar que una persona no tiene una expectativa de privacidad en un parque, pero no podría decirse lo mismo de su casa, su lugar de trabajo o su computador. *"Una invasión a la privacidad interfiere con la integridad de ciertas actividades e incluso destruye o inhibe algunas de ellas"*, afirma Solove.[42]

La afectación de la privacidad no se limita únicamente al hecho de que un tercero esté al tanto de asuntos de un individuo que este último quisiera que no se supieran; la ausencia de privacidad afecta también el proceso de subjetividad de la persona y la relación de ésta con su

[39] Cfr. Nunziato, D. En: Ibídem, p. 25 y ss.
[40] Ibídem Zittrain, J. y Palfrey, J, p. 31 y 32.

[41] Foucault, M en Reiman, J. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. Santa Clara Computer & High Technology Law Journal. Volume 11, Issue 1. 1995, p.28 [traducción libre].
[42] Op. Cit. Solove, D. p.9.

entorno. Según Cohen, la construcción de la identidad es también un proceso de prueba y error, de juego y ensayo.[43]

Usemos, nuevamente, un ejemplo: Internet es una entrada para la exploración de temas, contenidos e interacciones de todo tipo. Una persona puede estar interesada en la historia de la guerrilla en Latinoamérica, y con ese propósito busca vídeos y textos, intercambia mensajes y transmite opiniones. Esta actividad no se relaciona con su vida personal ni se basa en algún deseo de ingresar a un grupo armado ilegal. Hace parte de una manifestación espontánea (estudiar Historia, entender los movimientos sociales), que puede potenciarse gracias a la reclusión que le ofrece Internet. No obstante, ante un monitoreo de estas actividades, o un indicio de que está sucediendo, esta persona optará por restringir este aspecto de su individualidad.

El costo para la libertad de expresión es evidente. Un individuo que no goza de un espacio para reflexionar, pensar y formar su criterio, no podrá manifestarse de manera libre. *"Los efectos de esta pérdida de confianza podrían ser de amplio alcance. Así como con otras tecnologías de vigilancia, el uso creciente de la IPP crea el potencia para la autocensura e inhibición en línea"*.[44]

### c. Garantías fundamentales e incentivos perversos

El último punto que deseamos plantear se refiere, por un lado, a la manera como los gobiernos implementan las políticas de monitoreo y, por el otro, a los incentivos que generan. Y tal vez acá está el mayor síntoma de preocupación: llama la atención que los gobiernos quieran vigilar Internet, pero llama la atención sobre todo la manera como lo ponen en práctica.

Las declaraciones de Cameron y Sarkozy y los proyectos de ley en Argentina y México referidos tienen un común denominador: ponerlos en práctica implicaría el uso de mecanismos como la IPP. Si el objetivo es detectar palabras, datos e informaciones que se intercambian en la red permanentemente, la única manera de hacerlo es a través de tecnologías intrusas como esa. No existe, al menos hasta ahora, un proceso aséptico para monitorear Internet.

Surgen entonces varias preguntas: ¿cuál sería la fuente de estas medidas, una decisión administrativa, una ley o una decisión judicial?, ¿se hará en desarrollo de controles previos o posteriores?, ¿qué tipo de recursos tendrían los ciudadanos para apelar, o al menos conocer, las decisiones sobre el monitoreo de su actividad en línea?

Hablar de regulación de Internet requiere, como hemos visto, de un conocimiento técnico. Sin embargo, las preguntas planteadas se relacionan con garantías reconocidas por legislaciones nacionales y tratados internacionales, cuya aplicación no debe ser ajena al ámbito de Internet. De la misma manera como los gobiernos reclaman su soberanía en este espacio, es necesario reivindicar la vigencia de estos instrumentos en la era digital.

Aquí no describiremos el marco legal que aplica en este asunto. Baste con señalar que resulta imprescindible analizar las políticas de monitoreo en línea y, específicamente, el uso de tecnologías como la IPP, a la luz de derechos reconocidos en la Convención Interamericana de Derechos Humanos como el de las garantías judiciales

[43] Cfr. Op. Cit. Cohen.
[44] Op. Cit. Cooper, p. 147.

(artículo 8), la honra y la dignidad (artículo 11), y la libertad de pensamiento y expresión (artículo 13).

En relación con este último, la 'Declaración conjunta acerca de Internet', de junio de 2011, los relatores de libertad de expresión de las Naciones Unidas y de la Comisión Interamericana de Derechos Humanos, y la representante de la Organización para la Seguridad y la Cooperación en Europa, manifestaron lo siguiente:

> La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad (la prueba "tripartita").[45]

Por supuesto, sería excesivo argumentar que las autoridades judiciales y de inteligencia no deben tener ninguna clase de herramientas para monitorear la actividad en Internet de una persona. Estas prerrogativas deben existir, pero sus límites deben estar claramente establecidos. En términos prácticos, pueden aplicarse los criterios existentes para la retención de datos o para la interceptación tradicional de comunicaciones.[46] En la misma dirección apunta la prueba 'tripartita' de la que hablan los Relatores. Esto es, debe haber, al menos, proporcionalidad en la actuación, legalidad y control judicial.

Con este contexto en mente, la idea de un observatorio de redes sociales –como un órgano del Ejecutivo o como un cuerpo mixto–, en los términos en que propone el proyecto de ley argentino, puede convertirse en un instancia arbitraria de vigilancia. No sólo los ciudadanos desconocerían los términos en que tal monitoreo se llevaría a cabo, sino que también carecerían de acciones judiciales para cuestionarlo.

"*La mayoría de la regulación que autoriza a las agencia estatales a llevar a cabo filtrado y vigilancia tiende a estar escrita en términos amplios y vagos*",[47] argumentan Zittrain y Palfrey. En este punto coincide Nunziato.[48] Estas ambigüedades legales, que son problemáticas en sí mismas, son aún más riesgosas aplicadas a asuntos de tecnología. En el caso inglés, por ejemplo, las autoridades han dicho en su defensa que el uso de la IPP se limitará a obtener ciertos datos de la comunicación (como saber si una persona le envió un mensaje a otra), sin mirar el contenido. Lo cierto es que obtener esos datos de la comunicación implica técnicamente, en muchos casos, tener acceso a su contenido.

---

[45] Relatoría Especial para la Libertad de Expresión, comunicado de prensa R50/11. Disponible en http://cidh.org/relatoria/showarticle.asp?artID=848&lID=2. Consultada el 19 de junio de 2012.

[46] En la región ya existe regulación especial para la materia. La Ley 1273 de 2009 de Colombia, por ejemplo, incluye el delito de interceptación sin autorización de datos informáticos: *"El que sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses"*.

[47] Op. Cit. Zittrain y Palfrey, p. 33.

[48] Cfr. Nunziato, Dawn C. Preservar la libertad en Internet en las Américas. Op. Cit. Facultad de Derecho – Centro de Estudios en Libertad de Expresión y Acceso a la Información. Universidad de Palermo. p. 11 y ss.

El discurso oficial también termina por convertirse en un incentivo perverso para los intermediarios de Internet, sin mencionar los incentivos económicos ya existentes. El riesgo de terminar respondiendo legalmente por las conductas de sus usuarios, lleva a los PSI y OSL a monitorear cada vez más a sus abonados, incluso desbordando el límite de la relación contractual entre las partes. Todo lo cual sucede mientras el ciudadano navega por Internet de manera desprevenida.

Resulta prioritario entender el impacto que tienen las propuestas y discursos oficiales en la regulación de Internet. Llevada a la práctica, la idea de monitorear y detectar contenidos en línea pone en riesgo las garantías fundamentales de los ciudadanos, y amenaza con desmontar el entorno digital abierto y pluralista que conocemos. Adicionalmente, estas iniciativas deben darse de manera abierta y transparente, bajo la premisa de que los debates tecnológicos –cualquiera que sea su nivel de complejidad– deben estar al alcance de la sociedad y de las instituciones democráticas.

## 4. Recomendaciones

A manera de cierre, y sin excluir otros puntos que hemos señalado en el texto, hacemos las siguientes recomendaciones:

- **Necesidad de amplia participación y consulta:** las discusiones de proyectos de ley sobre monitoreo de contenidos en Internet que se lleven a cabo deben contar con una participación amplia, que garantice la inclusión de todos los puntos de vista y un adecuado nivel de conocimiento sobre los temas técnicos.

- **Necesidad de estudios de impacto a derechos humanos**: en relación con la recomendación anterior, sugerimos que los proyectos de ley que buscan establecer mecanismos de monitoreo de contenidos en Internet cuenten con un estudio técnico previo sobre el impacto que tendrían en materia de derechos humanos y en la arquitectura de la red. Los resultados de éste deben explicitarse en la exposición de motivos de la iniciativa.

- **Necesidad de transparencia e información de los PSI y OSL**: los Proveedores de Servicios de Internet y los Operadores de Servicios en Línea deben informarles a sus usuarios cómo y en qué condiciones monitorean sus contenidos. Esta obligación incluye el uso de tecnologías como la Inspección Profunda de Paquete.

- **Transparencia e información de los gobiernos**: los gobiernos deben hacer explícitas las políticas de vigilancia y monitoreo de Internet, bien sea en desarrollo de leyes existentes o de decisiones administrativas. Específicamente, deben ser transparentes con las obligaciones que imponen a los intermediarios.

- **Necesidad de delimitar el uso de herramientas de monitoreo**: las autoridades judiciales y de inteligencia pueden contar con herramientas legales para monitorear la actividad en línea de los ciudadanos. Sin embargo, éstas deben estar sujetas a las mismas restricciones que se aplican en otros temas, como la pro-

tección de datos y la interceptación de comunicaciones.

- **Necesidad de ampliar el debate con los usuarios**: las organizaciones de la sociedad civil que trabajan en estos temas deben hacer un esfuerzos por acercar a los usuarios a este debate. Esto incluye la formación en herramientas legales y derechos humanos aplicadas a Internet.

* * *

*El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) fue creado en el año 2009 en el ámbito de la Facultad de Derecho de la Universidad de Palermo con el objetivo de realizar investigaciones y estudios rigurosos que se constituyan en herramientas útiles para sectores de la sociedad civil, periodistas, instituciones gubernamentales y comunidad académica dedicados a la defensa y a la promoción de estos derechos, especialmente en América Latina.*

*La creación del CELE responde a la necesidad de construir espacios de debate y estudio dedicados a reflexionar sobre la importancia, los contenidos y los límites de estos derechos en la región. Para esto, el centro se propone dialogar y trabajar en conjunto con otras unidades académicas del país y de Latinoamérica. En este marco, los objetivos específicos del CELE son:*

- *Desarrollar estudios y guías de recomendaciones que tengan impacto en las políticas públicas vinculadas al acceso a la información y la libertad de expresión.*
- *Fomentar junto a distintas unidades académicas la profundización de estudios en cuestiones vinculadas a estos derechos.*
- *Contribuir a generar conciencia sobre la importancia de estos derechos en sociedades democráticas, fundamentalmente en las nuevas generaciones.*