

# La Fragmentación de Internet

Jorge Pérez Martínez. Catedrático UPM, *Chair of the IGF Spain*

Pilar Rodríguez Pita. Investigadora UPM, *Chair of the Youth IGF Spain*

## 1. Introducción

La razón principal por la que Internet se ha convertido en una la red de redes de alcance global es que se concibió desde el principio para permitir que un tipo de equipo ‘no definido’, funcionando con un software ‘no definido,’ conectado a una red ‘no definida’; que tiene asignado una dirección IP y utiliza el protocolo TCP capaz de intercambiar información con otro equipo ‘no definido’. Este agnosticismo respecto de las tecnologías utilizadas en su construcción y respecto a la naturaleza de los contenidos transportados, ha permitido la comunicación ‘extremo a extremo’ entre dos equipos (ordenadores, terminales, sensores, etc.) en cualquier momento y lugar.

Otra característica relevante de Internet es que su gobierno está muy dividido. Por un lado, existe un gobierno técnico encargado de la supervisión y control de lo que conocemos como ‘recursos críticos’ (direcciones IP, nombres de dominios, protocolos/parámetro, servidores raíz, etc.) que lo realizan un conjunto de instituciones privadas radicadas en EE. UU. (ICCAN, IAB, IETF, W3C, etc.), no reguladas por los gobiernos. Por otro lado, las redes de telecomunicaciones que transportan los paquetes de información están a cargo de operadores de telecomunicaciones sometidos a regulaciones de los gobiernos de los estados, gobiernos que a su vez acuerdan la regulación de las telecomunicaciones entre países mediante acuerdos firmados en instituciones multilaterales (UIT, OMC, etc.). Por último, las empresas que ofertan servicios y contenidos digitales (*Big Tech*, plataformas online, etc.) cada vez más sometidas a las diferentes legislaciones nacionales que reclaman su soberanía para defender los derechos e intereses de sus ciudadanos.

Internet fue una invención de EE. UU. La generosidad norteamericana de compartirla solo puede entenderse en el contexto geopolítico del nuevo orden internacional surgido tras la caída del muro de Berlín el 9 de noviembre de 1989. En la Conferencia Mundial de la UIT sobre Desarrollo de las Telecomunicaciones celebrada en Buenos Aires en 1995, el Vicepresidente de los Estados Unidos de América, Al Gore, exhortó a legisladores nacionales, responsables de la reglamentación y representantes del sector comercial a que colaboraran con miras a construir y poner en servicio una ‘Infraestructura Mundial de la Información’ e insistió en la necesidad de que “todos” los países del mundo participasen plenamente en los beneficios de esta "Red de Redes". Cualquier red de cualquier país podría conectarse a Internet, pero lo haría siguiendo unas reglas propuestas por EE. UU., que mantendrían a Internet abierta, libre, global, interoperable, confiable, segura... y no fragmentada.

Estas reglas, se han ido adaptando a la evolución de Internet, y se plasman en un conjunto de principios y compromisos, que no tienen valor jurídico, entre los que se incluye la gobernanza *multistakeholders* (gobiernos, el sector privado, instituciones gestoras de los recursos críticos, y la sociedad civil) de Internet. Unos principios y un modelo de gobernanza que ha sido permanentemente cuestionado por muchos países, entre ellos

China, India, Rusia y muchos países emergentes. Por otro lado, la UE, compartiendo los principios y el modelo de gobernanza, encuentra cada vez más dificultades en compatibilizar su “soberanía digital” con algunas de las reglas. El resultado es la progresiva fragmentación de Internet, una realidad que preocupa desde hace años a los diferentes *stakeholders* que participan en la gobernanza de Internet. En el nuevo contexto geopolítico, la posibilidad de que Internet se divida en muchas *splinternet* empieza a percibirse como una amenaza/oportunidad real.

## 2. La fragmentación de Internet. Concepto, tipos y ejemplos

Según la ICANN, la fragmentación de Internet es “la idea de que Internet puede estar en peligro de dividirse en una serie de segmentos del ciberespacio, poniendo en peligro su conectividad”<sup>1</sup>. Ha sido una preocupación creciente en la comunidad de gobernanza de Internet desde 2015, después de las revelaciones de Snowden (2013), la creación del firewall chino (2008) y la problemática transición de IPv4 a IPv6 (a partir de 2011) y se agudiza en 2020 cuando los gobiernos comenzaron a reclamar su ‘soberanía digital’.

Así, Europa, en el ejercicio de su soberanía digital, ha publicado la Ley de Servicios y Mercados Digitales (diciembre de 2020), el Reglamento General de Protección de Datos (publicado en mayo de 2016, en aplicación desde mayo de 2018) y el nuevo proyecto DNS4EU bajo el programa Connecting Europe Facility<sup>2</sup>. Estas iniciativas están definiendo un modelo europeo de Internet propio que en opinión de algunos *stakeholders* estaría favoreciendo la fragmentación. Por otro, por las crecientes tensiones geopolíticas entre el este (China y Rusia) y el oeste (Estados Unidos y Europa) favorecen la implantación de modelos de implantación y utilización de Internet muy diferentes.

El caso mas extremo de fragmentación sería la división de Internet en varias *splinternet* (una red que se rompe en astillas). Este término fue utilizado por primera vez en 2001 por el Instituto Cato<sup>3</sup>, como una alternativa de naturaleza privada (múltiples redes privadas interconectadas entre sí) frente a la Internet pública y global que se estaba construyendo. Recientemente, la *Internet Society* (ISOC) ha redefinido el término como “la idea de que la Internet abierta y conectada globalmente que todos usamos se fragmenta en una colección de redes aisladas controladas por gobiernos o corporaciones”, donde la web y los contenidos se bloquean dependiendo de la situación geográfica de los usuarios”<sup>4</sup>.

Según el Foro Económico Mundial (WEF), la fragmentación de Internet puede aparecer en tres formas: técnica, comercial y gubernamental<sup>5</sup>.

- Fragmentación técnica: ciertas condiciones sobre la infraestructura base que impiden a los sistemas interoperar e intercambiar paquetes de datos entre ellos, e impiden a Internet funcionar de manera consistente en todos los puntos finales (terminales). Este tipo de fragmentación la producen ciertos los *stakeholders* mediante técnicas de direccionamiento de red, firewalls, división de DNS, aislamiento de red privada, etc.
- Fragmentación comercial: prácticas comerciales que restringen o impiden ciertos usos de Internet para crear, distribuir o acceder a recursos de información. Este tipo de fragmentación la producen las empresas privadas actuando sobre *el*

*peering*, la estandarización, la neutralidad de la red, la geolocalización y el bloqueo geográfico, etc.

- Fragmentación gubernamental: políticas y acciones regulatorias de los países que restringen o impiden ciertos usos de Internet para crear, distribuir o acceder a recursos de información. Su origen se encuentra en el proteccionismo digital, la cibervigilancia, las prohibiciones de movimiento transfronterizo de datos, etc., y se justifica por razones de seguridad nacional y defensa de los valores, derechos e intereses de sus ciudadanos.

La fragmentación gubernamental es la más preocupante, entre otros motivos, porque casi siempre implica también el fraccionamiento técnico y comercial. No puede extrañarnos que sean decisiones gubernamentales las que produzcan las fragmentaciones técnicas más importantes.

### **La fragmentación técnica como consecuencia de acciones de los estados**

Uno de los principios fundamentales de internet se basa en la interoperabilidad, es decir, cualquier dispositivo conectado puede intercambiar paquetes con cualquier otro dispositivo, independientemente de su posición geográfica o su fabricante. Esto es gracias a un sistema global de direcciones de Internet y nombres de dominio, y un estándar DNS global.

Actualmente, podemos encontrar muchos países que se están poniendo fronteras a la Internet global, comenzando por China, donde desde 2008, su Firewall ha estado bloqueando ciertos contenidos para que no lleguen a los usuarios. Uno de los puntos de inflexión en la creación de esta firewall fue en 2009, después de que los disturbios en la región occidental de Xinjiang llevaran al bloqueo gubernamental de muchos sitios web, en su mayoría administrados por compañías estadounidenses, como Twitter, Facebook y Hotmail<sup>6</sup>. Desde entonces, hemos visto restricciones más estrictas en torno a las grandes empresas de tecnología, incluido el motor de búsqueda de Google y Wikipedia. Más recientemente, estamos viendo que se aplican las mismas prácticas en Irán, donde el Gobierno ha comenzado a restringir el acceso a Internet, con largos apagones<sup>7</sup>, después de que los manifestantes salieran a la calle para protestar contra la muerte de Mahsa Amini, una mujer de 22 años bajo custodia policial. La medida no es nueva en el país, donde en 2019 los usuarios experimentaron un apagón de Internet de cuatro días como respuesta a disturbios que desde entonces se han convertido en los más sangrientos en la historia reciente del país<sup>8</sup>. Esto son solo dos ejemplos de los muchos que se están dando en países con regímenes políticos no democráticos.

Otro ejemplo de fragmentación lo tenemos en Rusia cuando en 2019 aprobó la ley de "Soberanía de Internet" que introduce nuevos controles en Internet y otorga a los funcionarios amplios poderes para restringir el tráfico en la web rusa. Similar a la sección 706 de la ley de comunicaciones de los Estados Unidos, aunque menos restrictiva, el presidente ruso puede desconectar la red del país de la Internet global en casos de emergencia. La ley también exigía a los proveedores de servicios que instalaran equipos capaces de filtrar y obtener la información que pasa por los nodos clave de la Infraestructura<sup>9</sup>. Además, como parte de estas políticas, el gobierno ruso comenzó a probar en febrero de 2019 la desconexión de Internet del país como parte de una prueba de sus ciberdefensas, principalmente después de que la OTAN comenzara a considerar

sanciones debido a la continua ciberdelincuencia observada en el país. Bajo el Programa Nacional de Economía Digital, las redes rusas deben continuar operando incluso después de que las potencias extranjeras actúen para aislar al país, lo que significa que Rusia tendría que construir su propia versión del sistema de direcciones (DNS) de la red<sup>10</sup>. Las pruebas concluyeron en diciembre de ese año, con resultados exitosos<sup>11</sup>. Sin embargo, después de que comenzó la guerra en Ucrania, el Internet ruso se dejó sin interrupciones, con los Estados Unidos y Europa acordando que las sanciones no deberían interferir con el funcionamiento de las redes del país. A pesar de estas declaraciones, muchas empresas digitales han abandonado el país, incluidas Meta, Google y Apple<sup>12</sup>. Por último, Ucrania pidió a la ICANN, la Corporación de Internet para la Asignación de Nombres y Números, que revocara los nombres de dominio (.ru) y cerrara los servidores DNS primarios en el país, sin embargo, la ICANN rechazó la medida, argumentando que "nuestra misión no se extiende a tomar acciones punitivas, emitir sanciones o restringir el acceso contra segmentos de Internet, independientemente de las provocaciones. [...]. Esencialmente, la ICANN ha sido construida para garantizar que Internet funcione, no para que su función de coordinación se utilice para evitar que funcione".<sup>13</sup>

En opinión de algunos *stakeholders*, Europa también está contribuyendo al fraccionamiento de Internet al desarrollar su propio DNS en el marco del programa del 'Connecting Europe Facility'. Sin embargo, la Comisión Europea lo niega, afirmando que: "el DNS será transparente, se ajustará a las últimas normas y estándares y reglas de seguridad, protección de datos y privacidad por diseño y por defecto, y formará parte de la Alianza Industrial Europea para Datos y Nube"<sup>14</sup>. Uno de los principales problemas en torno a la implantación de nuevos DNS es la incapacidad de verificar los protocolos que lo conforman y la incapacidad de las instituciones para confirmar si los protocolos se están manteniendo, teniendo por tanto que confiar en la medición de los parámetros de rendimiento.

### **Fragmentación comercial**

La fragmentación comercial es algo inherente al desarrollo de los mercados digitales en los que las empresas compiten y colaboran para ofertar sus servicios y restringen/acuerdan el acceso a sus recursos de Internet. Lo que preocupa son aquellas prácticas comerciales que pudieran poner en peligro los principios en que se fundamenta Internet. En general preocupan las prácticas comerciales que pudieran afectar a la 'neutralidad de red', el despliegue de redes basadas en estándares propietarios, y los bloqueos derivados de la práctica comercial de personalización de los servicios.

La neutralidad de la red consiste en que los proveedores de Internet traten el tráfico de Internet por igual<sup>15</sup>. Desde hace mucho tiempo los operadores de telecomunicaciones sostienen que la errónea aplicación de este principio les impide competir con las *Big Tech*, limita sus ingresos y su capacidad de inversión en el despliegue de las nuevas infraestructuras. Recientemente, hemos sido testigos de este problema en Corea, donde SK Broadband exigió a Netflix que pagara por el uso de la infraestructura, después de que la transmisión de la popular serie "The Squid Game" llevara a la red a sus límites. Netflix intentó aliviar la carga instalando nuevos servidores de caché, sin embargo, el operador coreano emprendió acciones legales contra la plataforma que resultaron en que Netflix tuviera que pagar por el uso de la red coreana<sup>16</sup>.

Hasta ahora la Comisión Europea se había mantenido al margen, pero de acuerdo con el periódico POLITICO, la Comisión Europea presentará una propuesta para la “Ley de Infraestructura de Conectividad”, donde las *Big Tech* podrían verse obligadas a contribuir al despliegue de la red europea 5G. Hemos tenido indicios de una nueva legislación durante bastante tiempo, Thierry Breton había dicho anteriormente que los legisladores asegurarían que habría una retribución justa para las inversiones de telecomunicaciones en infraestructura para fines de 2022<sup>17</sup>; no mucho después el Consejo Europeo también afirmó que “todos los actores del mercado que se benefician de la transformación digital deberían asumir sus responsabilidades sociales y hacer una contribución justa y proporcionada a los costos de los bienes públicos, servicios e infraestructuras”,<sup>18</sup> por lo que la llegada de una nueva legislación parece solo el siguiente paso natural. Europa había establecido objetivos de conectividad muy ambiciosos en su brújula digital, incluido un objetivo de conectividad de “gigabit para todos y 5G en todas partes: todos los hogares europeos estarán cubiertos por una red Gigabit, con todas las áreas pobladas cubiertas por 5G” para 2030<sup>19</sup>. Sin embargo, el despliegue está siendo más lento de lo previsto, y el objetivo comenzó a parecer inalcanzable, con los operadores de telecomunicaciones teniendo que asumir los enormes costes de las licencias de espectro y el despliegue completo de la infraestructura. La propuesta de reglamento podría incluir las guías descritas en el *Connectivity Toolbox* publicado por la Comisión Europea, recomendaciones para las redes de muy alta capacidad y una revisión de las directrices sobre ayudas estatales de banda ancha<sup>20</sup>.

Otra práctica comercial que fragmentar internet es la extensión de redes basadas en estándares propietarios. Este problema se agudiza cuando se introduce un número masivo de dispositivos en la red como en el caso de IoT, es el caso de las soluciones propietarias como LoRa y Zigbee. Por último, preocupan también el rápido crecimiento del bloqueo geográfico como consecuencia de la personalización del usuario en función de su ubicación geográfica.

### **Fragmentación gubernamental**

En cuanto a la fragmentación gubernamental, es importante aclarar primero el concepto de soberanía digital, ya que podemos encontrar muchas definiciones dependiendo de la fuente. Para nuestro caso la ‘soberanía digital’ es *la capacidad de un país para actuar de forma independiente en el mundo digital*<sup>21</sup>. Sin embargo, hay una línea muy delgada entre la soberanía digital y el proteccionismo digital, la capacidad de un país para censurar ciertos sitios y movimientos de datos para socavar a los competidores extranjeros e impulsar a las empresas locales.<sup>22</sup> Un ejemplo clave de esta práctica es China, que además de bloquear técnicamente ciertos contenidos a través de su firewall, también han estado bloqueando ciertas plataformas para impulsar el crecimiento de sus propios gigantes digitales, un caso claro es el bloqueo de Amazon para permitir el crecimiento de Alibaba o el bloqueo de Facebook y Twitter para alimentar WeChat.

Aquellos países que no han realizado estas prácticas están viendo a sus empresas digitales locales incapaces de competir con las *Big Tech*; por lo tanto, se basan en la regulación para restringir ciertas prácticas que no se adhieren a sus principios y valores. En Europa, el ejemplo más reciente es la Ley de Servicios Digitales y la Ley de Mercados Digitales,

sin embargo, una de las regulaciones más controversiales fue el GDPR. El GDPR da a los consumidores más control sobre su información personal, y ha sido la causa de algunas de las mayores multas impuestas a las *Big Tech* en Europa.

Otra forma de fragmentación gubernamental es la censura de contenidos, como ha ocurrido en Rusia, donde las grandes tecnológicas Google y Meta se enfrentan a multas multimillonarias por no eliminar contenido considerado ilegal en el país<sup>23</sup>, una de las últimas fue el 18 de julio cuando Roskomnadzor multó a Google LLC con 21.077.392.317,8 rub les por no eliminar contenido sobre "la operación militar en Ucrania", convirtiéndose en la multa más grande a una empresa de tecnología en la historia del país.

Otro problema que proviene de la guerra geopolítica entre los países orientales y occidentales es la reciente prohibición de Estados Unidos a que reciban fondos federales aquellas empresas de tecnologías avanzadas que construyan fábricas en China en los próximos diez años<sup>24</sup>. Y como no, la llamada “guerra de los semiconductores” y otras tantas decisiones de Estados Unidos que muestra la posición decidida del país para seguir siendo un líder tecnológico en los próximos años a cualquier precio.

### **3. La Declaración para el Futuro de Internet y el Pacto Digital Mundial**

En abril del año en curso, la Casa Blanca anunció que Estados Unidos y otros 60 gobiernos habían firmado una nueva “Declaración para el Futuro de Internet”. Entre los 60 países firmantes se encuentran todos los Estados miembros de la Unión Europea, así como países de Asia, Oceanía y América. En el mundo hispano, tan solo firmaron Costa Rica, Argentina, Colombia, República Dominicana, Perú, Uruguay y España. Entre los países que no han firmado la declaración se encuentran China, India, Rusia, Nigeria, Brasil y Méjico; solo la suma de los potenciales internautas de estos países supera de largo más de la mitad de los internautas del mundo.

La Declaración incluye el compromiso de los países firmantes para:

- Proteger los derechos humanos y las libertades fundamentales de todas las personas en Internet
- Promover una Internet global que promueva el libre flujo de información
- Promover la conectividad inclusiva y asequible para que todas las personas puedan beneficiarse de la economía digital
- Promover la confianza en el ecosistema digital mundial y la protección de la privacidad
- Proteger y fortalecer el enfoque de gobernanza de múltiples partes interesadas que mantiene Internet en funcionamiento para el beneficio de todos.

Nada nuevo bajo el sol, son los mismos principios (democráticos) y de gobierno (gobernanza *multistakeholders*) que han caracterizado Internet en las últimas décadas. Estados Unidos y los países occidentales no renuncian a su modelo primigenio en favor de un modelo *multistakeholders*.

De forma paralela la ONU está poniendo en marcha un ambicioso “Pacto Digital Mundial” con la intención de buscar principios compartidos para un futuro digital abierto,

libre y seguro para todos; donde se abordaran temas tales como la conectividad digital, evitar la fragmentación de Internet, brindar a las personas opciones sobre cómo sus datos son utilizados, la aplicación de los derechos humanos en línea y la promoción de una Internet confiable mediante la introducción de criterios de responsabilidad por discriminación y contenido engañoso. Un intento más de buscar consensos más amplios que permitan obtener los beneficios de mantener un ecosistema digital mundial y, sobre todo, que no dé al traste con el mayor éxito de la globalización: en desarrollo de una Internet global.

Sin duda sería interesante que ambas iniciativas convergiesen, pero parece muy difícil en el escenario geopolítico actual.

#### **4. La gestión de la fragmentación**

Internet continuará fragmentándose cada vez más como consecuencia de las políticas técnicas, comerciales y gubernamentales que analizamos en el apartado anterior. Sin embargo, que Internet se fraccione no significa que se rompa la Internet global. Los autores de esta ponencia coinciden con Scott Malcomson, autor del libro '*Splinternet: How Geopolitics and Commerce are Fragmenting the World Wide Web (2017)*'. Que, en la reciente reunión del Foro de Gobernanza de Internet en Reino Unido, expuso siete buenas razones para que, aunque cada vez mas fragmentada, Internet continúe siendo global. A saber:

- 1) Las principales potencias tecnológicas (países) quieren tener acceso a todas las redes de los países con fines de seguridad, armamento cibernético y distribución de propaganda fuera de sus fronteras físicas.
- 2) Los agentes del mercado que se han beneficiado de la globalización, como las empresas de criptomonedas y las plataformas online no van a querer que se fragmente el ecosistema.
- 3) Los avances en los impuestos al comercio electrónico se han convertido en una fuente muy importante de ingresos para los estados.
- 4) La aceptación por parte de las multinacionales tecnológicas a que haya localización geográfica de los datos.
- 5) Los países pequeños se benefician del acceso al mercado global, en particular sus empresas.
- 6) Las grandes multinacionales tecnológicas quieren llegar al mayor mercado posible, y por lo tanto se convierten en constructores y mantenimiento de la infraestructura de internet.
- 7) Las comunidades *stakeholder* como ICANN tienen protección frente a la intervención por parte de gobiernos individuales cuando se encuentran en un internet global.

No todos los países quieren el mismo modelo de internet, ni están dispuestos a renunciar al modelo que han adoptado, por lo que las diferencias culturales y políticas y el propio dinamismo de los mercados digitales hacen que no se pueda evitar el fraccionamiento. Por otro lado, en términos de coste/beneficio para la Internet global, es mucho mejor tener 193 países luchando por sus propios intereses en una comunidad que tener tres bloques no interoperables.

En lugar de tener tres o cuatro troncos (3 o 4 *splinternets* separadas), es mejor tener un solo montón de astillas (múltiples *splinternets* conectadas).

---

<sup>1</sup> ICANN. Fragmentación de Internet. 2 de febrero de 2022. L.s. 26 de septiembre de 2022.

[https://icannwiki.org/Internet\\_Fragmentation](https://icannwiki.org/Internet_Fragmentation)

<sup>2</sup> Comisión Europea. Equipar las redes troncales con infraestructuras de resolución DNS seguras y de alto rendimiento – Obras. 20 de abril de 2022. <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works>

<sup>3</sup> Instituto Cato. Un Internet no es suficiente. 11 de abril de 2001.

<https://www.cato.org/techknowledge/one-internet-not-enough>

<sup>4</sup> Internet Society. Splinternet. S.S. 26 Septiembre 2022. <https://www.internetsociety.org/splinternet/>

<sup>5</sup> William J. Drake, Vinton G. Cerf, Wolfgang Kleinwächter. Internet Fragmentation: An Overview Word Economic Forum. Enero 2016.

[https://www3.weforum.org/docs/WEF\\_FII\\_Internet\\_Fragmentation\\_An\\_Overview\\_2016.pdf](https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf)

<sup>6</sup> El Guardián. China bloquea Twitter, Flickr (en inglés y Hotmail antes del aniversario de Tiananmen. (2 de junio de 2009). <https://www.theguardian.com/technology/2009/jun/02/twitter-china>

<sup>7</sup> Los apagones de Internet de Irán son un grave motivo de preocupación (septiembre de 2022)

<https://edition.cnn.com/2022/09/24/tech/iran-internet-blackout/index.html>

<sup>8</sup> El apagón de Internet de Irán alcanza la marca de cuatro días (Noviembre 2019)

<https://www.bbc.com/news/technology-50490898>

<sup>9</sup> Noticias de la BBC. Rusia internet: entra en vigor ley que introduce nuevos controles. (1 de noviembre de 2019). <https://www.bbc.com/news/world-europe-50259597>

<sup>10</sup> Noticias de la BBC. Rusia considera 'desconectarse' de internet. (11 de febrero de 2019).

<https://www.bbc.com/news/technology-47198426>

<sup>11</sup> Noticias de la BBC. Rusia 'prueba con éxito' su internet desconectado (24 de diciembre de 2019).

<https://www.bbc.com/news/technology-50902496>

<sup>12</sup> Noticias de la BBC. Rusia-Ucrania: ¿Está Internet al borde de la ruptura? (9 de marzo de 2022).

<https://www.bbc.com/news/technology-60661987>

<sup>13</sup> CNN Negocios. La solicitud de Ucrania de aislar a Rusia de la Internet global ha sido rechazada (3 de marzo de 2022). <https://edition.cnn.com/2022/03/03/tech/ukraine-russia-internet-icann/index.html>

<sup>14</sup> C europeomisión. Estrategia de ciberseguridad de la UE para la Década Digital: preguntas y respuestas (18 de noviembre de 2021) <https://digital-strategy.ec.europa.eu/en/faqs/eu-cybersecurity-strategy-digital-decade-questions-and-answers>

<sup>15</sup> La H BlancaOuse. Neutralidad de la red, el plan del presidente Obama para una Internet libre y abierta. (26 Febrero 2015) <https://obamawhitehouse.archives.gov/net-neutrality>

<sup>16</sup> Noticias de Telecomunicaciones. Netflix ordena pagar por el uso de la red en Corea (29 de junio de 2021) <https://telecoms.com/510357/netflix-ordered-to-pay-for-network-usage-in-korea/>

<sup>17</sup> El Ecos. Bruselas Quiere cobrar el Redes telecomunicaciones el Gafam (3 de mayo de 2022)

<https://www.lesechos.fr/tech-medias/hightech/bruxelles-veut-taxer-les-gafam-pour-financer-les-reseaux-telecoms-1404614>

<sup>18</sup> Posteítico. Los países de la UE quieren que las empresas tecnológicas paguen por la infraestructura de telecomunicaciones (11 de mayo de 2022) <https://www.politico.eu/article/eu-tech-firm-pay-telecom-infrastructure/>

<sup>19</sup> Comisión Europea. Brújula digital 2030: el camino europeo para la Década Digital (9 de marzo de 2021) <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118>

<sup>20</sup> Posteítico. Ejecutivo de la UE mira el dinero de las Big Tech para salvar 5G (27 de junio de 2022)

<https://www.politico.eu/article/commission-present-connectivity-infrastructure-act-eu/>

<sup>21</sup> Parlamento Europeo. Soberanía digital para Europa (2 de agosto de 2020)

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

<sup>22</sup> Washington Post. El proteccionismo digital de China pone en riesgo el futuro de la Internet global (25 de febrero de 2019). <https://www.washingtonpost.com/outlook/2019/02/25/chinas-digital-protectionism-puts-future-global-internet-risk/>

<sup>23</sup> Noticias de la BBC. Cómo Rusia intenta censurar las redes sociales occidentales (17 de diciembre de 2021) <https://www.bbc.com/news/blogs-trending-59687496>

<sup>24</sup> Estados Unidos prohíbe a las empresas de "tecnología avanzada" construir fábricas en China durante 10 años (Septiembre 2022) <https://www.bbc.com/news/62803224>