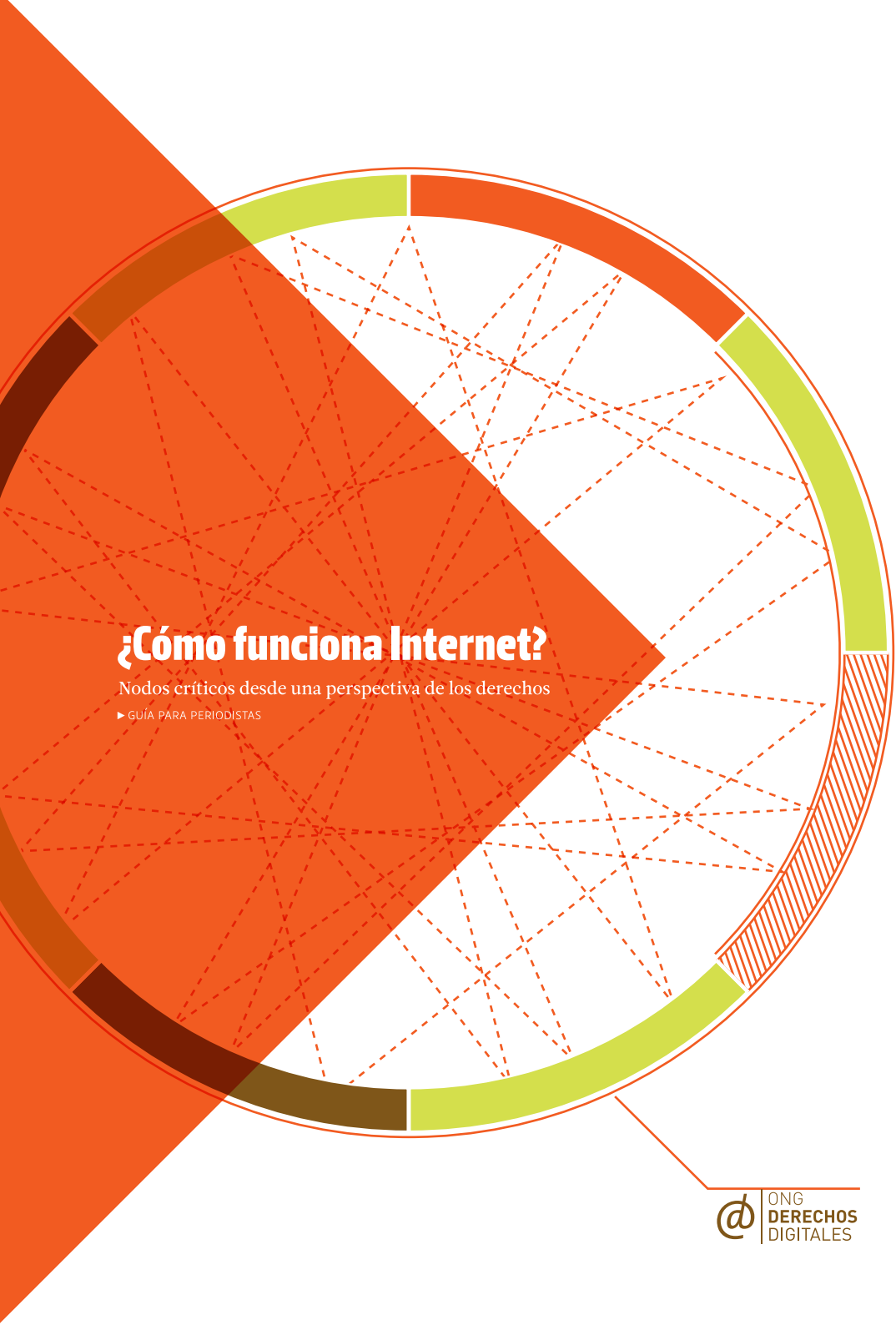


¿Cómo funciona Internet?

Nodos críticos desde una perspectiva de los derechos

▸ GUÍA PARA PERIODISTAS

ONG DERECHOS DIGITALES

¿Cómo funciona Internet?

Nodos críticos desde una perspectiva de los derechos

▶ GUÍA PARA PERIODISTAS

ONG DERECHOS DIGITALES

¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas.
Paz Peña Ochoa.

Una publicación de ONG Derechos Digitales que ha sido posible gracias al valioso apoyo brindado por **Internews**. http://www.internews.org

Diseño e ilustración, Estudio Navaja.
http://www.navaja.org

Impreso por Quick Print.

ONG Derechos Digitales

Diagonal Paraguay 458, Piso 2 Santiago de Chile. C.P. 855003.
Teléfono (56-2) 2 632 36 60
http://www.derechosdigitales.org
prensa@derechosdigitales.org

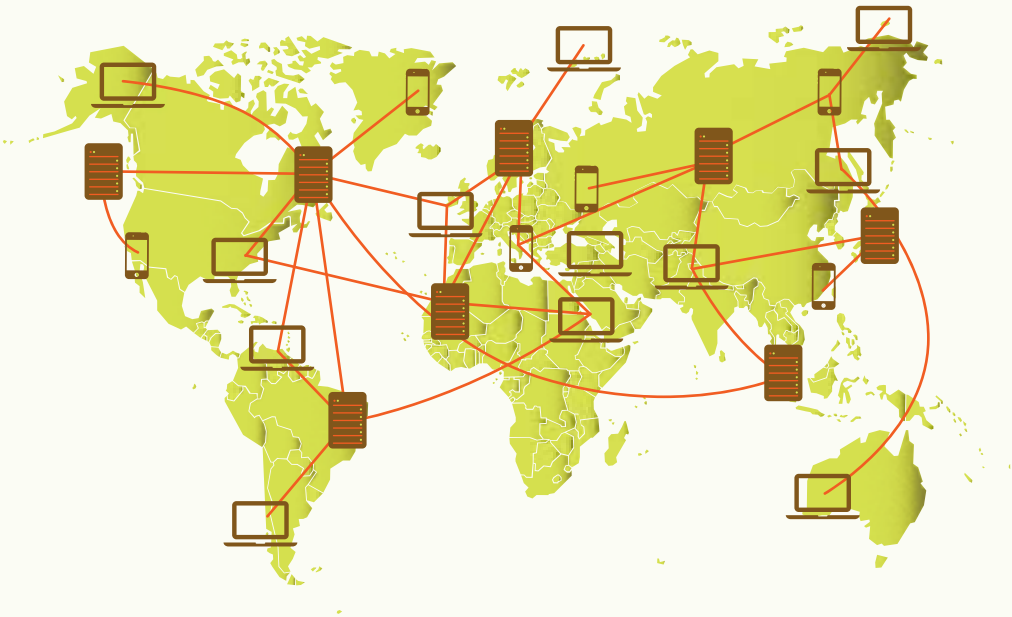
Índice

Introducción

¿Se puede reseñar un informe antipiratería *online* sin comprender de dónde viene y qué intereses defiende? ¿Es posible comprender y describir aplicaciones de redes sociales sin sopesar los costos en privacidad que tiene en sus usuarios? ¿Cuántas demandas a usuarios de Internet terminan siendo una excusa para atacar discursos críticos? ¿Qué implicancias tienen proyectos de ley sobre delitos informáticos en los derechos de los ciudadanos en Internet?

Internet es más que cables, tuberías, aplicaciones, computadores y otros dispositivos tecnológicos. La red es también una serie de relaciones entre organismos e intereses que influyen directamente en el desarrollo y progreso de Internet. Es allí, justamente, donde muchos cuestionamientos emergen y parte importante del interés periodístico se juega.

El interés de esta guía es indagar justamente en esos nodos críticos, conociendo las discusiones, las entidades relacionadas y las instancias donde los conflictos afloran, de tal modo de hacer una guía práctica de cómo funciona Internet que supere las fronteras de lo meramente técnico, y que permita a los periodistas comprender de manera práctica cómo se desenvuelven temas tan polémicos como derechos de autor, privacidad, neutralidad de la red y delitos informáticos.



Red de redes: Internet son redes de computadores y equipos físicamente unidos mediante cables que conectan puntos de todo el mundo.

Parte I: ¿Qué es Internet? Un repaso a la tubería

Internet es un sistema global de redes de dispositivos computacionales conectados. De allí la descripción más famosa de Internet como una **red de redes**.

Quizás por la difundida idea de comparar a Internet como una suerte de nube, alejada y omnipresente desde el cielo, muchas veces se pierde una realidad fundamental para estudiarla: su dimensión física fundamental. Internet son redes de computadores y equipos físicamente unidos mediante cables que conectan puntos de todo el mundo. Así, se compone de un gran número de máquinas con diversas funciones (desde el computador de tu casa que quizás su única función sea la consulta de sitios web, o servidores que alojan un sitio web de noticias al que permanentemente consultas, entre otros), distribuidos por todo el mundo y conectadas por los más diversos medios (cables de fibra óptica, satélites, entre otros).

Esta forma de arquitectura física, poco jerarquizada, nos lleva a dos principios básicos de Internet:

UNO. La red no es una red centralizada. Por el contrario, su diseño está hecho para que no exista un nodo central y pueda resistir ataques sin que la red de redes se caiga. Cualquier intento de control sobre, por ejemplo, los contenidos de Internet es casi imposible, y así lo veremos más adelante en la guía. Con todo, y como también revisaremos en este texto, la concentración de infraestructura crítica de Internet en un puñado de países, deja en cierto estado de vulnerabilidad a muchas conexiones.

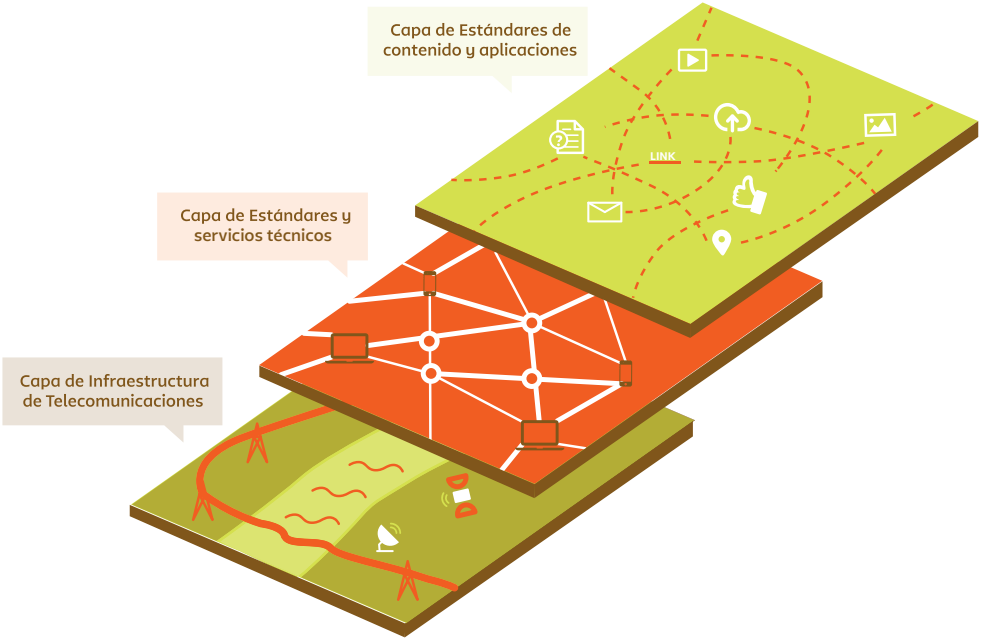
DOS. La red es neutral. Es decir, trata como iguales a todas las máquinas conectadas con respecto a los paquetes de datos que transporta. Si dos archivos pesan igual deben ser tratados igual sin importar el origen. Este principio ha permitido el surgimiento masivo y multipropósito de la red desde su nacimiento.

Pero las dimensiones de Internet no se agotan en lo físico. A nivel social, Internet es un lugar donde las personas se comunican y se reúnen. A nivel cultural, es el espacio para el encuentro de culturas y una plataforma de acceso al conocimiento inédita en la historia. Desde el punto de vista económico, es parte fundamental de la nueva economía mundial; como políticamente es hoy un espacio de dominación estratégica y de información fundamental.

A continuación, nos concentraremos en ver cómo funciona Internet a través de sus componentes técnicos, pero también ligando los actores y las discusiones que aún en esta dimensión se dan.

I. Estructura en capas de Internet

Parte importante de comprender cómo funciona Internet en términos estructurales y de gobernanza, es reconocer el nivel de capas paralelas que implica.[1] **Poder distinguir en qué capa se sitúa un acontecimiento, puede ayudar mucho al momento de abordarlo periodísticamente**.



1. Gobernanza de Internet. Asuntos, actores y brechas. Por Jovan Kurbalija y Eduardo Gelbstein. 2005. Publicado por DiploFoundation y la Sociedad para el Conocimiento Mundial.

a) Capa de Infraestructura de Telecomunicaciones: los caminos y puentes

Es la capa por donde fluye todo el tráfico de la red. En otras palabras, es la capa física por donde se transporta Internet. Se trata, por ejemplo, de instalaciones tales como antenas, satélites, fibra óptica, entre otros elementos fundamentales, y que en su mayoría, son de propiedad privada. Como se puede desprender, cualquier nueva regulación relacionada a telecomunicaciones, tendrá un impacto directo en esta capa.

Si pudiéramos hacer una metáfora simple, la capa de infraestructura son los caminos y puentes para el tráfico básico de personas.

Uno de los temas más relevantes de esta capa es la infraestructura crítica de Internet, pues es en los satélites, fibra óptica y otras inversiones de telecomunicaciones donde se ve la vulnerabilidad o fortalezas de los países en el mapa de conexiones.

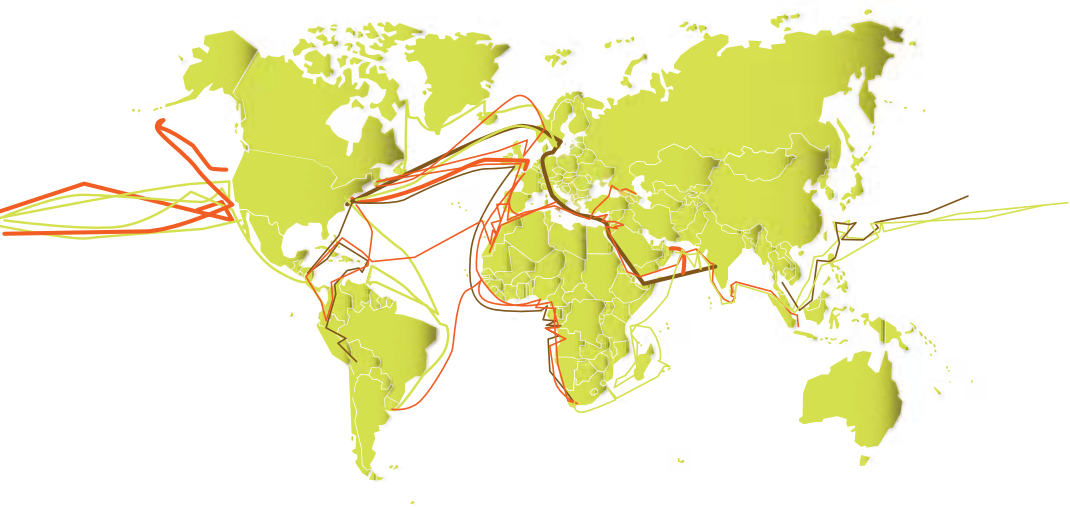
Por infraestructura crítica de Internet nos referimos, en un concepto general, a la red pública de datos donde parte importante de la infraestructura de Internet se juega. Actualmente[2], los mayores nodos de interconexión del mundo se ubican en tan sólo cuatro países: Estados Unidos (Nueva York y Virginia), Alemania (Frankfurt), Holanda (Amsterdam) y Reino Unido (Londres). Es desde estos centros neurálgicos donde el resto del mundo se conecta a Internet.

Si bien se puede afirmar que esa infraestructura está mayormente ligada a las grandes naciones que hacen importantes inversiones en telecomunicaciones para Internet (particularmente, Estados Unidos), este concepto tiene un alto impacto a nivel local. A continuación, veremos dos ejemplos.

• Primero, y desde un punto de vista estratégico, parte de la infraestructura crítica de Internet depende de otros países y no de Chile, lo que levanta un cuestionamiento natural: ¿cómo puede eso afectar a las decisiones soberanas de una nación? En la imagen de a continuación[3], podemos ver los cables submarinos que permiten en gran parte la conexión a Internet de los distintos países. Como se aprecia, la conexión de Chile es tremendamente débil comparado a países como Estados Unidos y otros de Europa. ¿En qué pie nos deja esta falta de infraestructura crítica?

2. ¿Dónde vive Internet? Por Anahí Aradas. 12 de julio del 2012. En http://www.bbc.co.uk
3. Greg's Cable Map, en http://www.cablemap.info/

Interpretación de *Greg's Cable Map*.



• Segundo, desde un punto de vista de continuidad de servicios: ¿cuán preparada está nuestra infraestructura local para resistir un ataque o un desastre natural? Muchas han sido las críticas en este frente, particularmente después del terremoto en Chile del año 2010.[4]

Esta capa está regulada por una serie de organizaciones públicas y privadas. A nivel internacional, las más importantes son dos:

1. UIT: Unión Internacional de Telecomunicaciones.[5]
Es el principal Organismo de las Naciones Unidas (ONU) para la sociedad de la información y temas relativos a la tecnología de las comunicaciones. Así, desarrolla reglas entre los operadores nacionales, la asignación de espectro radioeléctrico y la administración de las posiciones satelitales. También, establece estándares técnicos detallados y ofrece asistencia a los países en desarrollo.

4. ¿Nuestra Infraestructura crítica TIC no está a la altura? (Actualizado). Por Alejandro Barros, 22 de junio 2010, en http://www.alejandrobarros.com

5. ITU http://www.itu.int/es

2. OMC: Organización Mundial del Comercio.
Si bien este organismo aparece después de la UIT en la discusión de la red, con la liberalización del desarrollo de Internet al mercado de los años 90, la OMC comienza a tener un espacio fundamental al ofrecer un marco para las reglas generales del mercado. En particular, existen instrumentos internacionales como el GATT[6] y el GATS[7], que han regulado el tráfico de bienes y servicios en el mundo y que se involucran con Internet. Algunos de estos se han suscrito en el seno de la OMC y otros acuerdos bilaterales o multilaterales como los Tratados de Libre Comercio.

En el ámbito nacional hay un organismo fundamental en esta capa:

1. SUBTEL: Subsecretaría de Telecomunicaciones.[8]
Es un organismo dependiente del Ministerio de Transportes y Telecomunicaciones. Su trabajo está orientado a coordinar, promover, fomentar y desarrollar las telecomunicaciones en Chile. Tiene como principales funciones proponer las políticas nacionales en materias de telecomunicaciones, ejercer la dirección y control de su puesta en práctica, supervisar a las empresas públicas y privadas del sector en el país, controlando el cumplimiento de las leyes, reglamentos y normas pertinentes.

6. Acuerdo General sobre Aranceles Aduaneros y Comercio. Reuniones periódicas de los estados miembros, en las que se realizan negociaciones tendientes a la reducción de aranceles, según el principio de reciprocidad.

7. Acuerdo General sobre el Comercio de Servicios. Se inspiró básicamente en los mismos objetivos que su equivalente en el comercio de mercancías, el GATT.

8. SUBTEL http://www.subtel.gob.cl/

¿Dónde ocurren las noticias en esta capa de Infraestructura de Telecomunicaciones?

La capa de infraestructura siempre tiene un componente noticioso muy importante, porque básicamente son en sus encuentros de autoridades donde parte importante del futuro de Internet se juega.

WCTI:

El gran eje central de las noticias de esta capa es, sin lugar a dudas, las reuniones anuales que hace la UIT en diversos países del mundo llamadas World Conference on International Telecommunications (WCIT). En ellas no solo se discuten a nivel global las regulaciones del ámbito de las telecomunicaciones, sino además asuntos como innovación e inversiones.

Por su importancia, no solo es donde confluyen los representantes gubernamentales, sino también la industria y organismos de la sociedad civil. Por ende, parte importante del *lobby* ocurre en esta instancia.

La reunión del año 2012, en Dubai, fue una de las más polémicas del último tiempo[9], ya que la UIT planteó revisar el Reglamento de las Telecomunicaciones Internacionales (IRT) –vigente desde 1988–, y propuso que los gobiernos de la UIT tomaran mayor protagonismo en la regulación de la red con el fin de asegurar inversión en las infraestructuras y facilitar el acceso de todas las personas a ella. Aquello desató la discusión si esto no era más que un intento de controlar a Internet; y al mismo tiempo, si es válida la idea de creer que Internet es un campo neutro y libre, desconociendo que existen otros poderes que hoy imponen sus términos

9. Más información en "'Malos´ y 'buenos' disputan el poder de Internet". Por Mariano Blejman, en Página 12. 23 de diciembre del 2012.

en ella, sin ir más lejos, países como Estados Unidos. De los 193, solo 89 países firmaron la resolución final. Chile, a través de la SUBTEL, no firmó.

FGI:

La Cumbre Mundial sobre la Sociedad de la Información (CMSI) organizada por la UIT, condujo a la creación desde el 2005 del **Foro para la Gobernanza de Internet (FGI)**, también dependiente de la ONU, en el que participan múltiples partes interesadas como organismos internacionales, gobiernos, empresas, organizaciones de la sociedad civil, entre otras. En este encuentro anual, estos actores de todo el globo discuten el desarrollo de Internet y sus interacciones con otros ámbitos de las políticas públicas, a fin de contribuir a la sostenibilidad, la solidez, la seguridad, la estabilidad y el desarrollo de la Internet.

Parte del interés de esta cumbre, también dada en el WCIT, es que múltiples actores hacen declaraciones sobre puntos polémicos sobre Internet, tales como la "piratería" *online*, la libertad de expresión, etcétera.

b) Capa de los estándares y servicios técnicos: las reglas del tráfico

Es la capa que contiene la infraestructura que hace funcionar Internet, donde toma forma y se transportan sus datos. Si la anterior capa la comparábamos con carreteras y puentes, esta debería ser la capa donde nos ponemos de acuerdo en cómo vamos a circular. Es decir, algo así como las reglas del tráfico: dónde y cuándo vamos a parar, cuáles serán las velocidades máximas y mínimas, cómo van a ser los semáforos y cómo van a funcionar, etcétera.

En esta parte, hay una menor presencia de gobiernos (aunque sigue una enorme influencia de Estados Unidos, debido a la cantidad de infraestructura crítica que tiene[10]) y un aumento de instituciones privadas y profesionales que determinan muchos de los estándares técnicos para el funcionamiento de Internet.

Esta capa tiene dos perspectivas claves de trabajo:

- Estándares técnicos y de servicio (a destacar, protocolo TCP/IP; DNS y servidores raíz).

- Aspectos comerciales de la infraestructura de Internet.

Estándares técnicos y de servicio:

- **TCP/IP [11]: El principal estándar de Internet**

Es el principal estándar de Internet, pues especifica la manera en que se transportan los datos. Sin este protocolo, Internet simplemente sería imposible porque no habría entendimiento entre los componentes de la red.

La principal virtud de TCP[12]/IP[13], es que permite enlazar aparatos de diferentes tipos (un computador o un servidor, por ejemplo), que ejecuten sistemas operativos distintos (quizás Windows o Linux) sobre redes de área local (una oficina) y redes de área extensa (una o varias ciudades) y, por tanto, permite la conexión de equipos distantes geográficamente.

10 Ver en esta guía: "Capa de Infraestructura de Telecomunicaciones: los caminos y puentes".

12 Un protocolo es un conjunto de reglas al que se tiene que atener toda compañía y sus productos de software, de manera de garantizar la compatibilidad de todos ellos.

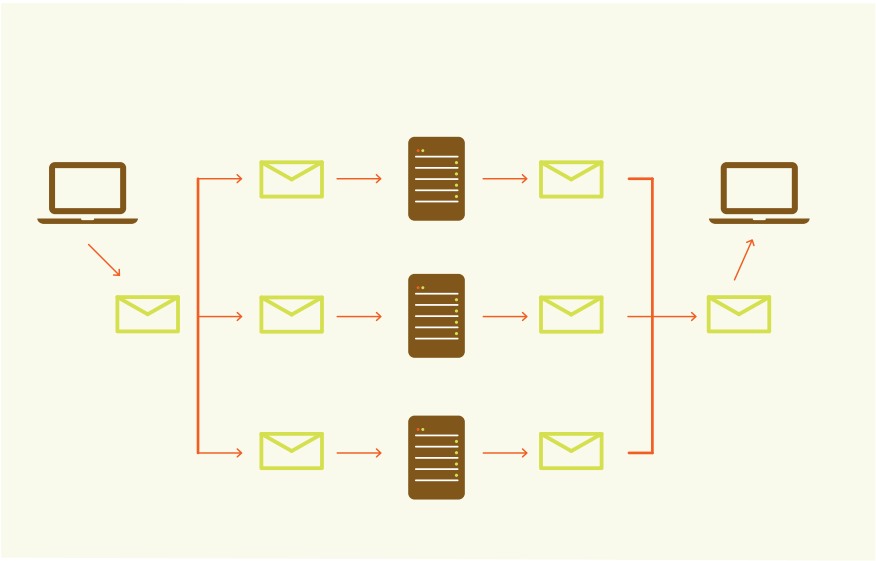
12 Transmission Control Protocol (TCP).

13 Internet Protocol (IP).

Como lo sugiere su nombre, TCP/IP es una aplicación de dos capas: la capa más alta, Transmission Control Protocol, se encarga de mandar los mensajes de la manera más eficiente posible. Así, administra la división de los mensajes o archivos en pequeños paquetes (*bits*) que son transmitidos a través de Internet y finalmente recibidos por otra capa TCP, que unifica los diferentes paquetes en el mensaje original.

La capa más baja, Internet Protocol, administra lo relativo a la dirección de cada paquete que el TCP dicide, para que pueda arribar a su destino correcto. Cada computador que hace de pasarela (*router*) en la red, examina esta dirección para decidir dónde será derivado el mensaje. Como algunos paquetes del mismo mensaje serán ruteados en forma independiente a la de otros, todos ellos deberán ser nuevamente reunidos en su destino correcto.

Protocolo TCP/IP



En este sentido, uno de los principios más importantes con el que funciona el TCP/IP, es que conforma "redes punto a punto", es decir, cada pedido del cliente es tomado como un nuevo pedido que no posee relación con el pedido anterior[14].

Esta parte de esta capa está regulada por:

1. IETF: Fuerza de Tareas de Ingeniería para Internet
Organismo que establece los estándares TCP/IP. Es una institución sin fines de lucro y abierta a la participación de cualquier persona, cuyo objetivo es velar para que la arquitectura de Internet y los protocolos que la conforman funcionen correctamente[16].

- **IP: Una identificación en Internet.**

En palabras simples, el Internet Protocol (IP), es un número que identifica un dispositivo conectado a Internet (desde un computador, un celular, una impresora, etcétera). Los números son únicos, tal como el número telefónico y, por tanto, permite la identificación y la comunicación del dispositivo con otros.

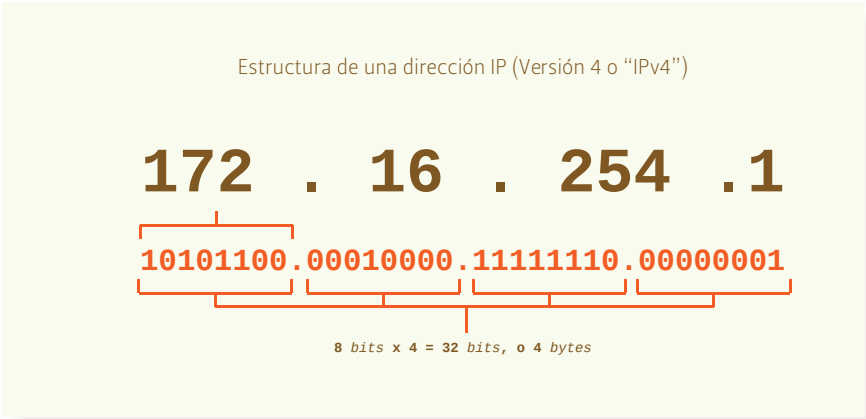
Existe la IP Pública, que es visible desde Internet y suele ser la que tiene tu *router* o *modem*, y suele ser proporcionada por tu ISP (empresa que te da acceso a Internet). Pero también está la IP Privada, que pertenece a una red privada, como la que podría tener una impresora o computador que está conectado a un *router*.

Hoy se asignan los números IP a través del IPv4 (la versión 4 de este protocolo), es decir, cuatro números decimales, que pueden variar cada uno entre 0 y 255, separados por puntos.

Con el crecimiento de Internet, este tipo de asignación está virtualmente agotada, por lo que desde hace algunos años se diseñó la IPv6, que signa 128 *bits* a cada IP en vez de sólo 32 como el IPv4, lo que aumenta de forma exponencial el número de IPs disponibles.

14 A diferencia de, por ejemplo, las conversaciones telefónicas que requieren una conexión dedicada durante la realización de la llamada.

15 Internet Engineering Task Force en http://www.ietf.org/



Esta parte de esta capa está regulada por:

1. IANA: Autoridad de Números Asignados de Internet.
Es un departamento de ICANN[16]. Se encarga de distribuir bloques de números IP entre los RIR (Registros de Internet Regionales).

2. LACNIC: Registro regional de Direcciones IP de América Latina.
RIR regional (hay otros para diferentes regiones, como el Asia Pacífico) que distribuye los números IP a los grandes ISPs y a los registros de Internet a nivel local y nacional.

- **DNS: El IP se hace manejable.**

Los contenidos y servicios de Internet están almacenados en otros computadores de la red llamados servidores.

Para acceder a un sitio web en Internet, la forma para que los usuarios puedan acceder al mismo es a través del número IP que tiene el servidor de *hosting* (almacenamiento de contenidos) de esa web. Por ejemplo, la dirección IP (es decir, el número que identifica el servidor) de google.com es 209.85.195.104.

16 Este organismo se verá con más detención más abajo en el texto, en: "DNS: El IP se hace manejable".

Ahora, ¿cómo hacemos para ver diversos sitios web sin tener que aprender de memoria estos números IP?

Aquí aparece el Sistema de Nombres de Servidor (DNS) que, básicamente, toma las direcciones de Internet (derechosdigitales.org, por ejemplo) y las convierte en números IP, de manera de poder hacer funcionar el tráfico de Internet a través del TCP/IP. También hace la traducción inversa, de números IP a direcciones de Internet.

Entonces, para abrir un sitio web, un computador debe tener acceso a un servidor de DNS, este último localiza la dirección numérica y, si el proceso es exitoso, puedes ver la web que deseas. Los proveedores de servicio de Internet, como Movistar o Entel, cuentan con servidores que proveen este servicio a sus clientes, pero por lo general estos pueden optar por otros servidores que puedan tener ventajas comparativas, como mayor velocidad o seguridad.

El Sistema de Nombres de Domino está compuesto por 13 servidores de raíz en el mundo (10 en Estados Unidos), servidores de dominio superior (".com" o ".net", por ejemplo) y una serie de servidores DNS localizados en todo el mundo (como el ".cl").

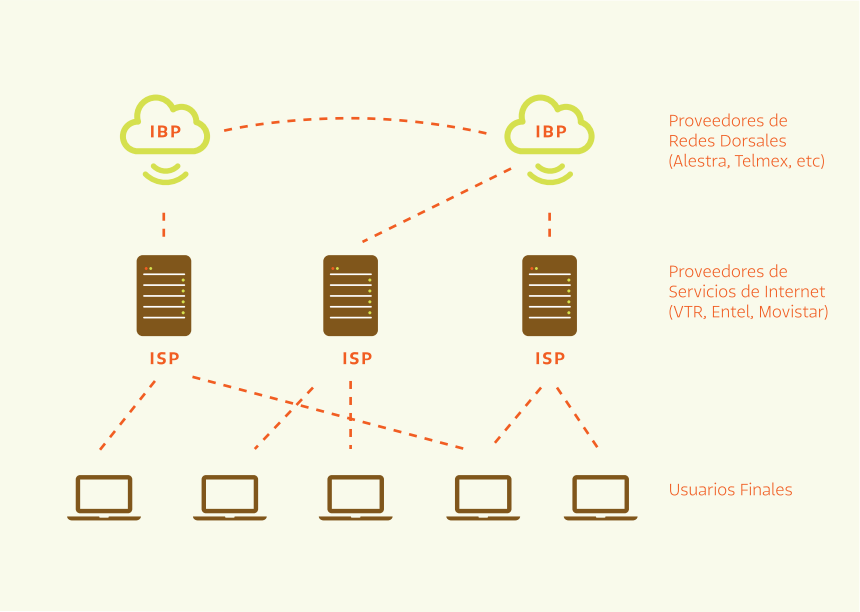
Esta parte de la capa de estándares técnicos y de servicios, está regulada por:

1. ICANN: Corporación de Internet para la Asignación de Nombres y Números
Organización sin fines de lucro que se encarga de la coordinación general del sistema DNS. Actúa como regulador económico y legal del negocio de los nombres de dominio para los gTLDs (dominios genéricos de nivel superior como ".com").

2. NIC Chile: Centro de Información de Redes Chile
Es un cTLD, es decir, un dominio superior por país, en este caso, ".cl". Este tipo de dominios son administradas por IANA; en 1986, este último le delegó al Departamento de Ciencias de la Computación de la Universidad de Chile, la responsabilidad de permitir la creación de nombres de dominio correspondientes a nuestro país, originándose el sufijo ".cl" a través de NIC Chile.

Aspectos comerciales de la infraestructura de Internet.

Para que tengas acceso a Internet desde un dispositivo, no solo se necesitan condiciones técnicas como las que recién vimos, sino también comerciales. En otras palabras, hay intermediarios que hacen inversiones y que buscan una retribución económica por eso.



Así, desde una perspectiva jerárquica, existen dos grandes protagonistas:

1. IBPs: Proveedores de Redes Dorsales

Son operadores de telecomunicaciones que cuentan con una infraestructura propia de red de fibra óptica, que les permite construir grandes redes dorsales de Internet nacionales o internacionales. Como solo son un puñado en el mundo, detentan un poder de mercado excesivo. Es, asimismo, una infraestructura crítica, en el sentido que la operación de Internet podría depender de las decisiones que toman los propietarios de las redes troncales.

2.ISPs: Proveedores de Servicio de Internet

Entre los IBPs y los usuarios finales (usuarios en una casa, un café, una oficina, etcétera) se encuentran los ISPs (Entel, Movistar, Claro, entre otros en Chile), que dependen de la infraestructura de uno o varios IBPs para ofrecer sus servicios. En muchos países, los ISPs son monopólicos por lo que tienen un enorme control de los precios de sus servicios.

En este panorama, es importante aclarar que todos los IBPs cuentan con alguna operación de ISP con la cual ofrecen servicios al usuario final, como por ejemplo AT&T y Worldcom en Estados Unidos.

La necesidad que tiene un usuario de conectarse con cualquier otro usuario dentro de Internet, crea a su vez el requerimiento de que los múltiples jugadores se mantengan interconectados, lo que afecta los costos del servicio y por ende el acceso a Internet[17]. En este contexto, aparece un nuevo protagonista:

3. IXPs: Puntos de Intercambio de Internet.

Es una infraestructura física, de propiedad privada, que brinda facilidades técnicas para que los diferentes ISPs intercambien tráfico en Internet. Esta instalación reduce la porción del tráfico de un ISP, lo que reduce el costo, mejora el enrutamiento y la tolerancia a fallos. A pesar del marcado crecimiento en algunas áreas del mundo, muchos países no cuentan con IXP (Chile sí lo hace)[18]. Como resultado, las redes de la mayoría de estos países no tienen más alternativa que intercambiar el tráfico local a través de costosos enlaces internacionales.

17 Un NAP Mexicano: ¿Indispensable para el cierre de la brecha digital? Por Carlos Silva. En http://www.csilva.net/

18 Normativa Técnica Internet en http://www.subtel.gob.cl

¿Dónde ocurren las noticias en esta capa de estándares y servicios técnicos?

En esta capa ocurre parte importante de los hechos noticiosos que tienen que ver con la afectación de derechos humanos en Internet, como privacidad, acceso a la cultura y libertad de expresión, por lo que tiene un amplio interés periodístico. Algunos ejemplos son:

¿Qué dice la IP de nosotros como usuarios? ¿Podemos preservar nuestra privacidad con este protocolo?

Según un informe elaborado por la Subdirección de Análisis Tecnológico de la Oficina del Comisionado de Privacidad de Canadá, a diferencia del simple conocimiento del número de teléfono de una persona, se podría realizar un retrato muy detallado del usuario con solo la dirección IP. Por otro lado, una sentencia del Tribunal Supremo de España en el año 2013, anuló la condena de dos personas como autores de un delito de estafa informática, por entender que la mera adjudicación de una dirección IP a los acusados no acredita la autoría del delito.[19]

¿Son hoy los ISPs un eslabón fundamental para el respeto de nuestros derechos?

Indudablemente. Los ISPs conectan a los usuarios finales a Internet y a los sitios web anfitriones. Este es el motivo por el cual para muchos gobiernos los ISPs son la opción más directa y simple de imponer control gubernamental y reglas legales en Internet. Así, algunos temas importantísimos siempre están ligados con estos actores, como los monopolios de las telecomunicaciones, su responsabilidad sobre los derechos de reproducción, su rol sobre los contenidos, el respeto por el debido proceso, la privacidad de sus usuarios, etcétera.

19 Ver más en "¿Es el número IP privado?" en Privacidad en la era de las redes sociales.

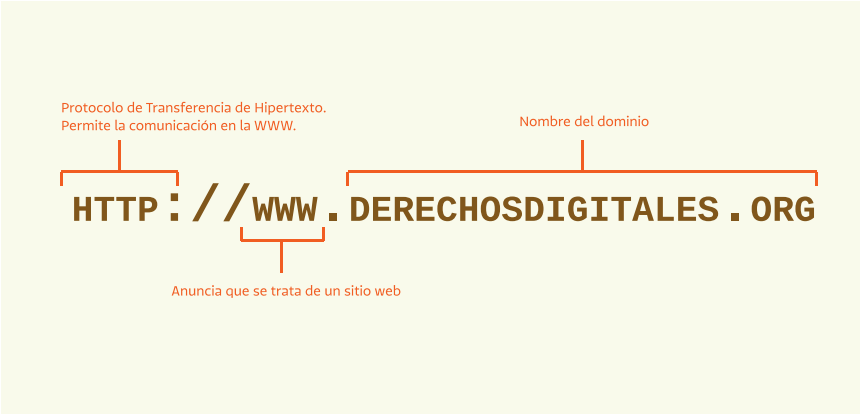
c) Capa de estándares de contenido y aplicaciones: el vehículo que te permite circular

Finalmente, luego de la capa de "Infraestructura" (los caminos y puentes) y de "Estándares y servicios técnicos" (las reglas del tráfico), está la de "Estándares de contenidos y aplicaciones", que es la que usualmente ven los usuarios y que identifican como Internet. Si continuamos con la comparación, esta capa equivaldría a los vehículos que las personas seleccionan para traficar por las carreteras y puentes, respetando las reglas del tráfico, de manera de hacer un sistema de tránsito eficiente.

Estos estándares permiten, por un lado, hacer técnicamente posible que los usuarios comunes intervengan Internet, y por otro, hacen inteligible al lenguaje humano las comunicaciones a través de diversas aplicaciones, como sitios web, correos electrónicos, en fin.

En esta parte es importante recalcar que Internet no es igual a sitios web. Estos últimos son un estándar de comunicación, pero no el único ni tampoco el más usado.

Veamos algunos de los estándares más importantes de esta capa.



1.Sitios web:

▸ **www: World Wide Web.**

Equivocadamente asociado como sinónimo de la red, la popular web o www, es solo un subconjunto de Internet. Basa su navegación en hipertextos, es decir, se pueden seguir enlaces que derivan a otros sitios o documentos, o incluso devolver información al servidor para interactuar con él. El acceso a la www se hace a través de los navegadores, como Chrome, Firefox, Safari, Internet Explorer, entre otros.

▸ **HTTP: Protocolo de Transferencia de Hipertexto.**

Es un protocolo de red para publicar sitios de web, usado en cada transacción de la World Wide Web. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web y sigue el esquema petición-respuesta entre un cliente y un servidor[20].

▸ *Cookies.*

El HTTP es un protocolo que no almacena el estado de la sesión entre peticiones sucesivas. Por eso, es necesario permitir al servidor Web recordar algunos datos concernientes al usuario, como sus preferencias para la visualización de las páginas de ese servidor, nombre y contraseña, productos que más le interesan, etcétera. Para ello, los navegadores de información almacenan esta información en archivos conocidos como *cookies*[21].

▸ **HTTPS: Protocolo de Transferencia de Hipertexto Seguro.**

Es una combinación del protocolo HTTP y protocolos criptográficos.[22] Se emplea para lograr conexiones más seguras en la www, generalmente para transacciones de pagos o cada vez que se intercambie información sensible (por ejemplo, una clave o *password*) en Internet.

▸ **HTML: Lenguaje de Marcas de Hipertexto.**

Es un código para la creación de documentos de hipertexto (documento que

20 Según Wikipedia, la arquitectura cliente-servidor es un modelo de aplicación distribuida en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes. Un cliente realiza peticiones a otro programa, el servidor, quien le da respuesta.

21 Las *cookies* son un componente polémico para la privacidad de los usuarios. Lo puedes ver en esta guía en el cuadro "¿Dónde ocurren las noticias en esta capa de estándares de contenidos y aplicaciones?" y "Privacidad en la era de las redes sociales".

22 Sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

puede contener enlaces a otros documentos) con los que se definen los sitios web. En palabras simples, se trata de un conjunto de etiquetas que sirven para definir el texto y otros elementos que compondrán una web. Aunque ahora suena simple, la implementación de esta idea en los 90 significó una revolución en la manera de acceder a contenidos y allanó el camino para el crecimiento exponencial de Internet.

▸ **XML: Lenguaje de Marcas Generalizado**
Se trata de un lenguaje más reciente que el HTML, y es utilizado para estructurar la información en cualquier documento que contenga texto (por ejemplo, una base de datos). Es un estándar abierto y libre.

2. Correos electrónicos:

A continuación, un conjunto de protocolos diferente al www, y que sirven para la gestión de correos electrónicos exclusivamente. Estos protocolos son casi invisibles para los usuarios, pues los clientes de correo que usan la www son programas que permiten usarlos de manera simplificada.

▸ **SMTP: Protocolo para la Transferencia Simple de Correo Electrónico.**
Protocolo TCP/IP usado en el envío y recepción de correo electrónico en Internet. Sin embargo, debido a sus limitaciones, se usa con uno o dos protocolos adicionales para recibir correos electrónicos, como POP3 o IMAP.

▸ **POP: Protocolo de Transferencia de Correo Simple.**
Uno de los protocolos utilizados por clientes de *email* para recoger mensajes en el servidor de *email*. Los mensajes son transferidos desde el servidor hacia el computador, cuando el usuario se conecta al servidor. Este protocolo es más antiguo y no permite sincronizar mensajes ni carpetas entre un dispositivo y el servidor de correos electrónicos, por lo que ha perdido muchísimo terreno frente al protocolo IMAP.

▸ **IMAP: Protocolo de Acceso a Mensajes de Internet.**
Como POP, este protocolo es utilizado por clientes de *email* para tener acceso a los mensajes que llegan al servidor de correos electrónicos. A diferencia del POP, utilizando IMAP la conexión entre el computador y el servidor de *email* debe estar siempre activa pues hay una constante interacción entre ambos. A

diferencia de POP, este protocolo tiene la ventaja de poder sincronizar correos con el servidor, incluyendo su estado de lectura, marca de seguimiento, y otras implementaciones.

3. Transferencia de archivos:

Antes de la masificación de la www, la transferencia de archivos en Internet se hacía por estos protocolos, con direcciones FTP que fueron los primeros "discos duros virtuales". A pesar del tiempo y de la evolución de las tecnologías, estos protocolos no solo siguen existiendo, sino que aún gozan de buena salud. Como veremos más adelante, estos protocolos siguen estando en la polémica, sobre todo cuando hablamos del conflicto entre derechos de autor e Internet.

- **FTP: Protocolo de Transferencia de Archivos.**

Es un software cliente/servidor que permite a usuarios transferir archivos entre computadores en una red TCP/IP, simplemente a través de un programa cliente FTP, con el que dos computadores se conectan y a través de una contraseña, se pueden intercambiar archivos de todo tipo.

- **P2P: Redes Entre Pares (Ares, BitTorrent, eMule y otros).**

Como se concluye por el nombre, se trata de una "comunicación entre iguales". En una red P2P, los computadores se conectan y comunican entre sí sin usar un servidor central, aprovechando, optimizando y administrando la capacidad de la red (ancho de banda) de modo que usa la mejor ruta entre todos los nodos o computadoras que la conforman, ya que los archivos no salen de un único servidor hacia los clientes sino que los clientes de descarga pueden ir compartiendo los archivos al mismo tiempo.

En esta etapa, existen múltiples protagonistas, sobre todo a nivel de empresas privadas, pero a nivel de gobernanza (regulación) de Internet, hay uno que destaca:

- **W3C: Consorcio de la World Wide Web.**

Consorcio internacional que se ocupa de la estandarización de aplicaciones y de dar recomendaciones para la World Wide Web.

¿Dónde ocurren las noticias en esta capa de estándares de contenidos y aplicaciones?

Esta es una de las capas más polémicas en cuanto a hechos noticiosos, pues como es la cara directa a los usuarios, es donde se ven más afectados sus derechos. Algunos ejemplos son:

¿Son las *cookies* peligrosas para la privacidad de los usuarios?

Si bien las *cookies* permiten, en ciertos aspectos, hacer más eficiente nuestra navegación por Internet, la verdad es que con ellas se almacenan los comportamientos de los usuarios al momento de su navegación por la red, no solo en un sitio web, sino que en muchos de ellos. Toda esa información sirve para que las compañías publicitarias hagan detallados perfiles de sus potenciales clientes, lo que no solo afecta la privacidad de las personas, sino también su derecho a anonimato. Por esa razón, algunos países tienen legislación sobre *cookies*. Pero quizás el gran problema es que la función de ellas sigue siendo desconocida para los usuarios.[23]

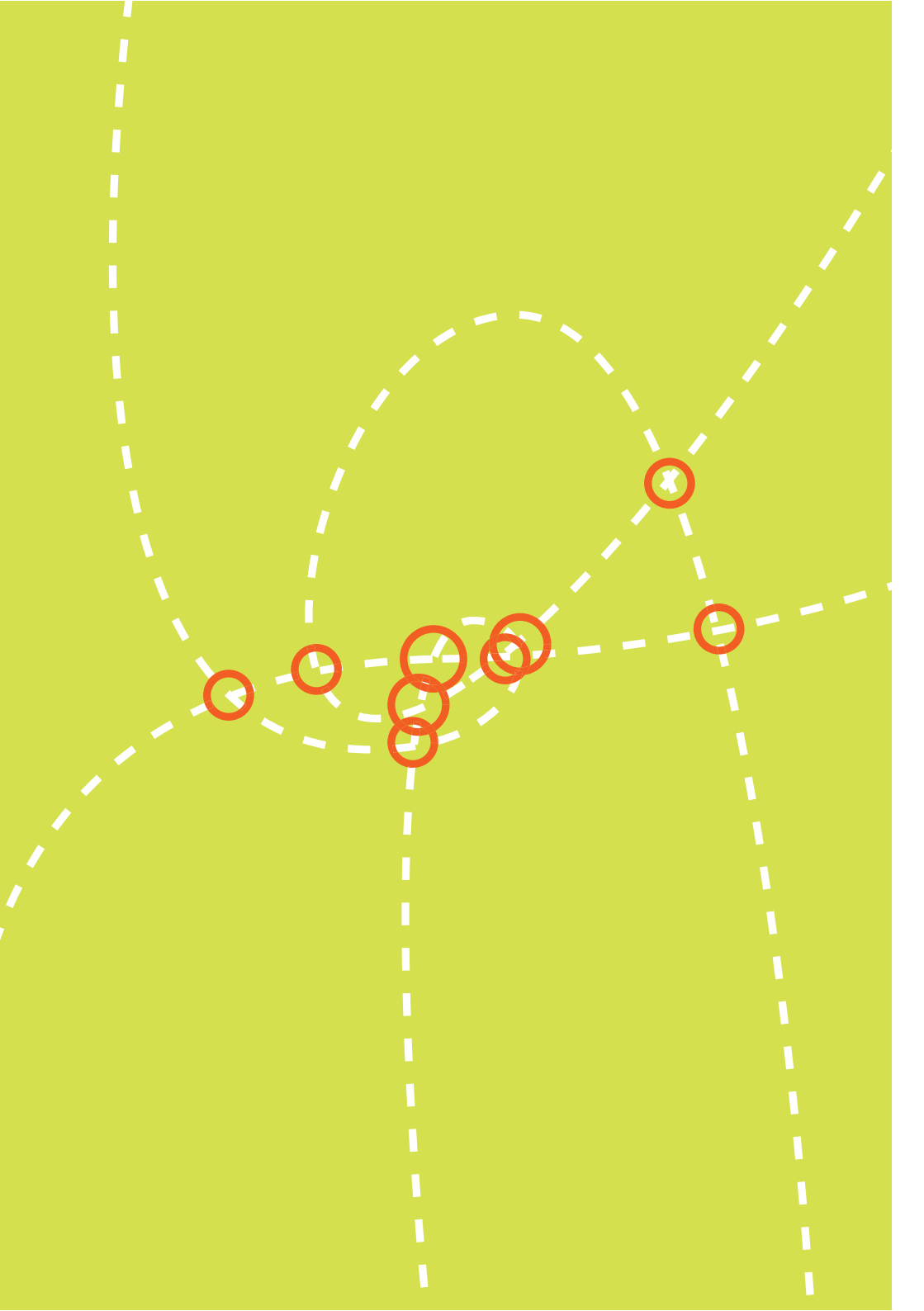
El P2P como protagonista de las batalla contra la "piratería" *online*.

Parte importante de la pelea de la industria del entretenimiento de Hollywood y de algunos gobiernos, ha sido contra programas que permiten el intercambio de archivos con el estándar P2P. La primera gran batalla fue a Napster (nacida en 1999), debido a la demanda de varias discográficas por el intercambio de archivos de música que no pagaban derechos de autor. El 2001, un juez ordenó su cierre y desde entonces Napster se convirtió en un servicio de pago. Esa no fue la única demanda: le siguieron servicios como Audiogalaxy o, más recientemente, The Pirate Bay. Parte importante de la discusión con este tipo de servicios

23 Más información en: "Capa de estándares de contenido y aplicaciones: el vehículo que te permite circular" y "Privacidad en la era de las redes sociales".

P2P es sobre los derechos de las personas a compartir los discos que compran, los modelos de negocios poco eficientes de la industria del entretenimiento, la cultura del acceso al conocimiento como sello de Internet, etcétera.[25]

25 Más información en "La batalla de la "piratería" *online*".



Parte II: Nodos críticos en Internet

Internet no es solo una red técnica, y por ende, su funcionamiento no depende solo de estos aspectos. Como hemos adelantado anteriormente, Internet también se trata de relaciones sociales, políticas y económicas que pueden afectar los derechos de los ciudadanos.

A continuación, identificamos algunos de los nodos más críticos en el desarrollo de Internet, los que no solo afectan los derechos y concilian la atención de legisladores y Estados, sino también son permanentes fuentes de hechos noticiosos.

I. Neutralidad de la red

a) ¿Qué se discute?:

La neutralidad de la red es el principio que garantiza el derecho de los usuarios a acceder a cualquier contenido, aplicación o servicio en Internet, sin la intervención de los proveedores o la censura de empresas, gobiernos y administraciones. Bajo este principio, las compañías de telecomunicaciones no podrían filtrar, bloquear, reconducir o favorecer el acceso a unos servicios por encima de otros. Su importancia es fundamental, pues sin ella, se dificultaría la aparición de nuevos servicios y negocios en la red, ya que lucharían en desventaja contra los grandes y establecidos, que podrían pagar a las operadoras para que los suyos fuesen más rápidos.

b) Matices de la discusión:

▸ **¿Es posible la neutralidad de la red en términos absolutos?**
Una posición crítica es que la neutralidad de la red es imposible. Internet no es libre ni lo ha sido nunca: está en manos del ICANN y, orgánicamente, del gobierno norteamericano, quienes velan no solo por sus propios intereses económicos, sino también político-estratégicos[25].

▸ **¿Puede el precio garantizar la neutralidad de la red?**
En un comienzo de esta discusión, una posición contraria a la neutralidad de la red estaba por parte de los ISPs. Un intento, aunque sólo fueron declaraciones, sucedió en el año 2006, cuando Cisco y Motorola propusieron construir tarifas de diferente categoría: platino, oro, plata y bronce; según las necesidades de cada cliente. Las compañías argumentaban que se trataba de adaptar mejor el acceso según el tipo de usuario[26]. Felizmente, esa posición no prosperó pero no está del todo desterrada en la discusión.

▸ **La existencia de dos redes: la libre y la de pago.**
Esta polémica nace con la propuesta conjunta del año 2010 entre Google y Verizon, donde apoyan la neutralidad de la red pero de forma "condicionada". Si bien ambas compañías sostienen que los usuarios de Internet deberían tener

25 Neutralidad de la Red: la nueva guerra fría. De Marta Peirano, El Diario, Zona Crítica. 4 de enero del 2013. En http://www.eldiario.es

26 ¿Qué es la neutralidad en la red? 5 de agosto del 2010. El País, Tecnología. En http://tecnologia.elpais.com/

un acceso en condiciones de igualdad a todo tipo de contenido en línea, plantean dos excepciones: excluir de su llamamiento los "servicios *online* adicionales", como los contenidos en 3D; y el negocio de Internet móvil. Las críticas no tardaron en llegar,[27] calificando la propuesta como una "falsa neutralidad de la red" que, en la práctica, convertirá a Internet en dos redes, una libre y abierta como hasta ahora, y otra "de pago" para otros servicios como la TV, los juegos *online* o los contenidos en 3D.

▸ **Saturación de infraestructura.**
Si bien la mayoría de servidores son máquinas profesionales instaladas en grandes centros de datos, como lo vimos en la primera parte de esta guía, cualquier usuario puede configurar su propio servidor en casa y así, por ejemplo, no tener que pagar el *hosting* de su sitio web. Esto, que es un principio básico en Internet, se podría ver amenazado con las condiciones que el ISP de Google, "Google Fiber", querría imponer: un usuario particular no puede conectar un servidor propio a su red de fibra óptica[28]. Las protestas de esta medida apuntan a que esta prohibición va en contra de la neutralidad de la red; Google desestima aquello y dice que es una clausula estándar para evitar la saturación de sus infraestructuras.

▸ **¿Puede haber una fiscalización eficiente de la neutralidad de la red?**
En Chile, primer país en el mundo con una legislación de neutralidad de la red, el problema de la fiscalización se ha comenzado a presentar. Así, ONG Cívico realizó una extensa investigación[29] a través de la información pública emitida por SUBTEL y, además, por documentos obtenidos por ley de transparencia, y determinó que a pesar de que el organismo estatal tenía antecedentes de prácticas discriminatorias y sus efectos para los usuarios, no cursó cargos ni tampoco mayores actuaciones frente a las empresas para ordenar la suspensión de estas prácticas. En suma, ONG Cívico cree que la entidad encargada carece de conocimientos técnicos para apuntar malas prácticas de los ISPs; por su parte, SUBTEL declara sí haber fiscalizado, con el resultado (desde 2011 a julio de 2013) de 20 cargos a empresas de Internet por incumplimiento a la ley de neutralidad.

27 Lluvia de críticas a Google y Verizon por su postura 'contra la neutralidad de la Red'. Pablo Romero en Agencias. 10 de agosto del 2010. En http://www.elmundo.es

28 Google y la neutralidad de la red: ¿dónde quedó el don't be evil? Por Guillermo del Palacio. 31 de julio del 2013. En http://alt1040.com

29 ONG Cívico denuncia abandono de deberes de SUBTEL en fiscalización de calidad en acceso a Internet. Por José Huerta en ONG Cívico. 11 de junio del 2013. En http://ongcivico.org

c) ¿Quiénes son los protagonistas de este nodo?

▸ ISPs

Como intermediarios entre la conexión a Internet y los usuarios (y por ende, con los cuales estos últimos hacen tratos comerciales para obtener conexión y ancho de banda), los ISPs son uno de los protagonistas fundamentales de la neutralidad de la red. Ellos son, efectivamente, los que tienen la responsabilidad de no interferir en el tráfico ni en los contenidos. El problema es que la tentación de intervenir es amplia. Como ONG Cívico ha venido denunciando en la implementación de la ley de neutralidad de la red en Chile, por ejemplo, muchos ISPs degradan las velocidades de populares servicios de *streaming*. Esta práctica es anti competitiva, porque estos servicios no podrán competir contra, incluso, servicios de propiedad de los ISPs que se encuentran verticalmente integrados (y que proveen, por ejemplo, TV por cable u otros servicios de video *streaming* en línea).

▸ Usuarios de Internet

Como consumidor, es el usuario el que debe monitorear los servicios de Internet que contrató al ISP y, en el caso de Chile, hacer las denuncias de incumplimiento de la ley de neutralidad de la red en la SUBTEL. Los usuarios son los principales afectados cuando no se respeta la neutralidad de la red y, por ende, uno de los principales fiscalizadores de su cumplimiento.

▸ SUBTEL

Organismo del Estado que en Chile tiene el rol de sancionar las infracciones a las obligaciones legales o reglamentarias asociadas a la implementación, operación y funcionamiento de la neutralidad de red.

▸ Estados

Los Estados están llamados a garantizar la neutralidad de la red, como un principio básico para el acceso igualitario al tráfico y los contenidos de parte de sus ciudadanos. Hoy, en el mundo, hay una presión ciudadana para que ellos establezcan este principio a través de la ley, y la gran discusión se concentra en que este principio salga invicto de otros poderosos *lobbys* con intereses comerciales y políticos.

d) ¿Cuáles han sido las iniciativas legales más importantes?

▸ **Ley de neutralidad de la red en Chile:**
La ley número 20.453, consagra el principio de neutralidad en la red para los consumidores y usuarios de Internet y convierte a Chile en el pionero mundial en el reconocimiento de este principio. En su único artículo, propone modificaciones de varios artículos de la vigente ley general de telecomunicaciones, en las que se obliga a los proveedores de red a "no bloquear, interferir, discriminar, entorpecer ni restringir arbitrariamente el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal". Los operadores podrán gestionar su tráfico y sus redes siempre que no afecten a la libre competencia, y además están "obligados a preservar la privacidad de los usuarios, la protección contra virus y la seguridad". Sólo podrán bloquear contenidos bajo expresa petición de un usuario y a sus expensas, en ningún caso de forma "arbitraria". Además, da la libertad al usuario de utilizar cualquier instrumento, dispositivo o aparato en la red, siempre que sean legales.

▸ **Ley de neutralidad de la red en Holanda:**
Este país adoptó una nueva legislación que protege el carácter neutro de la web con varias disposiciones de protección de los usuarios frente a posibles desconexiones y control del contenido del tráfico por parte de los proveedores de servicio. Permite, además, la gestión del tráfico en caso de congestión de la red o por motivos de seguridad, siempre y cuando se realice en interés del usuario. La normativa también incluye disposiciones que limitan las escuchas telefónicas y las restricciones debido al uso, por ejemplo, de voz sobre IP (VoIP) por parte de los proveedores de Internet. Por último, sólo se podrá desconectar a un cliente en caso de fraude o cuando no pague su factura de Internet.

▸ **La neutralidad de la red en la U.E.:**
Junto con una serie de otras medidas, el año 2013, la vicepresidenta de la Comisión Europea (CE) y responsable de Agenda Digital, Neelie Kroes, anunció avanzar en garantizar la neutralidad de Internet en Europa. Así, declaró que los ciudadanos de la U.E. deben poder disfrutar de la neutralidad de la red: "Pondré fin al bloqueo o estrangulamiento anticompetitivo para cada ciudadano, cada red o cada dispositivo". No obstante, la polémica estalló al filtrarse un borrador de un nuevo marco regulatorio de la U.E. que permitiría a los operadores establecer distintas calidades de servicio y llegar a acuerdos de transporte con los proveedores de contenidos.

e) Dos principios para la cobertura de la neutralidad de la red

Ya sea porque es uno de los aspectos más sensibles para el usuario de Internet o porque en el mundo es un principio que todavía se discute en distintos niveles políticos, la neutralidad de la red es un nodo de permanente interés periodístico.

A continuación, te presentamos dos principios que pueden ser de ayuda al momento de una cobertura periodística más completa de estos temas.

▸ **La neutralidad de la red es un principio fundamental de Internet**.
No respetar el principio de la neutralidad de la red es, simplemente, poner en peligro el Internet como lo conocemos (y que vimos en la primera parte de esta guía). Cada ataque a ella, ya sea de empresas o de Estados, es una intervención que debe ser denunciada con la mayor seriedad.

▸ **Los intereses estratégicos atentan contra la neutralidad de la red**
No solo los intereses comerciales atentan contra la neutralidad de la red, sino también los estratégicos de cada Estado, al tratar de controlar la red. En la actualidad, parte fundamental de la infraestructura crítica de la red está manejada por Estados Unidos, por lo que lo que haga ese país, sus aliados y no aliados con Internet, es hoy fundamental para la supervivencia de este principio. Los ojos periodísticos entonces no solo deben estar en los intereses de empresas.

II. Ciberdelitos

a) ¿Qué se discute?:

En una definición general, un ciberdelito o delito informático es cualquier actividad delictiva en la que se utilizan como herramienta los computadores o redes, o estos son el objetivo de la misma[30]. Estos delitos pueden referirse, mayormente, al fraude informático, la suplantación de identidad, la pornografía infantil, el *grooming*, etcétera. En esta guía, nos detendremos solo en algunos de ellos.

b) Matices de la discusión:

▸ ¿Se necesitan nuevos tipos penales?

Los ciberdelitos son exactamente los mismos que los delitos que se establecen en el Código Penal, y su única diferencia es que utilizan una plataforma digital para ser cometidos. Esta no deja de ser una apreciación polémica. Parte importante de las discusiones de este nodo, es la corriente que quiere hacer nuevos tipos penales para estos delitos pues considerarían que Internet es un "pueblo sin ley"; por otro lado, están los que consideran que no solamente hacer nuevos tipos penales es innecesario, sino que también peligroso para el desarrollo de Internet y el respeto de otros derechos humanos en la red.

▸ ¿Se justifica la ciberseguridad a toda costa?

La ciberseguridad es el conjunto de herramientas y políticas que pueden utilizarse para proteger los dispositivos informáticos conectados, los usuarios, los servicios y aplicaciones, muchas de ellas diseñadas para combatir los ciberdelitos (como se aprecia, puede ir desde leyes a simples programas de antivirus). La ciberseguridad es un concepto con importancia cada vez mayor en distintas instancias de discusión de políticas de Internet, como también en la presentación de aplicaciones. Con todo, siempre hay que comprender que detrás de la emergencia del concepto, también se maquinan modelos de negocio. En otras palabras, muchos estudios alarmistas con respecto a la ciberseguridad y los ciberdelitos vienen de fuentes con intereses económicos concretos, por lo que es importante hacer un análisis mesurado cuando se habla de este tópico.

▸ El *hacking* como delito y como protesta

En una definición simple, es el acceso ilícito a un sistema informático y es uno de los delitos más antiguos en este campo. Los objetivos más conocidos de sus ataques son sitos web del gobierno y algunas empresas, aprovechando blancos

30 El Ciberdelito: Guía para los países en desarrollo. De División de Aplicaciones TIC y Ciberseguridad (CYB) y el Departamento de Políticas y Estrategias de la Oficina de Desarrollo de las Telecomunicaciones, UIT. En http://www.itu.int

de vulnerabilidad en su seguridad. En muchos casos, la motivación no se limita al acceso ilícito al sistema informático, sino que éste es un medio para perpetrar otros delitos, como el espionaje o la manipulación de datos y los ataques de denegación del servicio (DDoS, ver recuadro siguiente). Pero en otros casos, se trata de hacktivismo, que es "la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software".[31] Ambas actividades son consideradas delitos, a pesar de sus intenciones diversas y sus valoraciones culturales diferentes.

31 Hacktivism and the Future of Political Participation. Por Alexandra Samuel. Agosto 2004. En http://www.alexandrasamuel.com

Los DDoS más noticiosos del último tiempo

Un ataque de denegación de servicio (DDoS, *Denial of Service*) es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación de servicio de los usuarios del sistema afectado.

Una de las guerras de DDoS más conocida, ocurrió debido a que en el 2010, Wikileaks (encabezado por Julian Assange) filtró a la prensa internacional una colección de cables confidenciales entre el Departamento de Estado estadounidense con sus embajadas por todo el mundo, lo que inició la persecución oficial de Assange por parte de EE. UU.

En un principio, un ataque DDoS forzó a Wikileaks a irse a un servidor de Amazon, que después les canceló el servicio por presiones de Estados Unidos. Poco después, su proveedor del dominio, EveryDNS.net, les quitó el servicio acusando que los ataques estaban poniendo en peligro la estabilidad de los demás sitios servidos por la empresa. Esto obligó a tener más de 500 servidores espejo (*mirrors*) alojando los contenidos para intentar evitar que los documentos se perdieran.

El contraataque no demoró en coordinarse y estuvo a cargo de Anonymous, quienes se atribuyeron el ataque de DDoS al banco suizo Post Finance, que congeló la cuenta de Assange, así como a PayPal, por cerrar la cuenta donde WikiLeaks recibía sus donaciones; entre otros servicios de Internet involucrados en la persecución de la plataforma.[32]

32 Más información en: WikiLeaks desata guerra de ataques DDoS. Por Cony Sturm, de Fayerwayer. 7 de diciembre del 2010. En http://www.fayerwayer.com

▸ Pornografía infantil y su persecución en Internet

Al contrario de la pornografía de adultos, donde existe divergencia de opiniones, cuando se trata de pornografía infantil hay unanimidad en su condena y los delitos relacionados con ella se consideran generalmente actos criminales. La gran diferencia de posiciones no está en la condena del delito, sino en la forma de combate a la pornografía infantil a través de la red. Esto, porque a pesar de que los pedófilos y redes que trafican este material suelen utilizar avanzadas técnicas de encriptado de información, que dificultan de sobremanera las investigaciones penales, muchas veces se ignora este hecho y se insiste en concentrar la vigilancia en redes donde estos delitos no se cometen y, lo más grave, pasando a llevar derechos básicos de los demás ciudadanos.

Así, muchas de las iniciativas legales que hoy vemos, insisten en la posibilidad de recurrir a métodos tales como imponer a los proveedores de servicios de Internet bloquear y/o filtrar el acceso a sitios web que contengan contenido pornográfico, no necesariamente infantil. Estas medidas contienen dos grandes problemas: desconocen que Internet no es una red centralizada, por lo que el control de todo el contenido es imposible (lo vimos en la primera etapa de esta guía); y aún más peligroso, violan los derechos humanos del resto de ciudadanos que, al asumir estas ineficientes medidas, deben renunciar a su presunción de inocencia, privacidad, libertad de expresión, entre otros (ver cuadro siguiente).[33]

▸ *Grooming*

Son las acciones deliberadas por parte de un adulto para establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener satisfacción sexual mediante imágenes eróticas o pornográficas del menor o, incluso, como preparación para un encuentro sexual. Como lo vimos en la pornografía infantil, no hay discusión en la importancia de atacar el delito, sino más bien la polémica radica en el cómo: si es necesario hacer nuevos tipos penales y si, en el camino a castigar estos encuentros, estamos violando los derechos humanos de todos los demás ciudadanos.

33 Para más información, ver el recuadro "¿Un ataque al abuso de menores o a la Internet libre?".

¿Un ataque al abuso de menores o a la Internet libre y los derechos humanos?

Cuando se cubre periodísticamente tecnologías como Internet, hay que aguzar la mirada crítica al momento de abordarlos. Acá, algunos ejemplos:

En Reino Unido se presentó la iniciativa de bloquear la pornografía a todos los usuarios:
Con la excusa de ir contra "la corrosiva influencia de la pornografía en los niños" y con el fin de "proteger a nuestros menores y su inocencia", el gobierno de David Cameron presentó un paquete de ideas que van de bloquear la pornografía en el Internet de los británicos (a no ser que los usuarios le comuniquen a sus proveedores de Internet –ISPs– que quieren eliminar el bloqueo y, por ende, que sí quieren recibir porno), obligar a los motores de búsqueda a censurar los resultados relacionados con pornografía infantil y declarar ilegal la posesión de la llamada "pornografía violenta".

Los cuestionamientos van desde lo poco funcionales que son las "listas de pervertidos" pues están pensadas en intimidar a las personas que opten por el desbloqueo; la falta de claridad de cómo se asegurará la privacidad de estos usuarios; las razonables dudas sobre cómo los ISPs asegurarán la limitación de esa censura pues nada dice que material que toque estos temas y que no tenga ánimo pornográfico no sea bloqueado; lo absurdo que es pensar que las redes de pedofilia usan buscadores comunes de Internet; o, simplemente, que ni todo el bloqueo del mundo impedirá que todos los días, por distintos métodos, estos contenidos seguirán circulando por la red pues su naturaleza no es centralizada.

En Perú quieren poner filtros obligatorios a los proveedores de Internet por contenido porno:

El congresista Omar Chehade y la bancada Nacionalista de ese país, presentaron un proyecto de ley para terminar con el acceso de menores de edad a contenido pornográfico por la red, a través del establecimiento de filtros obligatorios a los proveedores de Internet. Como en Reino Unido, este filtro estaría implementado por defecto y para evitarlo habría que ponerse en contacto con el ISP correspondiente. Además, un comité de representantes de entidades públicas sería el encargado de determinar qué contenidos serían objeto de censura.

Nuevamente, las críticas van desde el peligro a la libertad de expresión o el desconocimiento total de las autoridades sobre cómo funciona Internet. Con todo, Miguel Morachimo de Hiperderecho lo resumió así: "Crear una lista negra obligatoria de páginas web y servicios bloqueados por defecto es una idea que, además de imposible, atenta contra los derechos fundamentales. Sería equivalente a que todos los programas de televisión y publicaciones pasen por una revisión previa antes de hacerse públicos".

▸ **Ciberterrorismo: ¿todo vale?**
Ya durante los 90, el debate sobre la utilización de la red por organizaciones terroristas giraba en torno a los ataques cometidos en la red contra infraestructuras esenciales como el transporte o el suministro de energía (ciberterrorismo) y al uso de la tecnología de la información en conflictos armados (guerra informática). El gran punto de la discusión hoy es: ¿existen amenazas probadas del terrorismo hacia una red como Internet? ¿Cuánto de ello hay de real y cuánto de oportunidad para controlar Internet? Como lo reconoce incluso documentación desde el ITU[29], en el debate no se ha logrado siquiera llegar a un consenso con respecto a la definición de terrorismo: "En un Informe del CRS al Congreso de los Estados Unidos, por ejemplo, se afirma que el hecho de que un terrorista adquiera por Internet un billete de avión a los Estados Unidos es una prueba de que los terroristas recurren a Internet para preparar sus ataque". Además, se han visto con preocupación programas secretos como PRISM o proyectos de ley como CISPA que prueban cómo, con la excusa del ciberterrorismo, se violan derechos humanos fundamentales.

c) ¿Quiénes son los protagonistas de este nodo?

▸ **Chile: Brigada Investigadora del Cibercrimen.**
Unidad especializada, dependiente de la Policía de Investigaciones de Chile, que se encarga de los delitos cometidos vía Internet, tales como amenazas, estafas, falsificación, pornografía infantil y delitos informáticos, entre otros.

▸ **OCDE: Organización de Cooperación y Desarrollo Económicos.**
Desde los años 80, la OCDE ha analizado la legislación vigente y ha formulado propuestas para combatir el ciberdelito, estipulando directrices para los países miembros.

▸ **Unión Europea.**
Los poderes de la Unión Europea son limitados cuando se trata de legislar en la esfera del derecho penal. Es decir, sólo tiene la posibilidad de armonizar el derecho penal de los Estados miembros en esferas especiales, tales como la protección de los intereses financieros de la Unión Europea y el ciberdelito.

34 El Ciberdelito: Guía para los países en desarrollo. De División de Aplicaciones TIC y Ciberseguridad (CYB) y el Departamento de Políticas y Estrategias de la Oficina de Desarrollo de las Telecomunicaciones, UIT. En http://www.itu.int

▸ **APEC: Foro de Cooperación Económica Asia-Pacífico.**
En diversas instancias, la APEC ha tenido preocupación por el ciberdelito, como con su Grupo de Trabajo de Telecomunicaciones, que expresó su posición en cuanto a la legislación sobre el ciberdelito, remitiéndose para ello a los enfoques internacionales adoptados por instituciones que van de las Naciones Unidas al Consejo de Europa.

▸ **OEA: Organización de los Estados Americanos.**
Desde 1999, la Organización de los Estados Americanos (OEA) ha venido ocupándose activamente de la cuestión del ciberdelito en la región. Incluso, ha recomendado que los Estados consideren la posibilidad de aplicar los principios del Convenio de Budapest (ver a continuación), así como de adherirse a dicho instrumento, y de adoptar las medidas jurídicas y de otro tipo que exija la implementación del Convenio.

d) ¿Cuáles han sido las iniciativas legales más importantes?

▸ **Convenio de Budapest sobre el Cibercrimen (Convenio de Budapest).**
Su importancia es fundamental porque es el primer tratado internacional, diseñado en el seno de la Unión Europea, que trata sobre delitos cometidos a través de Internet y otras redes informáticas. Fue firmado por todos los países miembros, incluidos cuatro Estados no miembros del Consejo de Europa, a saber: Canadá, Estados Unidos, Japón y Sudáfrica, que habían participado en las negociaciones. Asimismo, parte importante de legislaciones de otros países del mundo se han adaptado a lo estipulado en este convenio. En particular, este tratado se encarga de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red, además de regularizar una serie de competencias y procedimientos, como la interceptación legal.

▸ **Ley N°19.223 sobre delitos informáticos en Chile.**
Pionera en la región, en junio de 1993 entró en vigencia en Chile la Ley N°19.223, sobre delitos informáticos. En ella se contemplan dos figuras delictivas: el sabotaje y el espionaje informático. La ley protege la calidad, pureza e idoneidad de la información, el patrimonio en el caso de los fraudes informáticos; la privacidad, intimidad y confidencialidad de los datos en el caso del espionaje informático, entre otros temas [35]. Con todo, esta ley ha recibido escasa aplicación porque las conductas que castiga no están bien definidas y porque a veces pareciera que protege más la infraestructura física que la información contenida.

35 Lo Delitos Informáticos. Por la Contraloría Universitaria. Julio 2007. Universidad de Concepción. En http://www2.udec.cl/contraloria/docs/materias/delitosinformaticos.pdf

e) Tres principios para la cobertura de los ciberdelitos en Internet

Parte importante de las legislaciones y campañas ciudadanas sobre Internet, apuntan de algún modo u otro a los delitos informáticos, siendo quizás uno de los temas más candentes, la regulación de la pornografía infantil y otros graves delitos contra infantes. Aquello acapara alta cobertura en los medios, pero desde una perspectiva de los derechos, debe ser un tema tratado con extrema cautela.

A continuación, te presentamos tres principios que pueden ser de ayuda al momento de una cobertura periodística más completa de estos temas.

- **El principio de soberanía nacional**.

En general, no solo en cuanto a los ciberdelitos, siempre hay dudas sobre qué ocurre cuando los delitos por Internet son cometidos en otro país. En el caso particular de los ciberdelitos, este es un tema también complejo. Por lo general, el principio de soberanía nacional no permite a un país realizar investigaciones dentro del territorio de otro país sin el permiso de las autoridades locales.

- **No es posible ni eficiente controlar Internet**.

Parte importante de las iniciativas legales respecto a ciberdelitos, caen en la ilusión de que Internet es una red centralizada que puede ser fácilmente controlable. Detectar cuándo una iniciativa cae en estas falacias, permite de inmediato saber que se trata de un proyecto que encontrará voces críticas, sobre todo desde organismos que trabajan derechos digitales.

- **¿Cómo se afectan los derechos de la ciudadanía?**

Como lo hemos visto en otros nodos críticos, es fundamental analizar una ley o una iniciativa, en este caso de ciberdelitos, desde una perspectiva de derechos humanos: cómo una iniciativa que puede ser loable en sus intenciones, puede terminar lesionando los derechos humanos del resto de los ciudadanos. Parte importante de las polémicas en el mundo de los ciberdelitos es porque la respuesta a esa pregunta devela más bien consecuencias negativas.

III. Privacidad en la era de las redes sociales

a) ¿Qué se discute?:

Una definición tradicional describe la privacidad como "el derecho a que lo dejen a uno en paz". De forma tradicional, la privacidad ha estado ligada principalmente a la relación entre ciudadanos y el Estado, aunque hoy, sobre todo en la era de Internet, se incluye nuestra relación con las empresas. Las definiciones modernas de la privacidad se enfocan en la privacidad de las comunicaciones (comunicaciones libres de vigilancia) y de información (información individual libre de manipulación por parte de terceros).

¿Se puede garantizar la privacidad de las personas en un contexto digital, con las facilidades de la tecnología para la copia exacta de información, el monopolio de parte importante de las comunicaciones, el rastreo de comportamientos, o incluso, la voluntaria entrega de información que los mismos ciudadanos hacen en las redes sociales *online*? Así, lo que se discute es cuánto el Estado y las empresas respetan nuestra privacidad y, también, cuánto nosotros como ciudadanos estamos dispuestos a ceder de ese derecho, conscientemente.

b) Matices de la discusión:

▸ **La discusión de la privacidad en Estados Unidos y en la Unión Europea.**
En la discusión de la privacidad hay dos grandes tendencias, representadas por Estados Unidos y la Unión Europea.[36]

En el primer país, el enfoque dominante es la "autorregulación" y, por tanto, las políticas de privacidad son establecidas por las empresas comerciales. Si bien una crítica podría ser que los ciudadanos están en posición de debilidad en comparación con las grandes empresas, lo cierto es al momento de presentar demandas, el sistema judicial es tan exigente con las compañías, que éstas evitan llegar a esas instancias. Por su parte, el enfoque de la Unión Europea es más bien opuesto: considera que la protección de la privacidad de los ciudadanos debe ser garantizada por las autoridades públicas. Así, para los ciudadanos europeos, existe una directiva de protección de datos y agencias en cada país que se encargan de velar por la protección de su privacidad.

36 Gobernanza de Internet. Asuntos, actores y brechas. Por Jovan Kurbalija y Eduardo Gelbstein. 2005. Publicado por DiploFoundation y la Sociedad para el Conocimiento Mundial.

Asimismo, la Unión Europea determina qué legislaciones tienen una protección adecuada, de manera de permitir el tratamiento transfronterizo de datos personales de ciudadanos europeos. Como EE. UU. evidentemente no cumple con ese estándar, se necesitó llegar a un acuerdo que pudiera permitir que el mercado funcione, a pesar de la diferencia de estándares. Así, el Departamento de Comercio de los Estados Unidos y la Comisión Europea acordaron "Principios *Safe Harbor*"[37] (Puerto Seguro), es decir, un conjunto de principios de protección de datos que permiten que las compañías de los Estados Unidos cumplan con el requisito de proporcionar protección adecuada a la información personal que se transfiera desde la Unión Europea a los Estados Unidos, establecidos según la ley de la Unión Europea. El EEA (Área Económica Europea) también ha reconocido que los principios *Safe Harbor* de los Estados Unidos proporcionan una protección de datos adecuada.

El choque entre la Unión Europea y las compañías de Estados Unidos

¿Qué pasa con compañías de Estados Unidos que desarrollan aplicaciones y servicios *online* para un mercado global y que llegan a los usuarios de la Unión Europea? El mayor conflicto entre estas dos partes, es el uso de los datos personales de los ciudadanos europeos por compañías de Internet que están en Estados Unidos.

Un ejemplo es el caso de Google, empresa a la que el año 2013, seis agencias de protección de datos europeas se unieron para denunciar que presuntamente estaría incumpliendo la regulación de privacidad que exige la U. E. Reveladora también es la calificada "mayor campaña de *lobby* que se recuerda en Bruselas", comandada por empresas y el gobierno de EE. UU., para aprovechar la revisión de las políticas de privacidad de la U. E.

37 El Acuerdo de Puerto Seguro con los Estados Unidos de América. En http://www.agpd.es/

▸ **La privacidad de un individuo ya no se ve amenazada solo por el Estado.**
En la vida moderna de gran parte de los países con un capitalismo avanzado, la información se ha convertido también en un bien de consumo muy apreciado. Sobre todo, cuando gracias a la tecnología, se pueden desarrollar aplicaciones que permiten perfilar a los individuos como potenciales clientes[38]. La fuerza de la información en el marketing es hoy una de las preocupaciones más importantes con respecto a la privacidad, que hace que nuestros datos como ciudadanos ya no sean solo de interés de los Estados, sino también de las empresas privadas. Asimismo, la privacidad también se ve amenazada en el día a día incluso en ambientes de trabajo, donde se aplican herramientas para violar la intimidad de los trabajadores, como el uso de cámaras o el espionaje de correos electrónicos.

▸ **Terrorismo: la asociación del Estado y las empresas.**
Tanto el Estado como las empresas recolectan grandes cantidades de información de los individuos. Hasta hace poco, lo que eran solo elucubraciones de que ambas partes se intercambiaban información con la excusa de prevenir actividades terroristas, ha sido confirmado a cabalidad a partir del caso Snowden y la NSA[39]. Esta asociación ha sido calificada por muchos como necesaria, pues es la forma para mantener a los ciudadanos seguros a pesar de las constantes amenazas de terrorismo y ciberterrorismo. Para otros, no solo se trata de un método inútil porque los atentados terroristas no han sido detenidos, sino que además esos "potenciales" actos no pueden ser la excusa para pasar por arriba de derechos tan importantes como la privacidad, la libertad de expresión y el debido proceso.

▸ **Cuando hay una aplicación gratis, el producto eres tú.**
Esta frase es una de las más populares para explicar que no existen aplicaciones en Internet gratis, sin que haya un costo pagado por los usuarios a través de la entrega voluntaria y permanente de su información personal. Esta última, permite configurar perfiles de información que son, finalmente, los productos que compran las empresas para distintos motivos, como el marketing. Los casos son diversos: Facebook, Twitter o Google: no pagas nada por sus aplicaciones, pero estas empresas ganan dinero gracias a tu información personal.

38 Ver en esta misma guía Cookies en "Capa de estándares de contenido y aplicaciones: el vehículo que te permite circular" y el cuadro correspondiente "¿Dónde ocurren las noticias en esta capa de estándares de contenidos y aplicaciones?".

39 Ver en este mismo capítulo: "¿Cuáles han sido las iniciativas más importantes?".

▸ **Más allá de las *cookies*: dejas huellas dactilares en tu navegador.**
Puedes desactivar las *cookies*[40] y ajustar los niveles de privacidad de tu navegador. Pero eso no será suficiente para preservar tu privacidad, dice el estudio de Peter Eckersley.[41] ¿La razón? La llamada técnica del *browser fingerprinting*. Los navegadores modernos (Explorer, Firefox, etcétera) han sido diseñados para enviar a los sitios web un torrente de información que, en general, se piensa que es inocua, por ejemplo: los números detallados de versión del navegador, la información del sistema operativo, el tamaño de la pantalla, qué fuentes están instaladas, y a veces, incluso, el orden en que se han instalado las fuentes. El punto que esta información, si se combina entre sí y se compara con los navegadores de otros usuarios, terminan haciendo que los datos, en un principio generales, pueden ser de carácter personal. Como dice Declan McCullagh,[42] es como ser capaz de encontrar el nombre de alguien si sabe su fecha de nacimiento, código postal y el sexo, lo que no es una tarea muy difícil.

▸ ***Cloud computing* y la trampa de la "nube".**
La "computación en nube" consiste en un conjunto de tecnologías y modelos de servicio que se centran en la utilización y suministro de aplicaciones informáticas, capacidad de procesamiento, almacenamiento y memoria a través de Internet y ya no a través de suites de licenciamientos, el propio computador u otro aparato de almacenamiento personal. Por una parte, el *cloud computing* puede generar importantes beneficios económicos, por la facilidad de acceso a tu información o el costo marginal de tecnología de primera (por ejemplo, Google Drive o Dropbox). Pero asimismo, una de las principales preocupaciones es el cuidado de los datos personales de las personas que usan este tipo de servicios, a saber, la falta de control sobre los datos y la insuficiente transparencia con respecto al tratamiento de estos.

Ante este último punto, un par de puntos fundamentales a aclarar. Primero, y como concluimos en la primera parte de esta guía, los datos que se manejan en Internet no están en una "nube" transparente y neutral, sino que en grises y calurosos *datacenters* de empresas, situadas en países determinados, con auto-

40 Ver en esta misma guía Cookies en "Capa de estándares de contenido y aplicaciones: el vehículo que te permite circular" y el cuadro correspondiente "¿Dónde ocurren las noticias en esta capa de estándares de contenidos y aplicaciones?".

41 En Panopticlick: panopticlick.eff.org

42 Tracking Web users without using cookies. En CNET. 17 de mayo del 2010. En http://news.cnet.com

ridades ávidas de datos personales. Muchas veces el nombre de *cloud computing* hace olvidar la dimensión física y política de cómo funciona Internet.[43] Segundo: a menudo se cree que la encriptación resuelve los problemas de vulneración a la protección de las comunicaciones en este sistema, lo que no es preciso. En Dropbox, por ejemplo, si bien la comunicación entre el cliente y el servidor es a través de un protocolo encriptado, eso no quiere decir que aquello que está almacenado en la "nube" lo esté. De hecho, no lo está[44].

▸ **¿Es privado el número IP?**
Las autoridades de protección de datos de los estados miembros de la Unión Europea determinaron que la dirección IP se considera como un dato de carácter personal. Esto contrasta con las opiniones de otros como Google o Yahoo que afirman que las direcciones IP pueden no ser personales o ligadas a un individuo, como en el caso de los cibercafés o de las oficinas cuyos computadores son usados por varias personas. Con todo, en el 2008, Google decidió borrar tras nueve meses, en lugar de los 18 que había hasta ese momento, el número de dirección IP que identifica a cada ordenador que se conecta a Internet, devolviendo el anonimato a los historiales de búsqueda de los usuarios. Su decisión respondió a un pedido de un grupo de organismos europeos de protección de datos personales.[45]

▸ **Aplicaciones móviles y el rastreo de datos.**
Parte importante de la discusión de la protección de datos e Internet pasa por las aplicaciones que están en los teléfonos inteligentes. Muchas de ellas tienen condiciones de privacidad realmente invasivas, como captar los datos de agendas telefónicas o funcionar solo con la activación de la georeferencia a través del GPS. La mayoría de las veces, estas condiciones poco favorables para la privacidad (tanto de aplicaciones pagadas como no pagadas) pasan desapercibidas por los usuarios y tampoco son valoradas por muchos analistas de tecnología.

▸ **Derecho al olvido y su choque con la libertad de expresión.**
Es el derecho a pedir el borrado de datos personales que se consideran obsoletos, descontextualizados o lesivos de otros derechos. Por ejemplo, si alguien en su juventud cometió alguna locura (una foto osada, quizás) y en la red se informa

43 Ver en este mismo capítulo: "¿Cuáles han sido las iniciativas más importantes?".

44 Acusan a Dropbox de mentir sobre la seguridad del servicio. Por Cony Sturm. 17 de mayo del 2011.
En http://www.fayerwayer.com

45 Revisar en esta guía el cuadro "¿Dónde ocurren las noticias en esta capa de estándares y servicios técnicos?" en "Capa de los estándares y servicios técnicos: las reglas del tráfico" y "¿Es el número IP privado?" en "Privacidad en la era de las redes sociales".

profusamente este hecho, tal vez el derecho al olvido puede entregar una herramienta útil al afectado, para que en un buscador de Internet no quede asociado para siempre su nombre con esos contenidos. Lo mismo aplica para otros hechos que, siendo ciertos, puedan brindar una idea demasiado parcial y errada sobre una persona, o que afecten desmedidamente su esfera privada. La polémica comienza cuando está la amenaza de extender la interpretación al derecho a pedir el borrado de cualquier dato personal de su titular, cuando no es estrictamente necesario o existe una excepción legal determinada que permita almacenar o tratar los mismos. También surgen interrogantes respecto a la posible colisión de éste con el derecho fundamental a la libertad de expresión, privilegiando determinados conceptos de los derechos de honra y vida privada antes que la libre difusión y acceso a las ideas.

▸ **Privacidad por diseño (*privacy by design*) y privacidad por defecto (*privacy by default*).** Como dice la creadora del concepto, Ann Cavoukian,[46] la privacidad por diseño promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización. Así, por ejemplo, la privacidad por diseño se extiende a una "Trilogía" de aplicaciones que engloban: 1) sistemas de tecnologías de la información; 2) prácticas de negocios responsables; y 3) diseño físico e infraestructura en red.

Por su parte, la privacidad por defecto busca que los sitios web, aplicaciones y otros software tengan configurada la privacidad por defecto y los usuarios no tengan que gastar tiempo en hacerlo. Así, el uso de los datos personales para cualquier otro objetivo que vaya más allá de los que estén especificados, sólo se permitiría con el consentimiento explícito del usuario.

▸ **Debido proceso digital y libertad de expresión.**
Nadie puede obtener datos personales sensibles así como así, sin que se respeten derechos garantizados por ley. El derecho al debido proceso es crucial, porque refuerza otros derechos fundamentales como la privacidad, el acceso a la información, así como la libertad de expresión, movimiento y asociación. Si al momento de obtener datos privados no se respeta el debido proceso, no solo estamos ante un comportamiento ilegal, sino que se deja al o los ciudadanos afectados completamente desprotegidos. Muchos son los antecedentes que indican que, ante

46 Privacy By Design. Los 7 Principios Fundamentales. Febrero del 2011. En http://www.privacybydesign.ca

supuestos delitos en Internet, en Chile los organismos competentes del Estado caen en violaciones al debido proceso[47], siendo la falta más común que la policía no obtenga una orden judicial para obtener datos sensibles de las personas. A pesar de que el Código Procesal Penal establece de manera incuestionable (art. 9) que cualquier actuación del juicio que comprometa los derechos fundamentales de un individuo requerirá de autorización judicial previa, sin distinción entre medios analógicos y medios digitales, ni derechos análogos y digitales.

Algunos casos chilenos donde no operó el debido proceso.

Muchos han sido los casos sobre investigación de usuarios en Internet donde, lamentablemente, no se ha respetado el debido proceso al momento de conseguir datos personales.

Uno de los casos más conocidos, fue la demanda a un tuitero por parte del empresario Andrónico Luksic, quien lo acusó por una supuesta usurpación de identidad a través de diversas cuentas de Twitter. Uno de los tantos puntos de polémica de este caso, fue que la fiscalía había obtenido información desde Twitter (basada en California, EE. UU.), para obtener las direcciones IP y correos electrónicos asociados a las cuentas de Twitter, sin una orden judicial mediante como establece el debido proceso en Chile.

La falta de debido proceso en casos judiciales respecto a Internet no es ninguna novedad en Chile. ONG Derechos Digitales, desde el año 2008 viene trabajando en resguardar la legalidad de las actuaciones de fiscales y policías en las investigaciones criminales que llevan a cabo. Ya en esa fecha, los casos de huelga.cl y loserpower.com daban cuenta de los bajos estándares de respeto a los derechos fundamentales con que trabajan los perseguidores penales en nuestro país.

47 Fiscales, policías e infracciones al debido proceso en Chile. Por Francisco Vera. 21 de febrero del 2013. En http://www.derechosdigitales.org

c) ¿Quiénes son los protagonistas de este nodo?

▸ **Empresas desarrolladoras de aplicaciones en Internet.**
Pequeñas o grandes, las empresas desarrolladoras de aplicaciones en Internet son protagonistas importantes de este nodo, ya sea porque pueden impartir un modelo de negocio basado en la recolección de datos personales de los usuarios; porque no incluyen estándares de seguridad para el manejo de información; y/o porque –con o sin conocimiento– entregan información personal a entidades de gobierno sin respetar el debido proceso. Muchos de estas situaciones las hemos visto con empresas tan conocidas como Facebook, Twitter o Google.

▸ **Agencias de vigilancia del Estado.**
La vigilancia es considerada una actividad de inteligencia del Estado, la que es hecha a través de organismos especiales. En el caso de Chile, por ejemplo, es hecha a través de la ANI (Agencia Nacional de Inteligencia) o de la NSA (Agencia Nacional de Seguridad), en el caso de Estados Unidos. Debido a la gran cantidad de información personal que se encuentra en Internet, estos organismos han puesto sus ojos en ella para realizar actividades de vigilancia. Si bien esta última no está prohibida, los mecanismos para hacerla sí están limitados por las leyes de cada país y por algunos tratados internacionales, los que deben ser respetados a cabalidad pues si no, se trata de una actividad ilegal. Por lo demás, esas actividades deben seguir ciertos principios básicos como proporcionalidad y debido proceso, entre otros.

▸ **Agencias de protección de datos personales de U. E.**
En la Unión Europa, cada uno de los países miembros tiene su propia agencia de protección de datos, como por ejemplo, la Agencia Española de Protección de Datos (AEPD). Estos organismos pueden iniciar acciones contra empresas de Internet que no respeten las medidas de protección de datos que aseguran los gobiernos de esta parte del mundo a sus ciudadanos. Estas agencias agrupadas conforman el Grupo Europeo de Protección de Datos del Artículo 29. Entre otras cosas, el GT 29 aprueba un informe anual con las novedades de cada Estado miembro en materia de protección de datos.

▸ **Sistema judicial**
Jueces, fiscales y policías de investigaciones un papel fundamental en el respeto del debido proceso. Ya hemos visto como en muchas ocasiones, acá en Chile, asuntos tan básicos como una orden judicial para la entrega de datos de un usuario de la red son simplemente ignorados.

▸ **El usuario**

Si bien mucho de la protección depende del comportamiento del Estado y de las empresas, es indudable que el usuario de Internet debe tener no solamente conocimiento sobre cómo se maneja la privacidad de sus datos en la red, sino que también debe actuar responsablemente. Concordante a esto, en sus manos tiene distintas acciones como preferir aplicaciones que respeten su privacidad; saber qué información publicar y qué otra no; conocer herramientas de seguridad (como el encriptamiento[48]), etcétera.

d) ¿Cuáles han sido las iniciativas más importantes?

▸ **Ley de protección de datos en Chile:**

En 1999, Chile se transformó en el primer país de América Latina en disponer de una ley general sobre protección de la información personal. Con los años, la ley demostró su ineficacia para proteger a las personas, facilitar la transferencia internacional de datos y adecuarse a los estándares internacionales. Esto llevó a nuevos proyectos de ley, como el que se discute hoy (año 2013) en el Congreso. A pesar de que son reconocidos algunos avances en la materia, ese proyecto en términos generales no avanza en materia de protección de datos y, muy por el contrario, "implica un retroceso que sacrificará los derechos de las personas y pondrá en riesgo la competitividad de la industria local"[49]. Con todo, en Chile y hasta que no se apruebe el nuevo proyecto de ley, la normativa vigente es la de 1999.

▸ **PRISM**

Programa de inteligencia llevado adelante por la NSA (Agencia Nacional de Seguridad), que involucra a varias empresas de Internet, incluyendo a Microsoft, Apple, Yahoo y Google, entre otras, y que permitiría (según las filtraciones de la prensa, porque hasta la fecha no hay información oficial) acceder en tiempo real a datos tales como correos electrónicos, mensajes, videos, perfiles de redes sociales, etcétera, con la excusa de la lucha contra el terrorismo. Parte importante del desconocimiento de PRISM (y otros programas que se han conocido últimamente) se debe a que las leyes de inteligencia estadounidenses no permiten a las empresas transparentar cuánta información les solicitan bajo el pretexto de la prevención del terrorismo. Por ejemplo, algunos dicen que es un sistema computacional que funciona dentro de la NSA, otros, que existen equipos de la NSA directamente dentro de las empresas mencionadas. Lo cierto es que el programa existe y que el analista que lo filtró a la opinión pública, Edward Snowden, ha sido tenazmente perseguido por Estados Unidos.

48 La encriptación es el proceso para volver ilegible información considera importante. Hay una serie de herramientas que permiten hacerlo con nuestros correos, chats, etcétera.

49 Chile: Proyecto de ley de protección de vida privada es un retroceso para ciudadanos e industria. Por Alberto Cerda. 10 de junio del 2013. En http://www.digitalrightslac.net

Algunos de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones

Legalidad	Cualquier limitación al derecho a la privacidad debe ser prescrita por ley.
Objetivo Legítimo	Las leyes sólo deberían permitir la vigilancia de las comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo.
Proporcionalidad	Las decisiones sobre la vigilancia de las comunicaciones deben tomarse sopesando el beneficio que se persigue contra el daño que se causaría a los derechos de los individuos.
Debido Proceso	El debido proceso exige que los Estados respeten y garanticen los derechos humanos de los individuos asegurando que los procedimientos legales sean respetados.
Notificación al usuario	Los individuos deberían ser notificados de una decisión que autoriza la vigilancia de las comunicaciones con el tiempo e información suficientes para permitirles apelar la decisión, y deberían tener acceso a los materiales presentados en apoyo de la solicitud de autorización.
Transparencia	Los estados deberían ser transparentes sobre el uso y el alcance de las técnicas y los poderes de la vigilancia de las comunicaciones.

¿Cuántos de estos principios se pueden aplicar en el análisis de PRISM?
Para conocer otros principios, visita necessaryandproportionate.org

▸ Discusión de la privacidad en la U. E.

Actualmente, se está discutiendo un nuevo reglamento europeo de protección de datos, que pretende adaptar a la era de Internet la actual directiva, vigente desde 1995. Como describe el diario El País de España,[50] la modificación consta de dos partes:

- Reglamento para las empresas: El reglamento limita mucho el acceso que tienen las empresas a los datos personales y refuerza el consentimiento que debe dar el usuario para que esos datos sean tratados con fines comerciales. Las empresas que incumplan las normas deberán hacer frente a multas que pueden alcanzar hasta el 2 % de la facturación anual.
- Directiva que regula el tratamiento de datos en el sector público.

Asimismo, Bruselas se propone regular otros elementos como el derecho al olvido.

En su avance, las acusaciones de *lobby* por parte de Estados Unidos y sus compañías, se han hecho tan fuertes que han sido reconocidas por las propias autoridades de la Unión Europea. De hecho, a finales de 2011, poco después de que la Dirección General de Justicia remitiera un borrador al resto de departamentos de la Comisión Europea, el texto llegó misteriosamente a manos del gobierno estadounidense y desde allí se desató una fuerte campaña por influir a los legisladores, lo que ha sido permanente espacio de atención de la opinión pública.

e) Tres principios para la cobertura de la privacidad en Internet

Ya sea por las demandas a grandes empresas como Facebook o Google, o por la escandalosa filtración de datos sensibles en Internet, entre otros temas que ya son del día a día, este nodo crítico de Internet ofrece amplia atención periodística.

A continuación, te presentamos tres principios que pueden ser de ayuda al momento de una cobertura periodística más completa de estos temas.

▸ La privacidad es un derecho humano, no un capricho del usuario

La privacidad no es un capricho ni un tema de moda debido a Facebook. Todo

50 EE UU presiona en la sombra para frenar la normativa de privacidad europea. Lucía Abellán. El País, Internacional. 21 de julio del 2013. En http://internacional.elpais.com

ciudadano tiene derecho a tener privacidad y aquello es un principio fundamental para ser respetado por las empresas y el Estado. Cada vez que ocurre un hecho noticioso respecto a, por ejemplo, filtraciones de datos personales en la red, es importante saber que aquello atenta contra los derechos humanos y debe ser atendido por el Estado con la gravedad que eso implica.

▸ La vigilancia del Estado no es un campo sin ley

Si un Estado decide vigilar a uno o más ciudadanos a través de Internet, debido a la excusa que sea, esa vigilancia está normada y cualquier violación a ella está contra las leyes, incluyendo el debido proceso. Un buen recurso para conocer estos principios a respetar en la vigilancia, está compilado en "Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones", hecho a propósito del escándalo PRISM.[51] Aquellos significa que, cada vez que exista un hecho noticioso donde se pone al descubierto la vigilancia del Estado a través de métodos en Internet o no, se debe averiguar si esta actividad cumplió con principios de derechos humanos al respecto. Cualquier violación de ellos, merece la mayor gravedad y la respuesta del Estado.

▸ Privacidad por defecto o la responsabilidad de las compañías en la protección de datos

Siendo la privacidad un derecho humano, las empresas que desarrollan aplicaciones digitales tienen la obligación de prestar condiciones de privacidad a los usuarios e informar de aquellas. Como hemos visto, hay buenas prácticas que deben alentarse a favor de la protección de nuestros datos, como la "privacidad por defecto" y la "privacidad por diseño". Con todo, y según el país, el control de estas condiciones será dependiente o del Estado o, simplemente, quedará en la autoregulación. Por eso es importante que, desde una perspectiva crítica, los periodistas se transformen en informadores de las condiciones de privacidad de un producto o compañía y exijan cada vez más altos estándares para la ciudadanía.

51 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. 10 de julio del 2013. En https://es.necessaryandproportionate.org

IV. La batalla de la "piratería" *online*

a) ¿Qué se discute?:
Básicamente, la discusión sobre la "piratería" *online* se concentra en el reclamo de los titulares de derechos de autor (no necesariamente los autores, sino los dueños de esos derechos) por el uso de obras sin su autorización en Internet. En palabras más simples, el reclamo se dirige a que las obras circulen por la red sin pagarle a los titulares. Estas obras pueden ser musicales, cinematográficas, editoriales, científicas, etcétera; y los reclamos pueden ir de utilizar un trozo de canción en un video casero en Youtube, subir una foto en alguna red social, el intercambio de música y películas, y mucho más. No obstante, la discusión es mucho más compleja que esta perspectiva.

b) Matices de la discusión:

- **No se trata de un robo:**

En el mundo digital, las copias de una obra (software, libros, fotos, etcétera) son exactamente iguales que el original y al hacer una, no desaparece la obra original. En otras palabras, el intercambio de archivos se basa en copias y no significa el robo de la obra original, que sigue estando presente igual que siempre luego de hacer reproducciones digitales. Otra muestra de esta circunstancia es que las leyes dan un tratamiento distinto a estas conductas, sin asimilarlas en ningún sentido, dado que es imposible hacerlo desde el punto de vista práctico.

- **No se trata de "piratería":**

Para ser estrictos, la piratería es una práctica de saqueo organizado o bandolerismo marítimo. Pensemos en la imagen clásica del marino con parche en el ojo y un pañuelo en la cabeza. Con el tiempo, ese concepto se asimiló a la venta falsificada de productos[52] y, con menos razón según esta perspectiva de la discusión, luego se asimiló la "piratería" al intercambio de archivos no autorizados en Internet.

Estos últimos son dos conceptos diferentes, fundamentalmente porque la piratería tradicional trata de una falsificación que, a través de su venta, busca tener réditos

52 De hecho, en el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Acuerdo sobre los ADPIC o, en inglés, TRIPS), se hace referencia a la palabra "piratería" para referirse al campo de la propiedad intelectual. Artículo 61: "Los Miembros establecerán procedimientos y sanciones penales al menos para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial". En http://www.wto.org/spanish/docs_s/legal_s/27-trips_05_s.htm

económicos para el falsificador en desmedro del autor original. En cambio, los archivos intercambiados en Internet son copias digitales exactamente iguales a la obra original, y en la mayoría de los casos, no se basan en una comercialización. Esto último, por cierto, es una de las discusiones más candentes: para los perseguidores de lo que llaman "piratería" *online*, servicios como Napster o Megaupload (que facilitan el intercambio de archivos) sí obtienen beneficios comerciales a través de la publicidad de los sitios; para otros, aquello no justifica criminalizar a los usuarios ni que se prohíban innovaciones como las redes P2P.

▸ **Ojo con quienes lideran los reclamos ¿quiénes resultan beneficiados?**
Muchos denuncian que la persecución al intercambio de archivos se hace por parte de una industria poderosa como Hollywood, que hasta antes de la emergencia de Internet, dictaba a su voluntad no solo la manera de hacer negocios, sino muchas veces los precios del mercado, en un mundo donde la producción cultural a nivel de industria es dramáticamente desigual entre países ricos y pobres. Así, muchos ven que Internet no solo ayuda a disminuir aquella brecha, sino también facilita el acceso a la cultura a personas que de otra forma jamás podrían acercarse a ellas.

▸ **Las cifras de piratería *online* ¿son creíbles?**
Cada cierto tiempo, diversos organismos y asociaciones liberan cifras sobre la "piratería" *online*. Muchos de esos estudios terminan en la prensa, convencidos de la supuesta objetividad de los números que, como es de esperar, siempre muestran el supuesto daño a la industria cultural por parte de los usuarios de Internet, de manera cabal e indudable. Pero lo cierto que cada uno de estos estudios es muy discutible, sobre todo al momento de analizar la metodología y la presentación de apresuradas conclusiones.

El especialista en nuevas tecnologías, el español Antonio Delgado, afirmó a propósito de estos estudios: "Conocer exactamente la cantidad de descargas de este tipo de material que se realizan desde España o en cualquier otro lugar del mundo es imposible. La forma habitual de aproximarse a este dato es mediante encuestas de mercado. Se encuesta a un número determinado de ciudadanos que estadísticamente representan al total de la población".[53] En Chile, en un estudio sobre las cifras de "piratería" de la Global Software Piracy Study, hecho por ONG Derechos Digitales y escrito por Pablo Viollier, se concluyó: "Bajo ninguna

53 Cómo se realizan los estudios sobre la piratería en Internet. Por Antonio Delgado. El Diario, Diario Turing. 1 de marzo del 2013. En http://www.eldiario.es/turing

circunstancia estas estadísticas deberían utilizarse como los datos oficiales de copia no autorizada de software a nivel global o de determinado país. Lo último es particularmente aplicable en lo que respecta a organismos públicos o fallos judiciales, los cuales por su naturaleza no pueden dejarse influenciar por estadísticas poco rigurosas y cruzadas por intereses particulares, como lo es el Global Software Piracy Study".[54]

▸ **Los "piratas" *online* compran más discos.**

Un estudio publicado por el Joint Research Centre de la Comisión Europea[55] afirma que la piratería *online* de música en Internet no afecta negativamente a las ventas en los canales de pago o legales. Es más, los investigadores aseguran que hay discos que no se venderían legalmente si no estuvieran también disponibles de forma ilegal a modo de prueba. Otra investigación, hecha por American Assembly, un centro de investigación en política pública en el que participa la Universidad de Columbia, concluyó que "los mayores piratas también son los mayores compradores de música legal"; en promedio, lo hacen 30 % más.[56]

▸ **Nuevas industrias culturales: *the sky is rising***

Internet se ve como una plataforma para la emergencia de nuevas industrias culturales más pequeñas, que antes no tenían acceso a la difusión de sus obras debido a los altos costos del modelo tradicional desarrollado fuera de Internet. Hoy, por ejemplo, muchas editoriales, sellos de música o cineastas, han optado por experimentar con Internet como plataforma de difusión y distribución de sus obras, incluso de forma gratuita, apostando a formas alternativas de financiamiento[57]. Asimismo, muchas tecnologías digitales y el acceso a obras han permitido la emergencia de renovadas formas de expresión, como los remix musicales y audiovisuales.

54 Análisis crítico de mecanismos para la medición de piratería de software. El caso particular del "Global Software Piracy Study". Pablo Viollier, en ONG Derechos Digitales. En http://www.derechosdigitales.org/

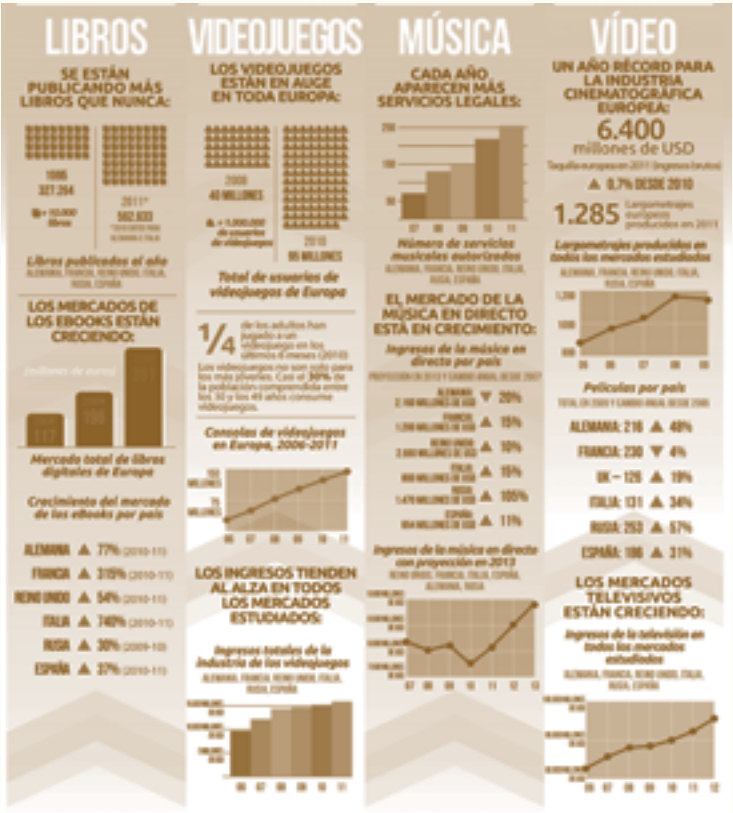
55 Digital Music Consumption on the Internet: Evidence from Clickstream Data. Luis Aguiar y Bertin Martens. 2013. En http://ftp.jrc.es

56 En http://piracy.americanassembly.org/

57 En Chile hay variados ejemplos de esto, como diversos sellos online o plataformas audiovisuales como Cinépata.

The sky is rising.

En Techdirt han puesto en línea su investigación *The sky is rising* (El cielo se está elevando). El reporte tiene ese nombre porque intenta desmitificar la idea de que la industria se está viniendo abajo por culpa de la piratería. Los datos demuestran que, al contrario de lo que señalan las grandes compañías del entretenimiento, en la misma época en que la cultura de compartir y la "piratería" se extienden gracias al Internet, las industrias culturales crecen en ganancias, y se generan nuevas oportunidades para artistas y creadores. El año 2013, la investigación se enfocó en datos de seis países, entre ellos España, y gracias a ello es que podemos encontrar el reporte traducido al Castellano (y entregado al dominio público).



http://www.techdirt.com/skyisrising2/

▸ **Algunos derechos reservados o acceso a la cultura.**
La polémica de la "piratería" *online*, ha hecho cuestionar también el sistema de los derechos de autor. En este último, el tradicional "todos los derechos reservados" de una obra significa que estos son atribuidos al titular de los derechos de autor de manera monopólica, durante toda la vida del autor y algunos años más después de su muerte.[58] Aquellas barreras a la explotación de una obra creativa, planteadas como justas para la retribución de un autor, con el tiempo se han ido acrecentando, haciendo que el acceso a la cultura y el conocimiento por parte del público sea siempre mediado a través de los monopolios de los grandes titulares de los derechos de autor.

Por las condiciones innatas de Internet, estas barreras parecen aún más absurdas. Por eso, y durante finales de los años 90 (aunque el movimiento es anterior) se populariza la denominada "cultura libre", que está en contra de los cerrojos impuestos al conocimiento por el tradicional *copyright* y su "todos los derechos reservados", y da un viraje, más que a la protección, al acceso a la cultura, proponiendo a los autores que adopten licencias que favorezcan el acceso a las obras. Con esta corriente, se consolidan las formas de licenciamiento del software libre[59] (licencias GPL, por ejemplo) y las que representan Creative Commons.[60]

▸ **La persecución de los derechos de autor como excusa de censura.**
Inicialmente, los derechos de autor fueron planteados como un mecanismo de censura que permitía a las autoridades tener control de las copias de las obras en los tempranos tiempos de la imprenta. Cientos de años después, la situación no dista mucho de aquello. En una plataforma de difusión de ideas y discursos críticos, la mejor manera de mantener control sobre esos contenidos es a través de demandas de derechos de autor.

58 En Chile, los derechos autor comprenden toda la vida del autor más 70 años después de su muerte.

59 Free Software Foundation: www.fsf.org

60 Creative Commons: www.creativecommons.org

¿Puede una disputa por un nombre de dominio ser una amenaza a la libertad de expresión?

Elmercuriomiente.cl, Barrickmiente.cl, Estafadoscorfo.cl, Estoyendicom.cl, y un largo etcétera. Todos, ejemplos de cómo los nombres de dominio en Chile se han establecido como un campo de disputa sobre el derecho de libertad de expresión.

Los nombres de dominio son la puerta de entrada, la carta de presentación de una web en el amplísimo espectro de Internet.

Mucho más que una simple marca, ellos reflejan el espíritu de sus creadores, la orientación de sus contenidos. Renunciar a un nombre de dominio tiene un gran costo para un proyecto, y por tanto, plantear una disputa por él y así acabar con los contenidos de un proyecto es, a todas luces, un recurso muy tentador y en nuestro país, algo frecuente. Así, diversos discursos críticos se ponen en entre dicho por el simple nombre de dominio, y las partes afectadas buscan disputar el dominio en NIC Chile.

¿Qué pesa más, la libertad de expresión o la propiedad intelectual? En Chile, las respuestas han sido, lamentablemente, vacilantes.

▸ **Usos justos ¿cuáles son los intereses públicos involucrados?**

Aun cuando exista una obra con sus derechos de autor en plena vigencia, la gran mayoría de las legislaciones comprende la necesidad que, en situaciones particulares, se pueda hacer uso de esas obras sin necesidad de solicitar la autorización previa y expresa del autor o el titular del derecho y, además, sin pagar ningún tipo de retribución económica para tales usos. Así también lo establece el Convenio de Berna,[61] el que pide siempre procurar que esas "excepciones y limitaciones al derecho de autor" (también conocidos como "usos justos") no deben causar un perjuicio injustificado a los intereses legítimos del autor. Con estas disposiciones vigentes, incluidas en la ley de propiedad intelectual de Chile, la pregunta que cabe hacerse es cuántas de las demandas por violaciones al derecho de autor en Internet, no se tratan de un "uso justo" de una obra.

61 Convenio de Berna para la Protección de las Obras Literarias y Artísticas: Tratado internacional sobre la protección de los derechos de autor sobre obras literarias y artísticas.

El famoso caso de Stephanie Lenz

De seguro tienes en tu videoteca algún registro familiar musicalizado: niños bailando alguna canción, cantando sobre un tema que les trae recuerdos, o quizás, haciendo una versión de alguna canción de un grupo que nos emociona. De hecho, no es extraño pensar que cada vez más son las personas que –para que estos videos no queden olvidados en una estantería– los suben a la web para compartirlos con sus amigos y familiares. Con estos antecedentes, ¿cabe la posibilidad de pensar que los protagonistas de estos videos están mermando los derechos de autor?

Veamos el caso de Stephanie Lenz. Esta ciudadana norteamericana fue demandada por el sello Universal por haber vulnerado sus derechos de autor. ¿Una pirata? ¿La persona detrás de una industria que lucra por los derechos de propiedad intelectual de otros? No exactamente. A Lenz le pareció una buena idea guardar como recuerdo un video que mostraba a sus hijos bailando una vieja canción de Prince que luego subió al portal Youtube. Para Universal fue suficiente excusa para exigir que se bajara el video de la red porque lesionaba los derechos de autor de los cuales son propietarios. La demanda fue retirada, finalmente, por tratarse del concepto de *fair use* o "uso justo".

► **Monitoreo de servicios P2P y la privacidad.**
¿Es válido monitorear las actividades de los usuarios en Internet para saber si se están vulnerando los derechos de autor a través de intercambio de material sin autorización? Aquello, que podría parecer exagerado, es un hecho que ocurre. Por ejemplo, se sabe que la red BitTorrent es monitoreada por distintas compañías dedicadas a la protección de contenidos con *copyright* (como Peer Media Technologies), que recolectan información de los usuarios para luego iniciar acciones legales. Estas empresas no revelan sus métodos de trabajo, pero un estudio publicado por investigadores de la Universidad de Birmingham muestra que los usuarios que comparten contenido ilegal pueden ser detectados en apenas tres horas.[62] Con todo, hay diferentes posiciones sobre esta actividad.

En el 2005, la agencia francesa de protección de datos decidió autorizar a las compañías discográficas el monitoreo de Internet para localizar intercambios de ficheros P2P; en contraste, está Italia, donde su autoridad para la protección de la privacidad consideró que estos procedimientos de monitoreo son ilegales, ya que la directiva europea sobre telecomunicaciones prohíbe a las compañías privadas efectuar controles masivos de datos.

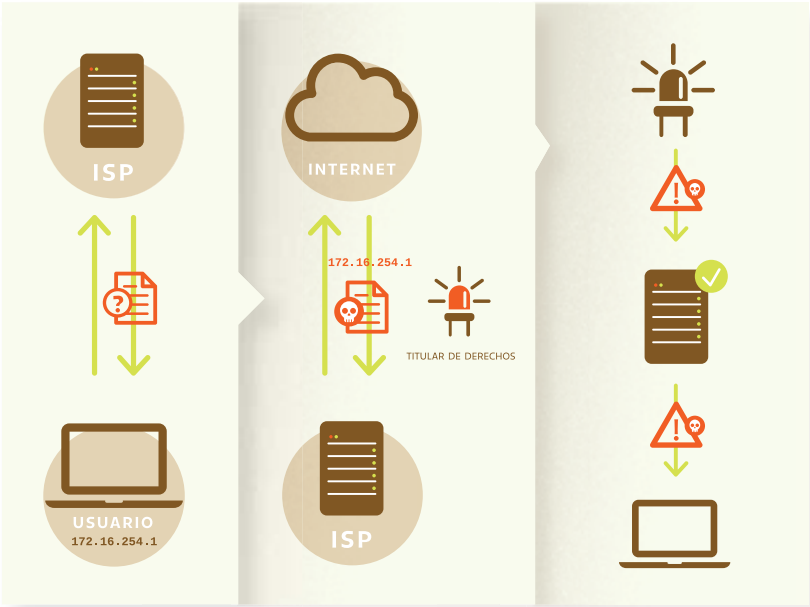
▸ **Responsabilidad legal de ISPs.**
Debido a la posición de intermediarios que tienen los proveedores de Internet entre los usuarios y la red, parte importante de la discusión se ha concentrado en la responsabilidad que tienen en la "piratería" *online*. Por un lado, está la posición que considera que los ISPs "contribuyen" de alguna manera a las infracciones que se cometen en Internet y, por lo tanto, podrían ser declarados responsables por las infracciones cometidas por sus clientes y usuarios. En este caso, se considera que los ISPs actúan como editores. Por otro lado, hay quienes creen que los ISPs son meros prestadores de equipos para la transmisión de información, por lo que no le cabría tener ninguna responsabilidad por lo que han hecho los usuarios.

En el caso chileno,[63] el capítulo sobre "Limitación de responsabilidad de los prestadores de servicios de Internet" de la Ley sobre Propiedad Intelectual chilena, establece exenciones de responsabilidad a los ISPs, cumpliendo lo comprometido en el Tratado de Libre Comercio entre Chile y los Estados Unidos. Conforme a dicho tratado, las partes se obligaron a proveer incentivos legales para la cooperación entre proveedores de servicios y titulares de derechos de autor, además de limitaciones a la responsabilidad de aquellos. Desde el tratado en cuestión, se fija un procedimiento de notificación y bajada de contenidos, relativo al retiro y bloqueo de los servicios de almacenamiento y de búsqueda y enlace, creando la obligatoriedad para ambas partes de establecer legalmente tal procedimiento, que involucre la "notificación efectiva" del material infractor al respectivo responsable del prestador de servicios. Es importante destacar que si bien establece la posibilidad de bajar ciertos contenidos, para la ley esta bajada debe ser efectiva siempre previa emisión de una orden judicial.

62 The Unbearable Lightness of Monitoring: Direct Monitoring in BitTorrent. De Tom Chothia, Marco Cova, Chris Novakovic, and Camilo González Toro. School of Computer Science, University of Birmingham, UK. En http://www.cs.bham.ac.uk

63 Responsabilidad de los proveedores de servicios de Internet (ISPs) en relación con el ejercicio del derecho a la libertad de expresión en Latinoamérica, por Claudio Ruiz Gallardo y Juan Carlos Lara Gálvez. De Hacia una Internet libre de censura Propuestas para América Latina. En http://www.palermo.edu/cele

¿Cómo se notifica a un usuario de un comportamiento "pirata" en Chile?



El usuario se conecta a Internet a través de un ISP (proveedor de servicios de Internet).

Puede que el usuario baje un material sin autirización de los derechos de autor (video, fotografía, MP3, etc.)

El titular de los derechos de autor o su representante, detecta el comportamiento ilicito del usuario. (generalmente por su IP).

Importante: Esta detección debe hacerse por vías legales.

El titular de los derechos o su representante, debe notificar al ISP. La ley de propiedad intelectual dispone que la información debe ser específica (85U).

Si procede el ISP debe notificar al usuario con todos los antecedentes.

c) ¿Quiénes son los protagonistas de este nodo?

▸ **Titulares de los derechos de autor.**

En este nodo, pocas veces hablamos del autor de una obra y muchas veces de los titulares de derechos de autor. Ambas, son figuras diferentes que a veces, solo a veces, coinciden en ser la misma persona. El autor, al crear una obra, es el dueño de los derechos patrimoniales, es decir, de aquellos que permiten el

provecho económico mediante la explotación de la obra. El autor puede hacer cualquiera de tales usos personalmente o ceder tales derechos para que los ejerza otra persona o institución, es decir, el titular de los derechos. En esta discusión, generalmente, los titulares de derechos de una obra son las grandes compañías, como las discográficas, productoras, editoriales, etcétera.

▸ **Entidades colectivas de gestión de derechos de autor**.
Que un autor pueda gestionar sus derechos sobre una obra puede ser casi imposible. Por eso nacen las entidades colectivas de gestión de derechos de autor, que pueden actuar en su nombre. Ellas, en primer término, pueden recaudar y distribuir la remuneración obtenida por la explotación de la obra, así como impedir y detectar infracciones de derechos y solicitar medidas para su compensación, etcétera. En un solo país se pueden encontrar diversas entidades agrupadas según tipo de obras (audiovisuales, por ejemplo).

¿Cuáles son las entidades colectivas de gestión de derechos de autor que más han batallado contra la "piratería" *online*?

Indudablemente, la más polémica en Hispanoamérica es la SGAE (Sociedad General de Autores y Editores) de España. Con una enorme influencia en los distintos gobiernos de ese país, han podido llevar adelante iniciativas como el "canon digital" (pagar tasa aplicada a diversos medios de grabación como compensación por las supuestas copias que se podrían hacer) o restrictivas leyes como la ley Sinde (que faculta a departamentos dependientes del Ministerio de Cultura el poder de cerrar sitios web que vulneren los derechos propiedad intelectual, previa autorización de los Juzgados). Su historia además ha estado recientemente cruzada por problemas de corrupción (una decena de sus miembros están involucrados en fraude administrativo y apropiación indebida) que ha tendido un manto de duda sobre la administración de los recursos que la organización maneja.

En Colombia, existe SAYCO (Sociedad de Autores y Compositores de Colombia) que es el organismo de ese tipo más grande de ese país.

A finales de 2011 se destaparon denuncias de empresarios musicales que acusaban la informalidad y los montos exagerados en los cobros de SAYCO para autorizar la realización de conciertos. Tanto así, que intervino el gobierno y obligó a reestructurar la administración de la entidad. Con todo, para muchos "aún es temprano para determinar si efectivamente SAYCO es la entidad idónea para proteger los intereses de los autores y compositores colombianos"[63].

En Chile, probablemente la entidad más conocida es la SCD (Sociedad Chilena del Derecho de Autor), que no ha tenido una gran incidencia en la agenda legislativa sobre el entorno digital, salvo en la discusión de la nueva ley de propiedad intelectual, que fue aprobada el 2010.

▸ **Público (usuarios de Internet).**
El público, en este caso, los usuarios de Internet, pocas veces son nombrados en esta discusión, a pesar del tremendo peso que tienen. Criminalizados la mayoría de las veces, poco se habla del derecho otorgado en el sistema de la propiedad intelectual de acceso a las obras. Aunque insuficientes, parte importante de esos derechos están consagrados en las excepciones y limitaciones del derecho de autor ("usos justos"), que la mayoría de las legislaciones del mundo incluyen en diversa medida.

▸ **IFPI Chile: Asociación de Productores Fonográficos.**
Es una asociación gremial global que en Chile busca también proteger las actividades destinadas a la producción y publicación de fonogramas y videogramas. Una de sus actividades reconocidas es "luchar contra la piratería" y cada cierto tiempo liberan campañas "educacionales" al respecto.[65]

64 ¿Y qué pasó con SAYCO? de Karen Cabrera en Open Business Latin America & Caribbean.

► **RIAA: Asociación de Industria Discográfica de Estados Unidos.**
Es una asociación estadounidense en que sus miembros son las compañías disqueras y los distribuidores discográficos más grandes de ese país. Entre una de sus tareas, está la de proteger los derechos de propiedad intelectual de sus asociados. Debido a su poderosa conformación, la RIAA tiene mucha influencia no solo a nivel de políticas públicas, sino también desde hace muchos años ha iniciado la judicialización de la persecución de la "piratería" *online*. Así, por ejemplo, llevó adelante la demanda contra una compañía como Napster, y con la misma fuerza ha demandado a usuarios de Internet, como Joel Tenenbaum, que tuvo que pagarles U$ 675.000 por bajar canciones a su computadora.

► **USTR: Oficina del Representante Comercial de Estados Unidos.**
Agencia del gobierno de Estados Unidos responsable del desarrollo de la política de tratados económicos de ese país. Tiene gran influencia en la discusión del derecho de autor en el contexto *online*, porque representa los poderosos intereses de industrias culturales y farmacéuticas de ese país. Su influencia la ejerce no solo en las negociaciones económicas con distintos países (los famosos capítulos de propiedad intelectual), sino que también a través de distintos instrumentos, como el **informe "Especial 301"**.[66]

► **IIPA: Alianza Internacional de la Propiedad Intelectual.**
Es una alianza de siete asociaciones que representan los productores estadounidenses de contenido y materiales protegidos por las leyes de propiedad intelectual, miembros tan diversos como la "Independent Film & Television Alliance" a la "Business Software Alliance". Junto con el USTR, cada año realiza e**l informe "Especial 301"**.

65 Ver por ejemplo "Agrupación de sellos envía "advertencias" a quienes descargan música pirata en Chile" en El Mercurio, 29 de julio del 2013, en http://www.emol.com/

66 Se publican comentarios al Informe 301 sobre propiedad intelectual. 15 de febrero del 2013. En http://www.derechosdigitales.org/

¿Qué es el informe "Especial 301" y cómo afecta a Chile?

Si estás relacionado con los temas que hemos hablado hasta acá, seguramente conoces el informe "Especial 301", que año tras año emite la USTR junto con la IIPA. En él, se destacan los logros alcanzados y problemas relativos a la idoneidad y eficacia de la protección y observancia de los derechos de propiedad intelectual por parte de los países que comercian con Estados Unidos. Entre ellos, claro, Chile.

El informe se basa en un ranking que cada año se renueva y que pone en una "lista roja" a los países que, según esta agencia de gobierno de Estados Unidos, no cumplen con sus estándares de protección a la propiedad intelectual, sin distinguir entre piratería tradicional y "piratería" en Internet.

Aunque este informe es presentado como el resultado inapelable de una metodología comprobada y objetiva, son muchas las organizaciones, centros de investigación y académicos del mundo que han presentado dudas sobre este informe. Dos son los grandes reparos:

1) El informe "Especial 301" solo representa los intereses económicos de la industria de Estados Unidos.

2) El informe "Especial 301" solo considera una perspectiva del sistema de propiedad intelectual (PI) desde la protección de los derechos de autor, y no considera el acceso al conocimiento y la cultura, que es parte fundamental de un sistema balanceado de PI.

Así, por ejemplo, el año 2010, el programa sobre "Información, justicia y propiedad intelectual" de la American University de Estados Unidos, realizó un reporte especial de este informe, y renqueó a los países considerando el acceso a la cultura y el conocimiento. Los resultados fueron diametralmente opuestos al informe "Especial 301".

En Chile, cada vez que este informe se hace público a través de la prensa, ONG Derechos Digitales insiste no solo en los reparos del informe, sino también sostiene que Chile no tiene razón alguna para aparecer en la lista roja del al informe "Especial 301". El año 2013, el gobierno chileno concluyó lo mismo y, a través de un comunicado de prensa, declaró:

"La 'Lista 301' carece de criterios claros para catalogar a los distintos países, sino que es más bien un reflejo de los intereses de la industria norteamericana de aplicar selectivamente sus estándares de propiedad intelectual a otros países".

¿Cuáles han sido las iniciativas legales más importantes?

► **DMCA: Acta de Derechos de Autor Digitales del Milenio.**
Es la polémica ley de derechos de autor de Estados Unidos, nacida para defender a las industrias de contenidos frente a la "piratería" *online*, y que está vigente desde 1998. Así, regula y sanciona la reproducción de derechos sin autorización, incluyendo la responsabilidad civil de los ISPs,[67] pero también sanciona la creación y distribución de cualquier dispositivo o programa que invalide una protección software o hardware (DRM), e incluso también cualquier estudio o análisis que demuestre vulnerabilidades en algún sistema. Lo interesante (o preocupante, dependiendo del punto de vista) es que Estados Unidos siempre busca exportar el DMCA a través de sus tratados comerciales internacionales, incluido el Acuerdo Estratégico Trans-Pacífico de Cooperación Económica (TPP) donde Chile está involucrado.

► ***Three Strikes:* "Respuesta Gradual".**
Se denomina así a este sistema como un guiño a los tres intentos fallidos de batear una pelota de béisbol, tras lo cual el bateador es expulsado del campo de juego. Es la desconexión de un usuario de Internet por reiteradas infracciones a los derechos de autor. La sanción se produce cuando al usuario se le ha notificado previamente en dos ocasiones que su cuenta de acceso a Internet ha sido sorprendida infringiendo derechos de autor. Este sistema de legislación está en países como Inglaterra, Nueva Zelanda, Taiwán y Corea del Sur;[68] por su parte, en el año 2013, y por decreto del Ministerio de Cultura francés, se puso fin a la ley Hadopi de ese país y que contemplaba este mecanismo, debido a sus altos costos y poca eficacia.

► **ACTA: Acuerdo Comercial Anti-Falsificación.**
Es un acuerdo multilateral voluntario, aún en negociación, que busca crear un marco legal para la protección de los derechos de propiedad intelectual en todo el mundo. Parte importante del rechazo al ACTA se debe a sus cláusulas donde se pueden llegar a bajar sitios web de Internet y obliga a los ISPs, bajo amenaza de cargos penales, a intervenir las comunicaciones de sus usuarios si se sospecha que alguno está enviando o recibiendo material protegido por derechos de autor. Todo

67 Responsabilidad de los ISPs por violación a la propiedad intelectual: Estados Unidos, Europa y Chile. Por Lorena Piñeiro en Revista Chilena de Derecho Informático. En http://www.derechoinformatico.uchile.cl

68 Respuesta gradual y debido proceso. Por Alberto Cerda. Octubre 2012. En http://www.derechoshumanoseninternet.org

esto sería una amenaza a la libertad de expresión y un atentado a la privacidad de los ciudadanos. En el 2012, por ejemplo, la Comisión Europea rechazó de forma definitiva el ACTA.[69]

► **SOPA: Detención de los Actos de Piratería en Línea**
Polémico proyecto de ley en Estados Unidos presentado el 2011, que buscaba combatir la "piratería" y la "falsificación" en Internet, imponiendo obligaciones adicionales a los intermediarios de Internet. Dirigida especialmente a proveedores de servicios, pretendía que el Fiscal Nacional solicitara órdenes judiciales para adoptar diversas medidas contra los sitios en que se infringieran derechos de autor, a fin de que cesaran esa infracción, o bien para impedir el acceso a ellos desde los Estados Unidos. Conforme al proyecto, una vez notificados de las resoluciones judiciales, los intermediarios de Internet debían bloquear el acceso al nombre de dominio infractor. Asimismo, autorizaba a los titulares de derechos de autor y derechos conexos para solicitar a los proveedores de servicios de pago y de publicidad, que cesaran sus servicios a las páginas dedicadas al "robo de propiedad estadounidense", inhabilitando así su sustentabilidad en tanto sitios completos, por algo tan pequeño como una única infracción.

► **TPP: Acuerdo Estratégico Trans-Pacífico de Cooperación Económica.**
Es un tratado de libre comercio multilateral, que involucra a 12 naciones: Estados Unidos, Japón, Australia, Nueva Zelanda, Malasia, Brunei, Singapur, Vietnam, Canadá, y los latinoamericanos México, Perú y Chile. La negociación del TPP es secreta, pero la filtración de su capítulo de propiedad intelectual permitió saber que el tratado busca convertir a los proveedores de acceso a Internet en los responsables de censurar contenidos unilateralmente, sin intervención de un organismo superior, como el poder judicial, que garantice nuestros derechos. Además, quiere endurecer las sanciones a las infracciones del derecho de autor, penalizándola con multas, desconexión de Internet y hasta cárcel.[71]

A continuación, un cuadro comparativo de algunas de estas iniciativas, hecho por Carlos Furche, presentado en el documento "Chile y las negociaciones del TPP: Análisis del impacto económico y político"[72].

69 El TPP e Internet, o cómo darle SOPA a todo el mundo. Por Juan Carlos Lara. 20 de junio del 2013. En http://www.derechosdigitales.org

71 Más información en tppabierto.net

72 El documento se encuentra en http://www.derechosdigitales.org/publicaciones/

RESUMEN COMPARATIVO DE PROPUESTAS

	PIPA	SOPA	TPP
Pone en riesgo las plataformas y comunidades en línea	√	√	√
Utiliza una definición excesiva de "piratería" que incluye sitios web y servicios que tú usas para almacenar, compartir y enlazar (a medios de comunicación).	√	√	√
Amenaza a una gran cantidad de servicios en línea legales e innovadores, como Twitter, Facebook y Youtube.		√	√
Establece un mal ejemplo para la censura de Internet a nivel global.	√	√	√
Usa las mismas herramientas técnicas que otros gobiernos – como China– ocupan para suprimir la libertad de expresión y a los disidentes.	√	√	?
Establece un ejemplo para otros países para bloquear cualquier tipo de contenido en línea desfavorable, lo que puede llevar a violaciones a los derechos humanos.	√	√	√
Quiebra la estructura de Internet.	√	√	?
Amenaza la seguridad en línea.	√	√	?
Permite requerimientos de EE. UU. a los proveedores de nombres de dominio (DNS) para bloquear que un usuario llegue un sitio web específico.	√	√	?
Interfiere con los esfuerzos en curso para mejorar la seguridad en línea, lo que hace más vulnerable a los usuarios a robos de identidad y otros tipos de seguridad informática.	√	√	?
Expone a los que tratan de evitar bloqueos de DNS a virus. Estos computadores infectados pueden ser secuestrados para su uso en ataques informáticos a otros sistemas, poniendo al país en mayor riesgo de ciberataques.	√	√	?

*SIN INFORMACIÓN = ?

d) Cinco principios para la cobertura de derechos de autor en Internet

Ya sea por la publicación de cifras sobre "piratería" *online*, por una aplicación o software que es obligado a cerrar o cambiar su modelo de negocio, por una nueva ley o por protestas virtuales en todo el mundo, los derechos de autor en la red son, indudablemente, uno de los temas más activos desde el punto de vista periodístico.

A continuación, te presentamos cinco principios que pueden ser de ayuda al momento de una cobertura periodística más completa de estos temas.

► **Casi nunca hay consensos sobre temas de derechos de autor e Internet.**
Como lo vimos en los matices de la discusión de este capítulo, efectivamente, el tema sobre derechos de autor en la red es un tema que está lejos de conciliar posiciones y, quizás por eso, seguirá siendo un tema polémico. Lo cierto es que en cada una de las noticias donde los derechos de autor estén involucrados, no será difícil encontrar una posición opositora, siendo casi siempre seguro que a fuentes que piden mayor protección de la propiedad intelectual, habrá otros que busquen más acceso a las obras.

► **El derecho de autor también se trata de acceso a la cultura.**
Como se desprende de lo anterior, este es uno de los principios fundamentales con las que un periodista debe cubrir asuntos de derechos de autor en general, pero sobre todo en Internet, en particular. El sistema de propiedad intelectual ha sido concebido como un sistema balanceado, donde si bien, por un lado, se busca proteger de manera justa al autor creador de una obra; por otro, también se debe conciliar el acceso de parte del público a esa obra. En definitiva, cuando se habla de derechos de autor, también, aparejado, se debe indagar sobre los derechos del público involucrados.

► **El autor no es necesariamente el que obtiene los beneficios.**
Hay que distinguir muy bien entre dos figuras que no necesariamente son la misma persona: el autor de una obra y el titular de sus derechos. El primero, al crear la obra, es el autor y el titular de sus derechos; pero puede que traspase esos derechos patrimoniales (no los morales) a un tercero, como por ejemplo, una compañía discográfica, cinematográfica, editorial, etcétera. De esta forma, las ganancias por esa obra durante la vigencia de los derechos de autor, van a ese titular de los derechos y no al autor. Esta distinción es especialmente importante al momento de distinguir quiénes reclaman por la "piratería" *online* y, por ende, se hace fundamental saber quiénes son los titulares de una obra.

► **¿Quién es la fuente de los estudios de piratería *online*?**

Las cifras sobre "piratería" en Internet abundan. Cada año salen decenas de estudios e informes nuevos respecto a este tema, pero algunos, claro, tienen más cobertura que otros. ¿Pero sabemos con seguridad que esas cifras son obtenidas de manera objetiva? Si bien es muy difícil tener acceso a la metodología de estos estudios, algo menos difícil es saber la fuente de esos datos. Cuando los datos de un estudio vienen de la industria afectada, es muy probable que el informe aliente los intereses de las empresas y desestime cualquier otra. Por eso, antes de dar por cierta una conclusión de un estudio, hay que sopesar la fuente y matizar los resultados. Tal como vimos antes en esta guía, con en el informe "Especial 301" o en "Las cifras de piratería *online* ¿son creíbles?".

► **¿Es justa la criminalización de los usuarios?**

Parte importante de las corrientes proteccionistas de los derechos de autor en Internet, buscan criminalizar a los usuarios. Ya sea por leyes, por cierre de programas o por simples discursos públicos, se busca aplicar todo el peso de la ley sobre personas que muchas veces solo están ejerciendo usos justos de una obra y que no tienen intención de perjudicar al autor en sus actos. Asimismo, y en este camino de ignorar que la propiedad intelectual también se trata de acceso al conocimiento y la cultura, la criminalización de los usuarios implica la desestimación de otros derechos fundamentales que son aún más importantes que la protección de intereses de una industria en particular, como la libertad de expresión. Así, cada vez que se publica una noticia sobre "piratería" *online*, siempre es importante saber en qué formas se criminaliza al usuario, si eso es justo y cuáles son las implicancias para los demás ciudadanos.

con el apoyo de

ONG DERECHOS DIGITALES

Internews
Local voices. Global change.