22/04/16

NOTA DE FUTURO 7/ 2016

FRAGMENTACIÓN DE INTERNET

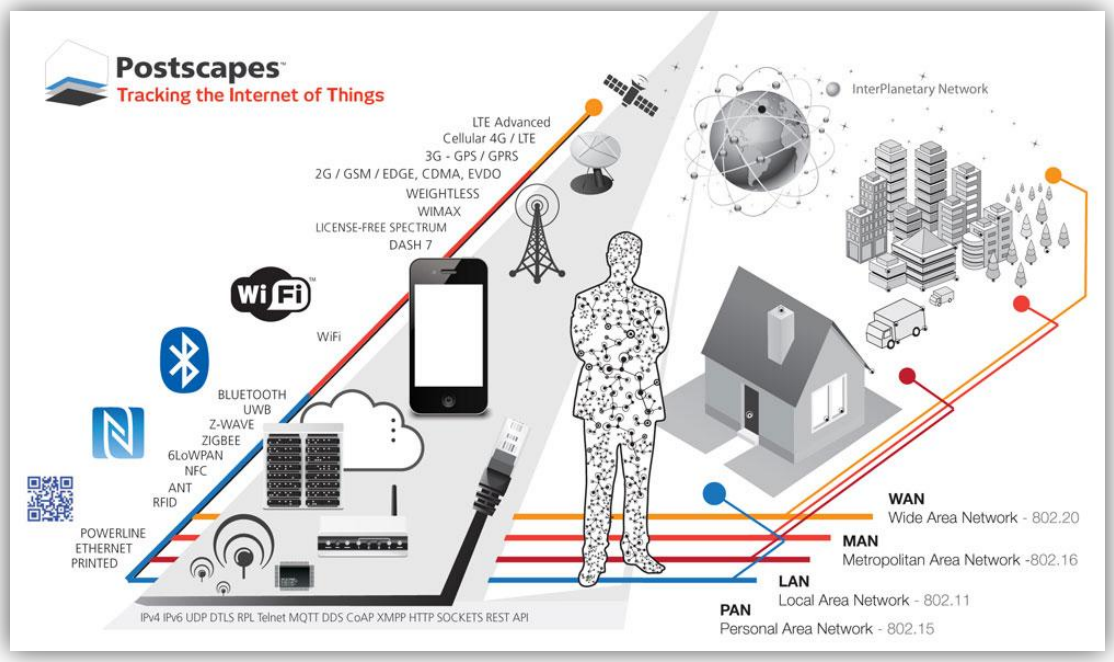
CENTRO DE ANÁLISIS Y PROSPECTIVA
GABINETE TÉCNICO DE LA GUARDIA CIVIL

La fragmentación de internet

El presente texto es una síntesis del documento disponible en:

http://www.weforum.org/reports/internet-fragmentation-an-overview
http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

Desde que Edward Snowden filtró información confidencial, el uso de internet, los datos que allí se encuentran y su uso se ha convertido en tema de preocupación global. El impacto de actividades paralelas en Internet y, por tanto, su fragmentación ha sido objeto de discusiones tanto de los expertos en la materia, como de los usuarios y de la comunidad empresarial.



Primeramente, para abordar la fragmentación es necesario ser consciente de que el problema debe ser afrontado por todos los interesados en un acto de cooperación masiva, ya que las regulaciones legales por parte de los gobiernos no son suficientes. Y acometer esta problemática es importante ya que, de lo contrario, todos los avances que Internet ha proporcionado a la sociedad podrían cambiar de tendencia si se hace un uso torticero de esta herramienta.

Hoy en día se puede afirmar que no existe un consenso sobre los distintos términos surgidos como consecuencia de la creación del ciberespacio.

Para comenzar: ¿Qué factores constituyen la definición de “Internet no fragmentado”? Los factores básicos incluyen el intercambio de paquetes de datos entre dispositivos habilitados para la tarea, enmarcado en un entorno de conectividad universal e interoperativa, en la que una acción tiene un efecto concreto sin importar la localización o el proveedor. Esto se consigue con unos estándares técnicos y protocolarios comunes. Por lo tanto, toda acción o condición que perjudique el funcionamiento eficiente de Internet descrito constituye una fragmentación técnica. La fragmentación comprende toda aparición de distintas presiones en el entorno de la red que conlleven distintos resultados que no sean coherentes y consistentes.

Esta primera definición resulta bastante restrictiva y limitada, ya que no tiene en cuenta cómo se usa Internet ni las fuerzas políticas y económicas que intervienen. Es por esto que sería más apropiado denominarlo Internet de acceso público en vez de no-fragmentado. El acceso público implicaría: alcance mundial, integridad, objetivos generales (sin limitaciones de uso en ningún área específica), apoyo de la innovación sin necesitar permiso, accesibilidad, interoperabilidad y consentimiento mutuo, colaboración, tecnología y sin distinciones entre competidores ni favoritismos. Teniendo en cuenta los factores anteriores, la fragmentación constituiría cualquier situación que no los cumpliera.

Estructura de internet:

- **Aplicaciones:** Es aquí donde reside la utilidad de los protocolos como HTTP (Protocolo de transferencia de hipertexto), SMTP...
- **Transporte:** Abarca los protocolos para cada transferencia de datos a tiempo real (TCP, UDP...)
- **Red:** La IP (protocolo de Internet) lleva paquetes de datos del origen al destino siguiendo unos protocolos.
- **Hardware/ Físico** (Ethernet o Wifi): Compuesto de circuitos de telecomunicaciones ópticas o conexiones por satélite.

Como añadido, también se puede contar con otra sección de transacciones y contenido que resulta útil para estudiar la información transferida junto con las interacciones y el comportamiento de las trasferencias.

Para complementar la explicación del funcionamiento de internet, un grupo de trabajo de las Naciones Unidas definió el término de gobernanza de Internet como el desarrollo y la aplicación de principios compartidos, normas, reglas, procedimientos de decisión y programas que dan forma a la evolución y uso de Internet por parte de los gobiernos, el sector privado y la sociedad civil en sus respectivos roles.

Antes de abordar los tipos de fragmentos hay que tener en cuenta una serie de factores que pueden motivar y dar forma a cada fragmentación. En este caso se desarrollan los cuatro más importantes: aparición, intencionalidad, impacto y carácter.

Aunque los factores son muy generales, sí que engloban el carácter de la mayoría de las posibles fragmentaciones. Además, el informe argumenta de manos de Eli Noam que la fragmentación no es necesariamente algo malo, se propone un internet público y otro privado para que ambos se complementen en pro de la sociedad. De todas maneras, no se debe olvidar que la fragmentación puede que sea una consecuencia inevitable por lo que no está en nuestras manos evitar o fomentar la fragmentación.

Una vez que se entiende el funcionamiento, la infraestructura y los factores modificadores de internet se puede proceder a explicar las distintas formas de fragmentación.

La primera es la fragmentación técnica, que afecta a las cuatro partes mencionadas anteriormente, impidiendo que el intercambio de los paquetes de datos sea global e interoperativa. La segunda es la fragmentación gubernamental, que engloba las acciones del gobierno para restringir el uso de internet, lo que afectaría a esa parte adicional de

transacciones y contenido. La tercera forma de fragmentación es la comercial, similar a la gubernamental pero ejercida por la comunidad empresarial a nivel privado.

Los tipos de fragmentación mencionados no son los únicos pero si los más importantes. También puede haber fragmentaciones de tipo cultural, idiomático o social.

Fragmentación técnica

La fragmentación técnica es un proceso técnico y evolutivo que se ha ido desplegando lentamente pero que ha ido dejando lagunas a su paso. Tanto no intencionada como intencionadamente, esta fragmentación ha seguido cuatro tendencias principales: direccionamiento, interconexión, nombramiento y seguridad.

Direccionamiento: Las direcciones de IP son las que identifican cada punto de la red de conexión que conforma Internet, dichas IP tienen 32bits, lo que posibilita más de 4.000 millones de combinaciones y, por lo tanto, direcciones IP. De la coordinación de las direcciones se encarga la IANA (Autoridad de Asignación de Números de Internet) administrada por el gobierno de Estados Unidos aunque hoy por hoy se está intentando desvincular al gobierno estadounidense de la institución-. Sin embargo, nos estamos quedando sin direcciones IP, por lo que se ha creado el Network Address Translation (Traducción de Dirección de Red), por el que se crean miniredes de IP privadas vinculadas a una IP pública (una de las más de 4.000 millones existentes). Un ejemplo sería un router con dirección pública que asigna IP privadas a los ordenadores que dependen de su conexión. Este sistema sí resuelve el problema de la escasez de direcciones IP pero a la vez fragmenta Internet entre IPs públicas y privadas. Existe una alternativa que es cambiar del sistema de direccionamiento actual IPv4 al IPv6 (128bits) y actualmente se está introduciendo en los nuevos dispositivos para usarlo en un futuro, cuando todos los terminales estén habilitados para usar la IPv6.El problema es que la convivencia de los dos sistemas puede hacer que en vez de pasar del IPv4 al IPv6, el traspaso nunca llegue y se usen los dos al mismo tiempo, lo que supondría una fragmentación, ya que ambos son incompatibles.

Interconexión de la red de redes: Como hay redes privadas y públicas, tiene que haber “puentes” entre dichas redes y esos “puentes” son, por ejemplo, los routers que transforman las IP privadas en una IP pública junto con un nº de puerto. Todo este sistema se rige por el Border Gateway Protocol, un protocolo que hasta ahora ha funcionado pero que se sabe que puede ser corrompido y se puede desviar el tráfico hacia lo que se llaman “agujeros negros” o hacia vías que permitan la vigilancia de información. Además, los paquetes de datos pueden ser transportados por otros usuarios que estén enviando paquetes de datos, lo que complica más aún el sistema. Desde que el sector empresarial comenzó a usar Internet en su negocio, las direcciones

IP son un bien preciado para llegar a sus clientes por lo que el hecho de haber IPs públicas y privadas no ha resultado una mala solución. Además, para que IPs públicas no manden paquetes de datos que no queremos, existen firewalls que filtran los paquetes de datos que provienen de la red de IPs públicas. Sin embargo, los firewalls no son suficientes, se requiere de métodos de encriptación y autenticación. En este sector de microredes privadas existen las VPNs, que son redes privadas (normalmente usadas por grupos empresariales para custodiar su información) que mediante uno de esos "puentes", anteriormente mencionados, conecta con las IPs públicas. La red TOR, creada por la US Naval Research Laboratory, es una red que encripta la información para que solo pueda ser descifrada por el emisor y el receptor del paquete de datos y es comúnmente utilizada por activistas de derechos humanos y por usuarios que llevan a cabo actividades ilegales, ya que este sistema, que funciona como una VPN, evita la vigilancia gubernamental.

Sistema de nombres de dominio: Cada dirección de IP usa un nombre llamado dominio, entonces, cada vez que queremos enviar un paquete de datos, primero tenemos que averiguar la IP del dominio que tenemos; para ello, nuestro servidor de dominios local pregunta al resto de servidores dónde encontrar la información hasta que al final los servidores a los que pregunta le indican la IP del servidor que aloja la IP del dominio que busca para finalmente acceder a la información que el usuario necesita. Este sistema por el cual los servidores se van preguntando por la dirección IP de un dominio, por ejemplo Facebook.com, se llama Sistema de Nombre de Dominios y es una organización jerárquica en la que se registran las IPs de cada dominio, a modo de agenda telefónica. Los servidores se especializan por capas, unos en .com y dentro del grupo unos en la palabra "facebook" hasta que se encuentra la IP buscada. Al principio solo había 13 servidores raíz.

Seguridad: La información se encripta a través de llaves simétricas o públicas o una combinación de las dos. La encriptación es fundamental para mantener la información privada ya que de lo contrario, cualquier usuario podría descifrar la información. En términos generales, está habiendo una tendencia global a la encriptación end-to-end para asegurar la confidencialidad e integridad de la información que se intercambia en Internet y al uso de certificados y firmas digitales para autenticar a los usuarios y la información que se intercambia. Esto limita la vigilancia y la inspección de los paquetes de datos privados.

Fragmentación Gubernamental

Internets nacionales, se bloquearía la información. Aunque existen presiones para que esto ocurra hay más presiones para que no pase. Este posible escenario facilitaría la implementación de leyes. En general cada vez hay más formas de fragmentación gubernamental.

Soberanía nacional y Cyberespacio: Los gobiernos siempre han querido controlar el flujo de actividades entre fronteras y, con Internet, la tendencia no es distinta y, aunque algunos gobiernos crean que la poca legislación sobre Internet es lo que lo ha hecho crecer con tanta rapidez, otros proponen regulaciones amigables con los mercados decididas entre muchos actores interesados. A pesar de la emoción de principios de siglo de tener un mundo paralelo con una sola economía y sin fronteras, los servidores que usamos para almacenar la información pertenecen a naciones con leyes que regulan sus actividades. Es en esta época donde se creó el Foro de Gobernanza de Internet, donde cada país expone su visión sobre la gobernanza de Internet.

Contenido y censura: Teniendo en cuenta la Declaración Universal de los Derechos Humanos, toda persona tiene derecho a buscar, recibir e impartir información e ideas sin importar las fronteras o el canal. Sin embargo, la Constitución del ITU da a los Estados la posibilidad de inhabilitar, según su legislación nacional, toda telecomunicación privada que pueda parecer peligrosa para la seguridad del Estado o contraria a su legislación, al orden público o a la decencia. Primero se vigilaba la información a través del control de los dominios y los servidores a través de software que actuaba como filtro. Una segunda generación de técnicas de control se dedicó a legislar las medidas anteriormente mencionadas y a crear protocolos de actuación. En tercer lugar, la táctica actual para controlar la información se basa en competir con contra-información para desmoralizar y desmotivar al atacante, todo esto acompañado de vigilancia y extracción de datos.

Comercio electrónico: Las posibilidades del comercio electrónico son innumerables y está demostrado que, cuanta más apertura a este tipo de comercio tiene un país, más se enriquece. Pero la presencia casi omnipotente de los productos estadounidenses ha llevado a muchos países a ejercer un proteccionismo en Internet para compensar dicha hegemonía. El comercio electrónico no solo afecta al número de ventas de una compañía, también lo hace a los impuestos (IVA) y a los derechos de los ciudadanos, entre otros aspectos. Los foros internacionales tratan el tema y hacen que los distintos interesados negocien sus condiciones y se mantenga el libre mercado en la red. Es obvio que esta dicotomía puede presentar fragmentaciones en el futuro.

Seguridad nacional, privacidad y protección de datos: Este aspecto se tuvo en cuenta con relación a Internet tras el atentado del 11 de Septiembre de 2001. Esta nueva tendencia se plasmó en un acuerdo en la Convención sobre cibercrimen celebrada en Budapest en 2001, que entró en vigor en 2004. El siguiente paso fue crear estrategias de ciberseguridad nacional para prevenir el ciberespionaje, tanto ofensivo como defensivo. Después, el uso de Internet para la organización de la primavera árabe de 2010 dio muestras de la efectividad del www para poner en jaque la seguridad nacional. El golpe de gracia lo dio Snowden. Es por esto que cada país tiene su propia política y no parece que una estrategia global sea posible ya que la restricción de cada estado varía.

Localización de información: Se han de tener en cuenta cinco aspectos: restricciones de procesamiento, de almacenamiento, de estructura de la red, de organizaciones y de movimiento transnacional. Esta política restringe los flujos de información y condiciona la localización de la información, según los intereses de la compañía o el país interesados. Y como ha ocurrido en los casos anteriores, los gobiernos no han tenido a bien ponerse de acuerdo con la estrategia.

Cibersoberanía: Existen dos visiones diferenciadas con respecto a la soberanía de Internet, como en el resto de aspectos mencionados, al igual que existe un foro internacional dirigido por Naciones Unidas para cohesionar las políticas en materia de Internet. Algunos expertos en la materia afirman que la fragmentación irá a más y, por tanto, habrá una tendencia clara hacia la soberanía cibernética que impedirá el flujo de las comunicaciones. Se podría afirmar que los netizens (ciudadanos de Internet) y la idea de Internet como una gran nación cohesionada es una utopía en manos de los países.

Fragmentación Comercial

No solo los gobiernos interfieren con sus intereses en la idea de un Internet abierto y sin fronteras, también algunas compañías contribuyen a la fragmentación con su proteccionismo.

Colaboración y estandarización: La naturaleza competitiva de los mercados impide que las compañías se unan para moldear las condiciones a su medida y promover un mercado más justo. Es cierto que existen unos protocolos y estándares que buscan regularizar e igualar las condiciones competitivas de las compañías, pero en ocasiones resultan contraproducentes y terminan por fomentar la fragmentación.

Neutralidad de la red: Con la multitud de actores que afectan tanto a Internet como al comercio, es muy complicado afirmar que la red puede ser neutral. En el comercio en la red no se puede alegar que exista una neutralidad ya que, para empezar, hay usuarios que no pueden llegar a ciertos proveedores y viceversa. No existe una igualdad de condiciones básica para que se califique al comercio en Internet de neutral, existe una fragmentación desde la base.

Jardines cercados: Este concepto se refiere a las aplicaciones y páginas web en las que te inscribes y puedes relacionarte con gente que también pertenece a esa aplicación. Esto tiene ciertas ventajas, ya que se crea un entorno seguro donde personas afines se comunican, pero también se discrimina a todas aquellas que no puedan o quieran pertenecer a estos jardines. El mejor ejemplo es Facebook o Twitter, ya que si no se está en él podemos quedar excluidos, incluso fuera del mundo ciber. Esta es una fragmentación clara porque discrimina.

Geo-localización y Geo-bloqueo: Este aspecto a tener en cuenta está estrechamente relacionado con las legislaciones de cada país, ya que dependiendo de esta se bloquea el acceso a ciertos servicios. Lo que presenta una fragmentación, ya que limita el acceso de los usuarios a todas los posibles servicios que ofrece Internet.

Propiedad Intelectual: Esta es una de las áreas que más problemas crea y que más se está intentando solventar. El caso más conocido es el de la piratería y es por la inexistente cohesión entre las políticas de los países con respecto a la Propiedad Intelectual.

Conclusiones

Es fundamental que los distintos actores que interfieren en el uso de Internet se pongan de acuerdo y actúen asumiendo su naturaleza, para ello deben de olvidar las fronteras y tener en cuenta que todo usuario debería disfrutar de la posibilidad de encontrar la misma información. Es por lo anterior que, para empezar, se debería crear una estrategia común en cuanto al desarrollo técnico de Internet y, después, gobiernos y actores de los mercados tendrían que crear un marco regulador, no restringido, para un uso correcto y seguro de una aplicación que tanto nos ha permitido avanzar.

Claudia Sánchez-Girón López

Estudiante en prácticas de la Universidad Pontificia de Comillas