

INTERNET LIBRE VS. SISTEMA DE REDES SOBERANAS

*Identificación de los países que
planean desconectarse y análisis de
los motivos*

MÁSTER EN ANALISTA DE INTELIGENCIA
CÁTEDRA SERVICIOS DE INTELIGENCIA Y
SISTEMAS DEMOCRÁTICOS



Universidad
Rey Juan Carlos

Equipo de Analistas:



PATRICIA LEÓN
CECILIA GREGORI
LEOPOLDO GIL
AIDA CASTELLANOS
JESÚS ARCENEGUI

07/01/2020



Tabla de contenido

0. Introducción.....	3
1. Marco Teórico y Estado de la Cuestión	5
1.1 Bases teóricas	
1.1.1 Definiciones para acotar conceptos	
1.1.2 Necesidad de examinar este tema : los imperativos académicos	
1.1.3 Hipótesis planteadas	
1.2 Evolución cronológica de Internet	
1.3 La conectividad de Internet hoy:	
1.3.1 Penetrabilidad	
1.3.2 Tipos de control	
1.3.3 El Gobierno de Internet: Dinámicas globales vs. Dinámicas nacionales	
2. Estudios de caso: Perspectiva general y Justificación elección de casos.....	23
2.1 China	
2.2 Rusia	
2.2.1 Aparición y evolución de RuNet	
2.2.2 Tipos de cortes en RuNet	
2.2.3 Evaluaciones de los controles	
2.3 Irán	
3. Motivos de la censura y el bloqueo en Internet	38
3.1 Motivos en relación a la Comunidad LGTBI	
3.2 Motivos económicos	
3.3 Para limitar la exposición a la información exterior y promulgar valores nacionales	
3.4 Para paralizar la movilización de la SC controlando el relato político	
3.5 Para distorsionar la celebración de elecciones libres	
4. Conclusiones	46
5. Bibliografía	47

0. Introducción

Eran las 8 de la mañana del 31 de enero de 1990 cuando en la Plaza Roja de Moscú abría la primera franquicia de McDonald's en territorio de la Unión Soviética. Decenas de personas esperaban su turno en la cola para poder consumir el conocido producto estadounidense; surgido de la instauración de una fábrica por valor de 40 millones de dólares, en la periferia de la ciudad.

Sin embargo, en 2014 el gobierno ruso anunciaba su cierre debido al incumplimiento de las normas relativas al Plan de Inspecciones del régimen sanitario y epidemiológico. Ello era sólo una pantalla, pues la causa subyacente se encontraba en la respuesta del Kremlin a las sanciones occidentales por la crisis de la anexión de Crimea, que ni Ucrania ni Occidente reconocían como legítima.

Este fenómeno ilustra el paulatino pero imparable crecimiento que señala Joseph Nye en relación a las técnicas de *Soft Power* en detrimento del tradicional *Hard Power*, dibujando un contexto mundial sumido en la globalización, y cuyos escenarios donde se libran las batallas son múltiples y diversos. Así, uno de los principales campos, debido a la transmutación del paradigma de la Sociedad Industrial a la Sociedad de la Información y el Conocimiento – conceptualizada por Castells- es el espacio virtual.

Internet, junto a otras tendencias de ámbito regional e internacional, ha contribuido a la quiebra de las soberanías nacionales de los Estados-Nación y se ha consolidado como una herramienta clave de la conectividad mundial, de los procesos sociales y políticos democratizadores, así como de la lucha por los Derechos Humanos.

No obstante, no le faltan enemigos. La información libre y accesible aún lo es sólo en algunos puntos del globo, mientras que en su mayoría se libran batallas entre murallas chinas doradas y capas de cebolla. Como indica Félix Arteaga, investigador principal de Seguridad y Defensa del Real Instituto Elcano no son pocos los actores que tienden a reforzar la fragmentación de los distintos sistemas de la Red, tanto desde la óptica pública tratando de prevenir la influencia exterior para dominar su propio territorio nacional, como desde la óptica privada, tratando de proteger sus mercados cautivos en sus grandes plataformas.

Se puede afirmar con toda seguridad que los actores gubernamentales se debaten permanentemente en el binomio de las oportunidades y las amenazas que supone mantener y garantizar el acceso al Internet “libre” por parte de la Sociedad Civil. Así, mientras tratan de no quedarse desconectados de la esfera global –pues ya es casi por todos asumidos que un Estado aislado es más débil (piénsese sólo en las consecuencias para el comercio o el turismo)-, al mismo tiempo, como recuerda Ángel Luis Rubio Moraga, investigador de la

7 de febrero de 2020

Universidad Complutense de Madrid, existe una clara voluntad gubernamental para que una mayor libertad de expresión no suponga también la pérdida de poder institucional.

De este modo, se hace patente –como indica Vercelli- la necesidad de investigar la cara menos amable de Internet: cuestionar si existe libertad de acceso, conocer las limitaciones a la libertad de expresión, o descubrir los diferentes tipos de bloqueo, censura y autocensura que conviven e identificar las tendencias clave de este fenómeno.

Para ello, este trabajo se configura en tres partes diferentes:

En primer lugar, se desarrolla el Marco Teórico y el Estado de la Cuestión, aludiendo tanto a las bases teóricas que se deben conocer para enfrentar este tema, como a la necesidad académica y práctica de trabajar sobre este asunto, y al planteamiento de la hipótesis principal.

En segundo lugar, se abordan los tres estudios de caso, elegidos debido a su relevancia internacional y por reflejar las tendencias de “desconexión” actuales existentes a gran escala.

Finalmente, se desarrolla una clasificación que ayudará a comprender el abanico de motivos existentes para la censura y el bloqueo en Internet.

* * *



1. Marco Teórico y Estado de la Cuestión

1.1 Bases Teóricas

1.1.1 Definiciones para acotar conceptos

Dada las posibles interpretaciones que pueden realizarse de los conceptos utilizados a lo largo de este informe, se considera oportuno aclarar algunas definiciones en los términos aplicados:

➤ Internet:

Se utiliza el término acotado por el Federal Networking Council en 1995:

Internet hace referencia al sistema global de información que: 1. Está enlazado en forma lógica por un espacio global único basado en el protocolo de Internet (IP) y sus extensiones subsecuentes; 2. Es capaz de soportar comunicaciones utilizando el protocolo de control de transmisiones/protocolo de Internet (TCP/IP) o sus extensiones subsecuentes, y/o otros protocolos compatibles con IP; y 3. Ofrece, utiliza o permite tener acceso, bien sea de forma pública o privada, altos niveles de servicios a partir de las comunicaciones y la infraestructura descrita aquí.

Por ello, cuando el documento menciona la nomenclatura “Internet Libre” se hace referencia a la acepción cuyo significado se refiere al libre acceso al mismo, sin restricciones empresariales ni gubernamentales; entendiendo al que se conecta la gran mayoría de la gente (Clearnet), sin entrar a discutir sobre dicho concepto frente a la Deepweb o Darknet. En el lado opuesto al “Internet Libre” se encuentra el “Internet cerrado”; cuyo contenido es monitorizado, censurado o bloqueado.

➤ Cortes de internet:

El texto se guía por la definición de Merino en 2019:

Se trata de una interrupción deliberada de Internet o comunicaciones electrónicas, incluyendo las redes sociales, con el fin de imposibilitar el acceso de la población de un sitio web específico y dominar así el flujo de la información.

Asimismo se utiliza el término *Internet Shutdown* para hacer alusión al corte o apagón intencional de las comunicaciones en un territorio delimitado por una franja temporal.

➤ Sistema de redes soberanas:

Se utiliza la definición de Vercelli:

El Sistema de Redes Soberanas consiste en un bloqueo/ filtrado de información y contenidos con voluntad de permanecer en el tiempo.

➤ Neutralidad de la Red:

El informe se apoya en el significado señalado por Robert Easley, entendiendo que constituye el principio por el cual los proveedores de Internet y los Gobiernos que lo regulan deben tratar a todo el tráfico de la Red de forma indiscriminada.

1.1.2 Imperativo académico para examinar este tema

En 1651, Thomas Hobbes publicó su conocida obra "*Leviatán*", que articulaba la base del contrato social sobre la idea de que no era posible vivir en el Estado de Naturaleza, puesto que *Homo homini lupus est*; es decir, "el hombre es un lobo para el hombre".

Algunos siglos después surgió el ciberespacio, cuya dimensión alberga no solo un canal inmenso de transmisión de datos, sino un espacio paralelo de interacción social, económica y política. Por ello, tal y como se planteó por los pensadores ilustrados del S. XVIII, el ciberespacio como sociedad virtual debe ser regulada para que no se cometan excesos.

El problema aparece a la hora de establecer dónde reside la soberanía en un espacio sin fronteras al generarse situaciones o conflictos que tradicionalmente estaban bajo la órbita de acción del Estado-Nación; pues si bien un país puede legislar sobre Internet e incluso elaborar grandes volúmenes legales, eso no implica que tenga el poder coercitivo para lograr que tales normas sean cumplidas.

De esta forma los autores consideramos necesaria la elaboración de literatura académica sobre este asunto, queriendo aportar nuestro grano de arena investigando cuáles son los Estados que hoy por hoy llevan a cabo prácticas de censura, así como cuáles son los motivos alegados gubernamentalmente y los reales.

Paralelamente nos gustaría señalar el carácter innovador de este proyecto, puesto que si bien existen múltiples investigaciones sobre los cortes de Internet en un determinado país, no es mucha la literatura existente que establece comparativas entre ellos, interrelaciona los diferentes motivos y traza las líneas estructurales de este campo de estudio.

1.1.3 Hipótesis planteada

La globalización, la consolidación de la Sociedad de la Información con la expansión de Internet, o los fenómenos de multiterritorialidad –como la descentralización tanto regional como internacional- son algunos de los factores que han ocasionado la ruptura de la soberanía tradicional de los Estados Nación. En este contexto, los Gobiernos tratan de mantener el poder utilizando diferentes herramientas; una de las cuales son los cortes de Internet, bien sean temporales o permanentes.

En este marco, la investigación estará destinada a corroborar o refutar la siguiente hipótesis:

La censura –entendida como aquellos obstáculos establecidos que supongan cualquier dificultad para acceder a un contenido absoluto y plenamente libre para la ciudadanía- se sitúa en una larga línea de grises, pues abarca desde la ejecución de *Shutdowns* totales hasta el filtrado de contenido ilegal e ilícito (por ejemplo, a través de fórmulas de protección de la infancia de contenidos pornográficos y dañinos, o la lucha contra la información ilícita o xenófoba).

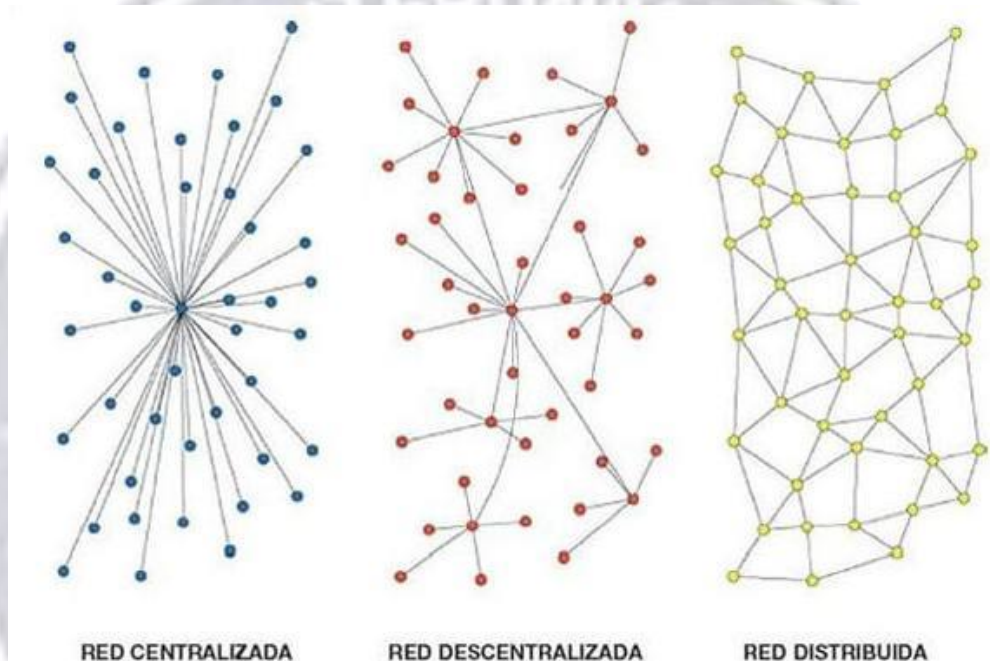
Así, si bien en los países democráticos también existen bloqueos de acceso a la información y censura de contenidos, cuanto más autocrático es el régimen político de un Estado más burdo y descarado es este proceso.

Para ello, el objeto de estudio principal se centrará en una muestra macro –examinando los casos de China, Rusia e Irán- y una muestra micro, que consistirá en analizar veinte países, para poder extraer una clasificación de los principales motivos concretos por los que los Estados ejecutan cortes digitales.

1.2 Evolución cronológica de Internet

Los orígenes de Internet se remontan al período de la guerra fría, tras finalizar la Segunda Guerra Mundial, momento caracterizado por el enfrentamiento entre el llamado bloque Occidental liderado por Estados Unidos y el bloque Este liderado por la Unión Soviética. Es conveniente citar el momento histórico en el que la Unión Soviética lanza su primer satélite. El Sputnik 1, nombre de dicho satélite, fue lanzado el 4 de octubre de 1957. Este hecho supuso un desafío para el Departamento de Defensa de los Estados Unidos y contribuyó a poner de manifiesto la necesidad de priorizar el desarrollo científico y tecnológico para evitar quedar obsoleto y facilitar, de este modo, la victoria a su enemigo. Fue entonces cuando se crea la Agencia de Proyectos de Investigación Avanzada, ARPA (*Advanced Research Projects Agency*). La misión de esta agencia estadounidense era, por lo tanto, desarrollar nuevas

tecnologías para uso militar. ARPA comenzó a desarrollar una red militar más fuerte con capacidad suficiente para soportar ataques por parte del enemigo. El objetivo era crear una red en la que las comunicaciones que se estableciesen dentro de ellas no se vieran afectadas en caso de sufrir un ataque nuclear. Esta red debía considerar todos los nodos por igual para que, de este modo, el tráfico no se viera afectado si un nodo era atacado. Con una red centralizada, si el nodo central es atacado, la red entera queda inactiva. De esta forma, al no existir un nodo principal, cada nodo tendría la capacidad para decidir qué ruta debían llevar los datos hasta alcanzar su destino. Asimismo, los datos se dividirían en “paquetes”, cada uno de los cuales podría seguir una ruta distinta hasta llegar al destino común.



En 1961 Leonard Kleinrock, profesor de Ciencias de la Computación en la UCLA (Universidad de California, Los Ángeles) e investigador del Instituto de Tecnología de Massachusetts, MIT (*Massachusetts Institute of Technology*), publicó el primer trabajo sobre la conmutación de paquetes para transferir datos. La conmutación de paquetes es una tecnología que permitiría dividir los datos en pequeños fragmentos o bloques denominados “paquetes” que serían enviados a través de la red para llegar a su destino final, pudiendo seguir distintas rutas en función de las características del tráfico en ese momento.

En 1962 ARPA estableció un programa de investigación computacional y a finales de año, J.C.R. Licklider, científico y profesor en el MIT, fue nombrado director de la Oficina de Técnicas para el Procesamiento de la Información, IPTO (*Information Processing Techniques Office*). Licklider desarrolló el concepto de Galactic Network que pretendía describir una red interconectada globalmente que permitiese acceder a los datos desde cualquier parte del

mundo. Posteriormente, J.C.R. Licklider compartió su idea con sus compañeros de la agencia ARPA. Gracias a Licklider, el Pentágono, conocedor de dichas investigaciones que buscaban construir una red de comunicaciones más robusta, destinó grandes cantidades de dinero a la financiación del desarrollo de estas redes informáticas.

Por otro lado, entre 1962 y 1964, Paul Baran de la Corporación Rand, elaboró unos informes en los que se describía una posible estructura de comunicaciones semejante a una tela de araña, cuya finalidad era también impedir la inoperatividad de la red tras un ataque. Este proyecto se basó en la teoría de la conmutación de paquetes de Leonard Kleinrock. Igualmente, fue en 1963 cuando el Comité Estadounidense de Estándares (ASA o ANSI) crea ASCII (*American Standard Code for Information Interchange*). ASCII es un código de caracteres que tiene su base en el alfabeto romano. Más tarde añadieron las mayúsculas y minúsculas y se redefinieron algunos códigos.

En 1965 Lawrence G. Roberts, investigador del MIT, consiguió la conexión entre dos ordenadores a través de una línea telefónica conmutada de baja velocidad. Concretamente la conexión se realizó entre un ordenador TX2 ubicado en Massachusetts y un Q-32 situado en California. Esta pequeña red de ordenadores fue creada utilizando la teoría de la conmutación de paquetes que previamente había ideado su compañero del MIT, Leonard Kleinrock.

Para la fecha de 1967 ya se había realizado suficiente trabajo y ARPA pudo publicar su primer diseño de una red de ordenadores llamada ARPANET (*Advanced Research Projects Agency Network*). Dicho diseño fue el resultado de la combinación de las mejores ideas de los equipos del MIT, la National Physics Laboratory- UK (R. Scantlebury y D.W.Davies) y la Rand Corporation.

En 1968 L. G. Roberts (investigador en la Agencia de Investigación de Proyectos Avanzados de Defensa, DARPA) presentó al director de ARPA un proyecto para la construcción de la futura red. Fue la consultora BBN la que obtuvo el contrato para la realización de dicho proyecto.

Un año más tarde, en 1969, se estableció ARPANET, la primera red sin nodos centrales. Esta red estaba conformada por cuatro universidades estadounidenses: Universidad de California Los Ángeles (UCLA), Universidad de California Santa Bárbara (UCSB), Universidad de Utah y Stanford Research Institute (SRI). La primera transmisión tuvo lugar el 29 de octubre de 1969, entre UCLA y SRI. Por entonces, se creó también el primer programa de control de redes, el Network Control Program (NCP) que posteriormente pasó a llamarse Network Control Protocol y que fue la base de las comunicaciones en ARPANET hasta que apareció el protocolo TCP/IP. Un protocolo de comunicación es un conjunto de reglas que definen los pasos a seguir para que dos computadores se comuniquen entre sí.

En 1972, los creadores de ARPANET, buscando una forma para comunicarse fácilmente entre ellos, idearon un programa que permitía el intercambio de mensajes entre los ordenadores conectados a la red. El inventor del correo electrónico fue el ingeniero Raymond Tomlinson, trabajador de la empresa BBN Technologies quien inventó en 1971 el primer programa de correo electrónico. A él se le atribuye igualmente la creación del símbolo '@' empleado en la mensajería.

ARPANET se internalizó en 1973 con la incorporación Gran Bretaña y Noruega, a través de la Universidad College of London y NORSAR (*Norwegiann Seismic Array*) respectivamente.

La palabra "Internet" comenzó a usarse a comienzos de la década de los años 80. Fue también por estas fechas cuando se definió el protocolo TCP/IP (*Transfer Control Protocol/Internet Protocol*) diseñado por Vinton Cerf y Robert Kahn. La primera prueba de comunicación utilizando el protocolo TCP/IP se realizó en 1975 entre la Universidad de Stanford y la UCL. Sin embargo, no fue hasta 1982 cuando el Departamento de Defensa de los Estados Unidos lo declaró como estándar para las comunicaciones en el ámbito militar. Poco después, en 1983, ARPANET migró completamente a dicho protocolo, abandonando el Network Control Program (NCP). Este protocolo marcó un hito importante pues permitió soportar no solo las comunicaciones entre ordenadores de una misma red, sino las comunicaciones entre redes interconectadas mediante gateways. En este mismo año, por decisión del ministerio de Defensa de Estados Unidos, ARPANET se dividió. Por un lado, de los 113 nodos que conformaban ARPANET, 68 pasaron a formar parte de una nueva red con carácter puramente militar llamada MILNET (*Military Network*). Al resto, que seguían manteniendo su carácter científico- académico y civil, se fueron uniendo más nodos procedentes de distintas partes del mundo, creando lo que más tarde se conocería como Internet.

Si bien es cierto que es difícil establecer una fecha exacta del nacimiento de Internet, podría considerarse 1983 la fecha en la que realmente nació cuando se separa se la parte militar y se crea el sistema de nombres de dominios que permitió solventar una de las mayores dificultades con las que se encontraron a medida que ARPANET crecía. El gran crecimiento hacía cada vez más complicado localizar un determinado equipo y las tablas, con las direcciones de los hosts, debían actualizarse con mayor periodicidad para conocer dónde se encontraba cada uno de ellos. Fue Tim Berners-Lee, británico licenciado en la Universidad de Oxford e investigador en el CERN, quien creó el primer servidor World Wide Web y el primer programa cliente WorldWideWeb. El World Wide Web (WWW) es una red de "sitios" que pueden ser buscados y mostrados con un protocolo llamado HTTP (*HyperText Transfer Protocol*), lo que permitió buscar y mostrar documentación a través de Internet de manera más sencilla. El llamado nombre de dominio (DN, *Domain Name*) es una secuencia de caracteres que sustituye a las direcciones numéricas, las llamadas direcciones IP. Esto facilitó el acercamiento a los seres humanos pues resultaba más fácil memorizar una secuencia de caracteres (www.ejemplo.com) que una de números comprendidos entre el 0 y el 255 (20.125.125.125). Asimismo, fue

también Tim Berners-Lee quien logró que Internet fuese más atractivo mediante la elaboración del HTML que permitía combinar textos, imágenes y establecer enlaces a otros documentos. Desde entonces la Gran Red Mundial (*World Wide Web*) fue creciendo de forma exponencial.

En 1990 ARPANET dejó de existir y se celebró la primera conferencia sobre ciberespacio en la Universidad de Texas en Austin.

En 1993 Marc Andreessen y Eric Bina, del Centro Nacional de Aplicaciones de Supercomputación, NCSA (*National Center for SuperComputing Applications*) de la Universidad de Illinois publicaron Mosaic, un programa que permitía navegar por Internet con mayor facilidad. Supuso una mejora notable en la forma en qué se mostraban los gráficos. Posteriormente Mosaic se convirtió en Netscape, creado por Marc Andreessen y Jim Clark. Este navegador facilitó considerablemente la utilización de la World Wide Web. En 1994 la empresa Netscape lanzó su primer navegador basado en Mosaic, consiguiendo dominar más del 80% del mercado. Netscape fue el primer navegador comercial en el mundo de Internet. Un año más tarde, en 1995, Microsoft lanzó su primer navegador, Internet Explorer. Pese a ser técnicamente peor que el navegador de Netscape se fue apoderando de la cuota de mercado por ser gratuito. Finalmente, Netscape terminó desapareciendo.

Con la llegada de los navegadores y la publicación de la tecnología WWW Internet se fue abriendo al público, empleándose en diversas actividades. Este crecimiento se aceleró con la aparición de nuevos ordenadores más baratos y potentes. Al mismo tiempo, en abril de 1994 dos estudiantes de Ingeniería eléctrica de la Universidad de Stanford, David Filo y Jerry Yang, fueron archivando las direcciones de Internet que más les gustaban, agrupándolas por temas. Posteriormente, decidieron publicarlas para que cualquier persona pudiera consultar dicho catálogo de direcciones de forma gratuita. Así nació Yahoo!. En este mismo año Jeff Bezos funda la compañía llamada Amazon.

A finales de 1995, Jack Smith y Sabeer Bhatia, estudiantes de posgrado de la Universidad de Stanford, crearon Hotmail, buscando una forma de poder comunicarse sin que sus comunicaciones de correo electrónico pudiesen ser vistas desde las computadoras de la que por entonces era la compañía en la que trabajaban, Apple Computer. Fue lanzado comercialmente en 1996 y un año más tarde, en 1997, Hotmail fue comprada por Microsoft, pasando a llamarse MSN Hotmail. En 1996 la empresa finlandesa Nokia lanza el primer teléfono móvil con Internet, un Nokia 9000 Communicator presentado en la Feria Tecnológica CeBIT de Hannover en 1996.

Unos años más tarde, en 1998, Larry Page y Sergey Brin, dos estudiantes de doctorado de la Universidad de Standford fundan la compañía Google. No obstante, Google fue iniciado a comienzos de 1996 como proyecto universitario de Page y Brin. En 1997, el buscador web de

Google, que empleaba una nueva tecnología para clasificar las páginas web en función de su importancia, se consolida como el buscador más utilizado a nivel mundial.

En 1999, ante la necesidad de crear un mecanismo que permitiera conectar de forma inalámbrica distintos tipos de dispositivos, nace la tecnología Wi-Fi. Las empresas 3Com, Intersil, Airones, Nokia, Lucent Technologies y Symbol Technologies se unieron para crear la Wireless Ethernet Compatibility Alliance, llamada hoy día Alianza Wi-Fi, organización que impulsó dicha tecnología.

Dos años más tarde, en 2001, aparece la primera enciclopedia libre de Internet llamada Wikipedia. Jimmy Wales y Larry Sanger son los creadores de la mayor enciclopedia de internet. Posteriormente, en 2002 se funda la red social orientada a negocio conocida como LinkedIn pero, fue lanzada un año más tarde, en 2003. En este mismo año, la compañía Apple lanza Safari, un navegador web de código cerrado desarrollado que sustituiría a Internet Explorer, navegador predeterminado que incluían anteriormente los ordenadores de Apple. Paralelamente se lanza MySpace (servicio de red social), WordPress (sistema de gestión de contenidos) y iTunes Store. Asimismo, el danés Janus Friis y el sueco Niklas Zennström diseñaron Skype, un software que permitía comunicaciones de texto, voz y vídeo en Internet.

En 2004, Google lanza su propio servicio de correo electrónico llamado Gmail. También, en 2004 se funda Facebook. Fue Mark Zuckerberg, estudiante de la Universidad de Harvard el autor de la idea original. Un año después aparece YouTube, plataforma líder de vídeos y, seguidamente, en 2006 nace Twitter. El año en el que Google lanza al mercado su primer navegador web, Google Chrome, fue 2008, convirtiéndose en poco tiempo en el navegador más utilizado a nivel mundial. Finalmente, desde 2009 hasta nuestros días, Internet se ha visto favorecido con la llegada de más aplicaciones como WhatsApp o Instagram, así como de servicios tales como Spotify o Netflix. No obstante, Internet sigue creciendo y su grado de penetración continúa aumentando en todo el mundo.

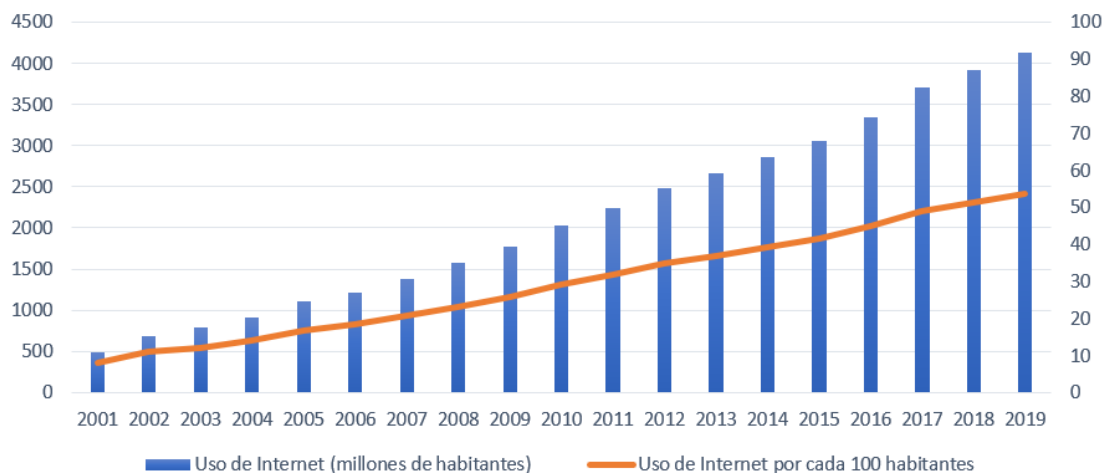
1.3 La conectividad de Internet hoy:

1.3.1. Penetrabilidad

Hoy en día se torna incuestionable la magnitud del impacto que el desarrollo tecnológico está ejerciendo en el devenir social. Si bien es cierto que la industria de las telecomunicaciones continúa experimentando un crecimiento más acelerado que otros sectores, es el alto grado de penetración en la vida de las personas lo que lo convierte en poderoso. Es decir; la soberanía digital no es más que una pequeña parte de un debate mucho mayor que gira en torno al poder y que presenta una dimensión que abarca aspectos sociales, económicos y políticos, siempre y cuando el número de usuarios conectados sea significativo.

Así lo avalan los datos recogidos por la Unión Internacional de Telecomunicaciones, ITU: según sus informes la cantidad de población que utilizó Internet en el año 2019 fue 4.131

Uso de Internet a nivel mundial, 2001-2019

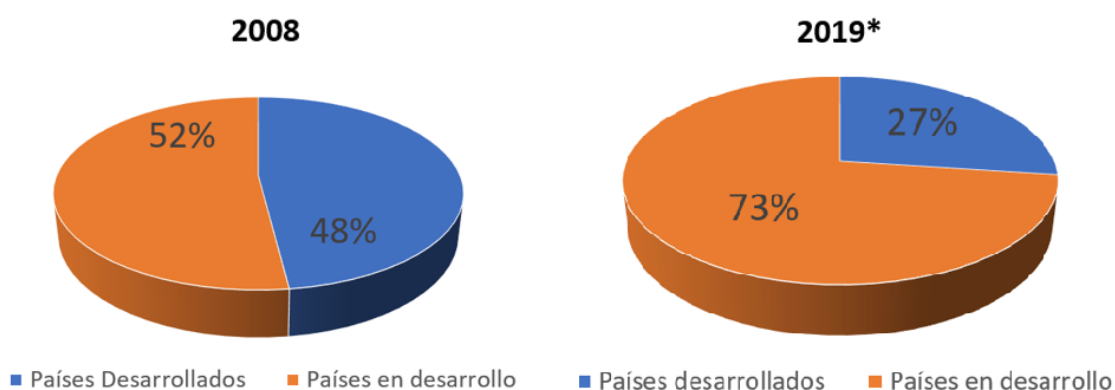


Fuente: ITU World Telecommunication/ICT Indicators database

millones de personas, frente a los 1.570 millones que lo usaron en 2008.

Del mismo modo, podemos observar en el siguiente gráfico que el número de usuarios en los países en desarrollo ha incrementado notablemente su porcentaje frente al total de los usuarios mundiales.

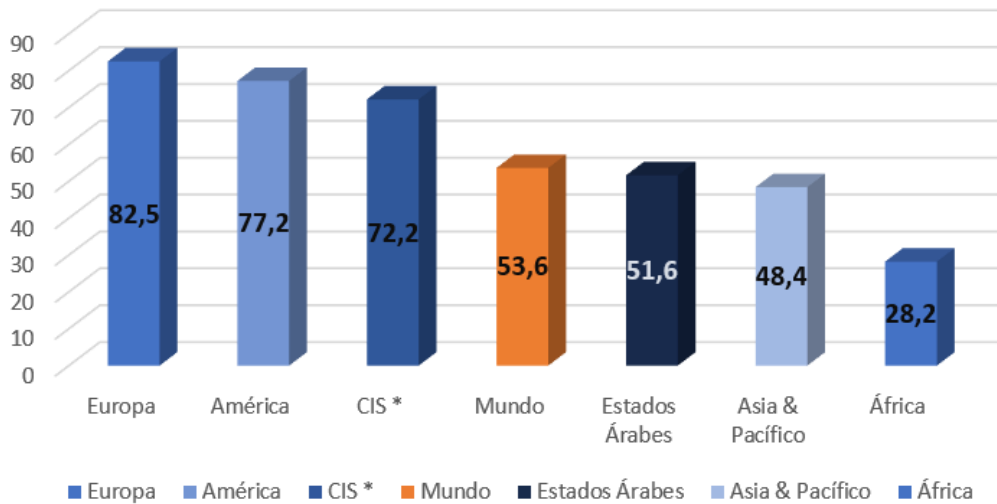
Individuals using the Internet, by level of development



The developed/developing country classifications are based on the UN M49, <http://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx.html>
 Note: * Estimate
 Source: ITU World Telecommunication /ICT Indicators database

No obstante, podemos observar en la siguiente imagen que las regiones cuyo número de usuarios de Internet es mayor siguen siendo aquellas dónde se encuentran los países más

Uso de Internet por cada 100 habitantes en 2019



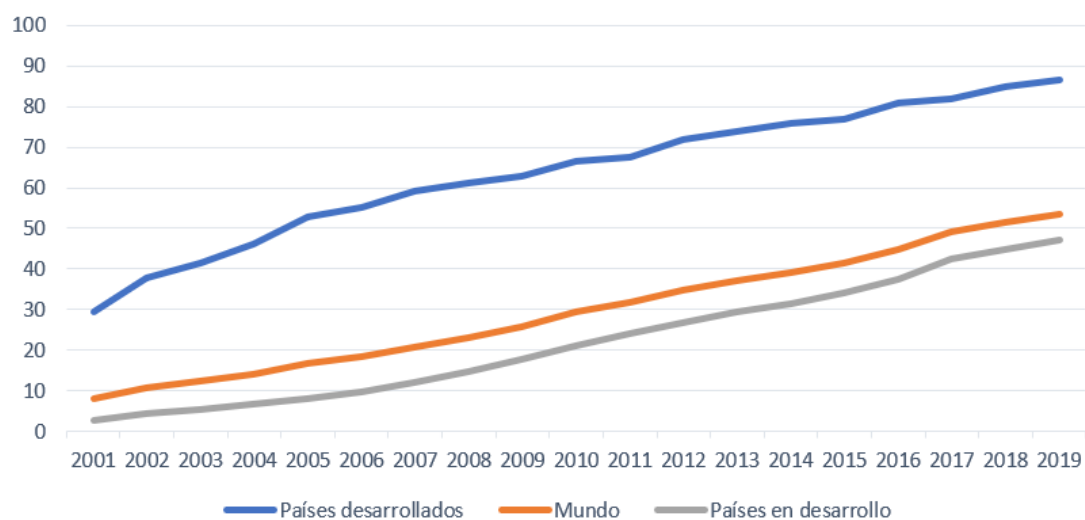
CIS *: Comunidad de Estados Independientes (*Commonwealth of Independent States*)

Fuente: ITU World Telecommunication/ICT Indicators database

desarrollados.

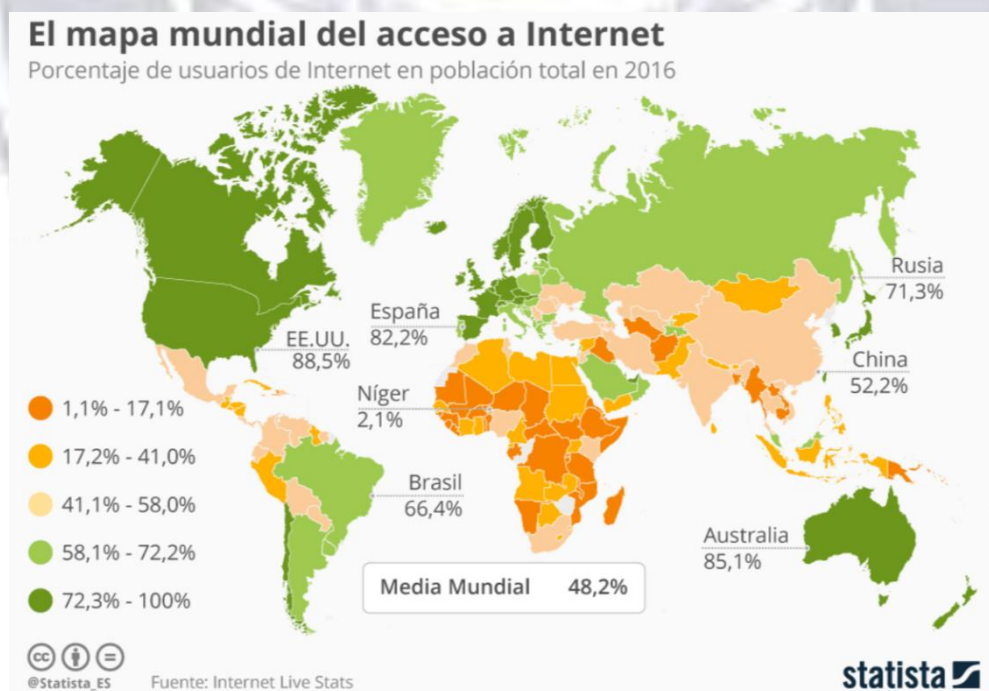
De esta forma, mientras que en los países desarrollados los porcentajes de población conectada a Internet son elevados, con casi cerca del 87%, los países menos desarrollados apenas llegan al 20%.

Uso Internet por cada 100 habitantes según el nivel de desarrollo del país



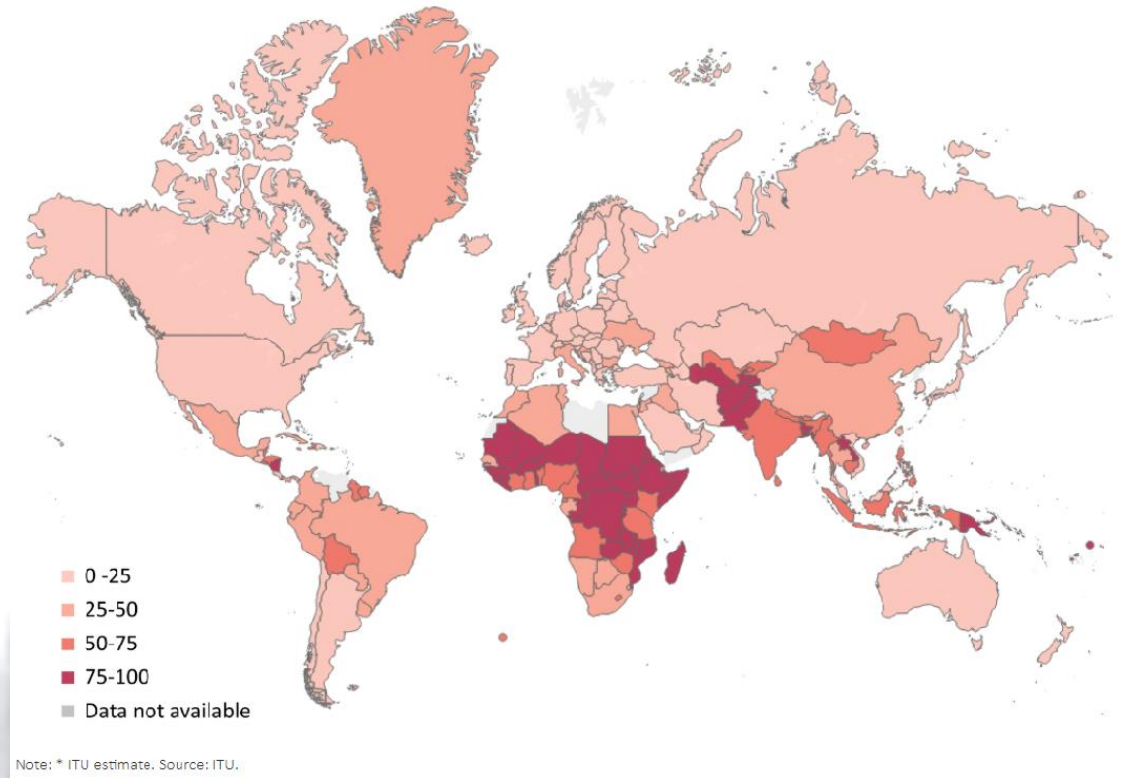
Fuente: ITU World Telecommunication/ICT Indicators database

Así, en el siguiente mapa se exponen los porcentajes de penetrabilidad de Internet por país en 2015:



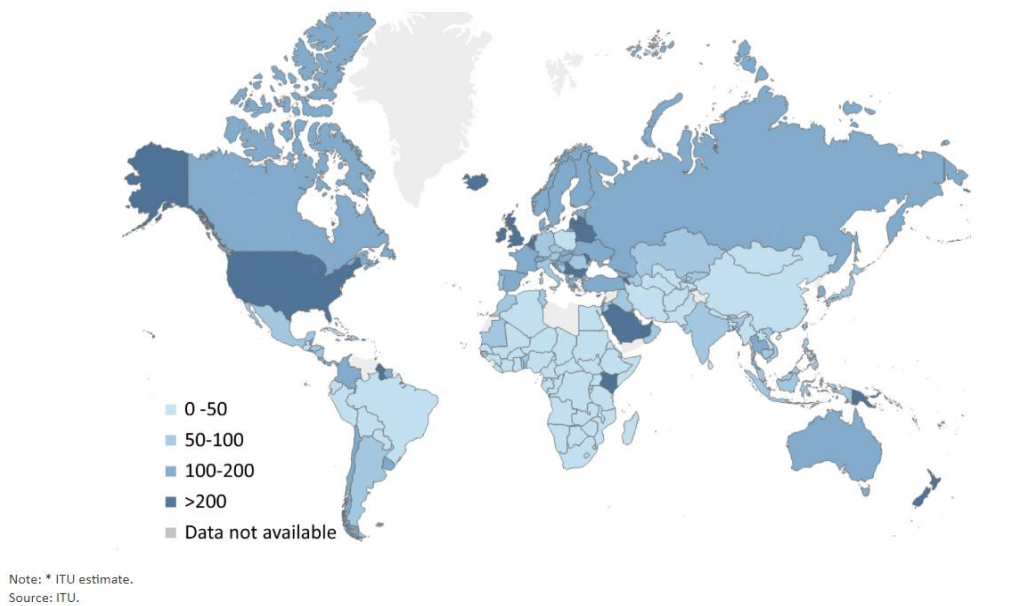
7 de febrero de 2020

Paralelamente, el siguiente mapa destaca las diferencias regionales en el uso de Internet, mostrando la cantidad de población que permanece aún desconectada. Las regiones que recogen las cantidades más elevadas de desconexión son principalmente África y Sur de Asia.

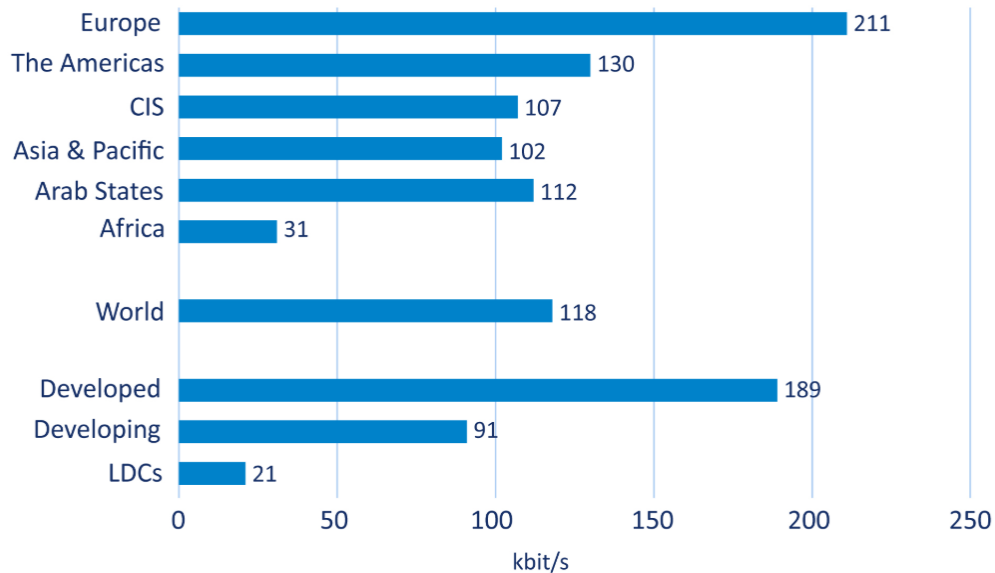


En contraste, podemos ver las regiones más conectadas de Internet:

International bandwidth usage per Internet user (kbit/s), by region 2019*



International bandwidth usage per Internet user (kbit/s), by region 2019*



Note: * ITU estimate.
Source: ITU.

En términos de Kbit/s consumidos por usuario de Internet, Europa es de lejos el mayor consumidor (211 kbit/s). África se queda atrás, con 31 kbit/s por usuario de Internet. Asimismo, según datos de la ITU el uso del ancho de banda internacional creció un 33,4% en promedio anualmente entre 2015 y 2019. A su vez, Asia y el Pacífico representan más del 40% del uso global, seguido de Europa (25%) y América (21%). Las otras tres regiones combinadas representan solo el 11% del total mundial.

Asimismo, las diferencias tecnológicas pueden propiciar nuevas formas de exclusión entre los que pueden o no pueden tener acceso a la información, es lo que se conoce como "pobreza informativa", una nueva forma de diferenciar a los países ricos de los países pobres.

En cuanto a los proveedores de contenido conviene destacar que aunque en principio cabría suponer que las tecnologías de información y de telecomunicación permitirían que cualquier empresa se pudiera localizar en cualquier lugar y proveer, desde allí, al mundo entero, la realidad demuestra que existe una gran concentración de la industria proveedora de contenidos de Internet, localizándose de forma prioritaria en las áreas metropolitanas de los grandes ciudades.

Esta situación puede suponer que los planes de negocio de las compañías suministradoras del servicio establezcan suplementos a determinados usuarios, en función del tipo de conexión a la que accedan. Esta estrategia comercial supondría que las rentas bajas accederían a una Red

hecha a imagen y semejanza de determinadas empresas, tal y como ya de hecho sucede en estados de África, Asia o América.

El riesgo es doble, por un lado las operadoras pueden ejercer un control sobre la Red que termine por desvirtuarla, pero también es cierto que las grandes proveedoras de contenidos pueden pactar con las primeras para acrecentar su poder.

De lo que no hay duda, es que esta vía generaría una mayor concentración y facilitaría acuerdos entre los gigantes que proveen de contenidos y las corporaciones privadas que suministran acceso a la Red. No se puede ignorar que el mercado de Internet está ya muy concentrado, lo que debería ser una preocupación para las autoridades:

- Google tiene cerca del 80% del “search advertising” (publicidad en motores de búsqueda); Además, posee el 97% de la cuota de búsqueda a través de móviles.
- Facebook y sus apéndices Instagram, WhatsApp y Messenger poseen el 77% del tráfico de las redes sociales en dispositivos móviles.
- Microsoft Windows es usado por el 90% de los ordenadores a pesar del Mac de Apple y Linux.
- Apple vía iTunes controla el 87% del mercado de descargas de música.
- El 90% de los beneficios de los smartphones se los reparten entre Apple y Samsung.
- Amazon tiene una cuota del 74% en el mercado de e-books.

En términos económicos clásicos estas empresas actúan en términos de monopolio, suponiendo un serio problema para la libre competencia.

En este sentido, se está generando una fractura digital entre aquellos que acceden o no a Internet y las condiciones de dichos accesos, de tal forma que los territorios no conectados a Internet pierden competitividad económica internacional y, por consiguiente, son bolsas crecientes de pobreza incapaces de sumarse al nuevo modelo de desarrollo.

En estos momentos, todo indica que la brecha digital entre los conectados y los que no lo están, sean Estados en vías de desarrollo o ciudadanos de los propios Estados que se han quedado al margen, se agranda.

1.3.2 Tipos de control

A medida que Internet ha ido ganando protagonismo, regímenes de todo tipo (democráticos, híbridos y autocráticos) han establecido políticas de creciente control y securitización de Internet, tal como reflejan los informes de «Freedom on the Net¹» (Freedom House,

¹ La metodología de «Freedom on the Net» incluye 21 macro-preguntas y cerca de 100 ítems, en tres categorías: 1) Obstáculos al acceso: barreras de infraestructura y barreras económicas al

2016). Asimismo, AccesNow corrobora esta tendencia afirmando que los cortes de Internet fueron 188 en 2018, lo que implica un 85% más que en 2017 y un 161% más que en 2016.

Los mecanismos de control de Internet varían según el tipo de regímenes políticos, de tal forma que, generalmente, cuanto más autocrático es el régimen más se observan controles de Internet de primera generación, censura de contenidos y violaciones a los derechos de los usuarios, mientras que en regímenes híbridos se observan más comúnmente controles de segunda generación, que involucran obstáculos al acceso, sin que se llegue al bloqueo de contenidos y a los apagones de la red.

Tras examinar los múltiples estudios de caso podemos afirmar que, con excepciones reconocidas por la Comunidad Internacional como es el caso de la India, cuanto más autoritario es un Estado más mecanismos de censura implanta, ejerciendo un alargamiento del control social que ya existe fuera del ciberespacio. Por el contrario, los Estados democráticos ejercen menos poder sobre Internet, ya que suele ser muy costoso en términos de reputación internacional y legitimidad interna.

Mecanismos de control de primera generación:

- Filtrado de palabras clave.
- Bloqueo de contenidos y de sitios web (bloqueo de URLs por DNS)
- Impuestos al uso de Internet.
- Requerimientos administrativos a los proveedores de acceso.
- Reportes policiales rutinarios de la actividad ciudadana en Internet.
- Actuaciones judiciales como consecuencia de por expresiones políticas en la web.

Asimismo, los países con regímenes autoritarios tienden a limitar el desarrollo de la infraestructura de acceso a Internet y a incrementar los controles sobre los proveedores de servicios, recurriendo a prácticas de control que no requieren mecanismos técnicos sino que se basan en mecanismos policiales, judiciales o administrativos.

acceso, control legal y de propiedad de los proveedores de servicios de Internet e independencia de los organismos reguladores; 2) Límites del contenido: regulaciones legales sobre el contenido, filtrado técnico y bloqueo de sitios web, autocensura, vitalidad y diversidad de los medios de comunicación en línea y el uso de herramientas digitales para la movilización cívica; 3) Violaciones de los derechos de los usuarios: vigilancia gubernamental, privacidad, repercusiones en la expresión y las actividades en línea, encarcelamiento, acoso extralegal o ciberataques.

7 de febrero de 2020

Los regímenes híbridos sólo utilizan mecanismos de control de primera generación en momentos de alta conflictividad política, especialmente si se producen protestas masivas que puedan amenazar su estabilidad.

El modelo del “dilema del dictador” teoriza que en regímenes híbridos, los mecanismos tradicionales de filtrado de palabras clave y bloqueo de contenidos son poco sofisticados y selectivos, aplicándose sólo en casos específicos para los cuales pueden legitimarse (ej. terrorismo, pornografía infantil), dichas restricciones podrían ampliarse en situaciones de protestas masivas, especialmente si dichas protestas son amplificadas por el uso de la web.

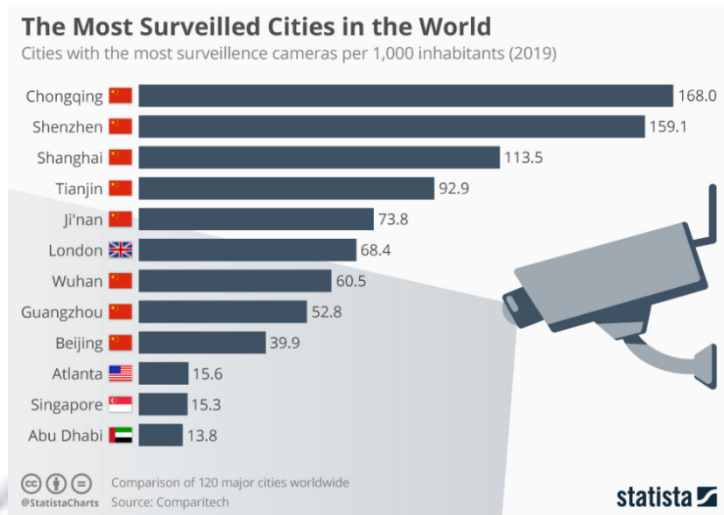
A partir de 2009 empezaron a generalizarse controles de segunda generación como:

- Restricción temporal de la conectividad en regiones en donde se producen protestas.
- Bloqueo just-on-time de aplicaciones móviles.
- Requerimientos informales de remoción de contenidos a los ISPs y a los administradores de sitios web.
- Ralentización de las conexiones en momentos de alta conflictividad política y establecimiento de altos costos de los servicios para limitar el acceso masivo a Internet.

Este tipo de control es propio de regímenes híbridos en los que también se recurre a ejércitos de botnets para inundar las plataformas de redes sociales con comentarios pro-gubernamentales, influir en discusiones en línea, reportar o atacar a quienes hacen comentarios antigubernamentales o simplemente publicar contenidos de desinformación.

También se pueden producir casos de monitoreo masivo, uso de información publicada en línea para hostigar o acusar legalmente a activistas políticos u otras formas de propaganda automatizada, así como ciberataques perpetrados contra activistas opositores o “*patriotic hacking*”.

Las tecnologías desarrolladas en la segunda mitad del siglo XX han propiciado la aparición de nuevas formas de control social. Uno de los aspectos novedosos es la sistematización de tecnologías de vigilancia que pretenden reemplazar progresivamente a la coerción física como medio para mantener el orden y la armonía de la población.



1.3.3 El Gobierno de Internet: Dinámicas globales vs. Dinámicas nacionales

Desde el principio Internet se ha ido gestionando de una manera autónoma e informal y, en la actualidad, la posición de gobierno la ejerce una institución privada sin ánimo de lucro que se ubica en California y que se encuentra bajo la tutela del Departamento de Comercio estadounidense, denominada “Internet Corporation for Assigned Names and Numbers” (ICANN) que tiene, entre otras cosas, la característica de que elige su consejo de administración ejecutivo por votación global entre una lista abierta, en la que puede inscribirse cualquier persona facilitando únicamente su correo electrónico. Esta autoridad es la que en principio distribuye los dominios, acuerda los protocolos, entre otras funciones.

En la actualidad, la posición preponderante de EEUU levanta recelos en un buen número de países, entre ellos Rusia, China, Brasil o India que parecen estar apostando por redes soberanas donde puedan ejercer un control directo tanto de los contenidos como del acceso a ellos.

Desde hace varios años se discute la posibilidad de que Internet sea administrada por cada gobierno en la esfera nacional, y por una organización como la Unión Internacional de Telecomunicaciones UIT perteneciente a la ONU, en el plano internacional, lo que facilitaría la adopción de decisiones de carácter multilateral.

Es evidente que el concepto tradicional de soberanía no alcanza para afrontar los efectos de la globalización, y es necesario adaptarlo partiendo de la premisa de que la “no territorialidad” es una característica fundamental de la “Red de redes”.

7 de febrero de 2020

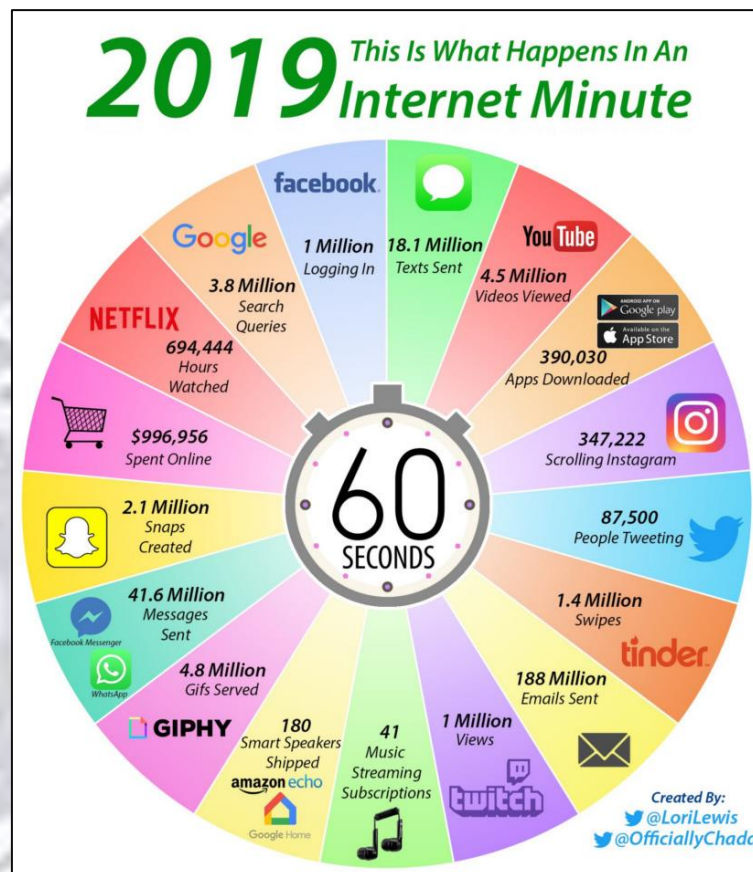
Los Estados deben enfrentarse al reto de legislar el ciberespacio y redefinir conceptos tan relevantes como los elementos que constituyen el Estado según Jellinek: Soberanía, ciudadanía o territorio; ya que si bien las nuevas tecnologías ofrecen la posibilidad de una optimización de la democracia, también representa la oportunidad para que los temas locales se conviertan en globales, haciéndose problemas generales.

A pesar de los intentos realizados a nivel institucional, la capacidad tecnológica de la legislación internacional es tan escasa que se multiplican las posibilidades de escapar a su control. La falta de uniformidad en las disposiciones legales y la carencia de fuerza coercitiva para su aplicación provoca que ningún Estado u organismo internacional cuente con la fuerza necesaria para controlar de manera eficaz la actividad en la red.



2. Estudios de Caso

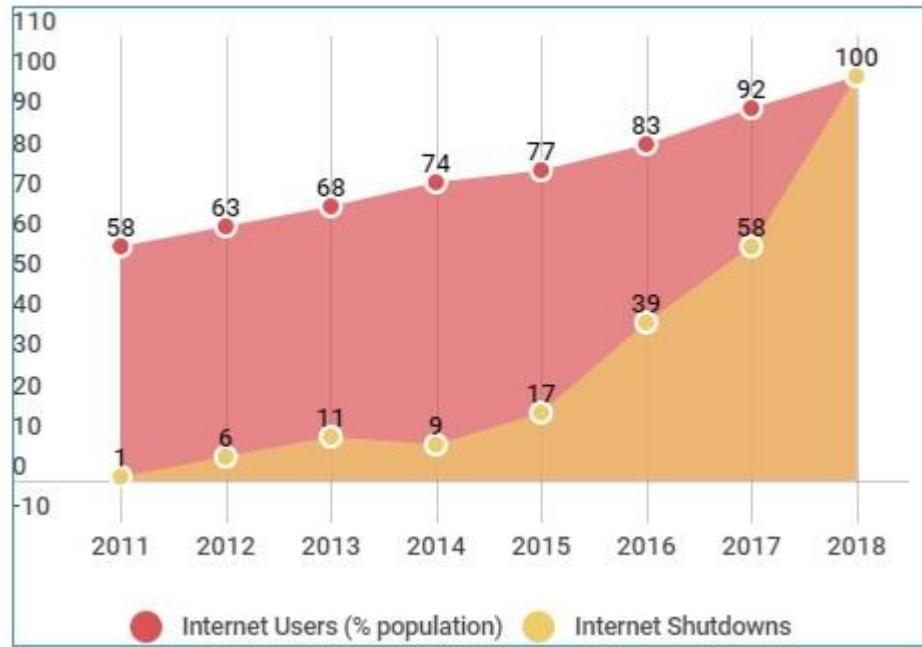
Desde 2014 hasta hoy el número de usuarios de Internet ha crecido de 2,95 billones a 4,42 billones, la velocidad de Internet alrededor del mundo está en su nivel más alto en la Historia, y sólo en un día hay más de 4 millones de publicaciones en blogs.



Sin embargo, esta mejora en la accesibilidad ha venido acompañada de nuevas herramientas para cerciorar los contenidos por parte de las autoridades gubernamentales a lo largo de todo el globo. Según el Informe *Freedom of the Net 2018* de Freedom House, 26 de 65 países han visto una disminución en la libertad de internet desde junio de 2017. “Los gobiernos más represivos están tratando de usar Internet para sus propios objetivos, lo que a menudo puede ser para reprimir la disidencia, silenciar a los periodistas, silenciar a la sociedad civil y controlar mejor a sus ciudadanos”, señala Allie Funk, analista senior de Freedom House y coautora del informe.

Para mostrar la dependencia de estos dos factores (la penetrabilidad de Internet y el crecimiento de la censura), el siguiente gráfico –de elaboración propia a partir de los datos proporcionados por Statista y el Informe sobre el Desarrollo Mundial de las

Telecomunicaciones de la Unión Internacional de Telecomunicaciones- muestra la comparativa entre el número de *Internet Shutdowns* llevados a cabo en el período 2011-2018 y la evolución del porcentaje a nivel mundial de los usuarios de Internet, respecto de la población total en cada período temporal.



China es la fuerza impulsora clave detrás de esta tendencia hacia el autoritarismo digital, pero no está sola. Los países del norte de África implementan cada vez más políticas cibernéticas al estilo chino: Nigeria promulgó recientemente medidas que requieren que los datos del consumidor se alojen dentro de sus fronteras y el año pasado Egipto aprobó una ley que le permite prohibir las cuentas de redes sociales con más de 5,000 seguidores si estas cuentas publican 'noticias falsas' o critican al gobierno. Mientras, en Asia se mantiene la misma tendencia: India -la mayor democracia del mundo- mantiene aislada a Cachemira, situándose como el principal Estado que promueve los cortes de Internet; mientras en Sri Lanka y en el Kazajistán se bloquean Redes Sociales y aplicaciones de mensajería para congelar los flujos de comunicación; y en Indonesia se reduce la velocidad de Internet al mínimo.

América Latina se apaga digitalmente mientras crecen los conflictos sociales, y en Europa se empiezan a implementar algunos filtros de acceso a la información, siguiendo el ejemplo de la NetzDG alemana, cuyo objeto es combatir la agitación y las noticias falsas en las redes sociales.

En este sentido, España tampoco queda al margen de las tendencias macro, publicando el pasado noviembre el Real Decreto-Ley 14/2019, *por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector*

público y telecomunicaciones. Si bien esta norma no permite el cierre gubernativo de servicios como Facebook o Telegram ya que tales servicios no pueden ser intervenidos por normativa europea, sí se contempla la posibilidad de ordenar -“sin audiencia previa” al interesado- el cese de la actividad de las redes de comunicación, cuando exista una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional.

En este escenario, la siguiente figura elaborada por Visual Capitalist a partir de los datos de Freedom House permite observar la comparativa entre los países más bloqueados y los menos, por regiones.

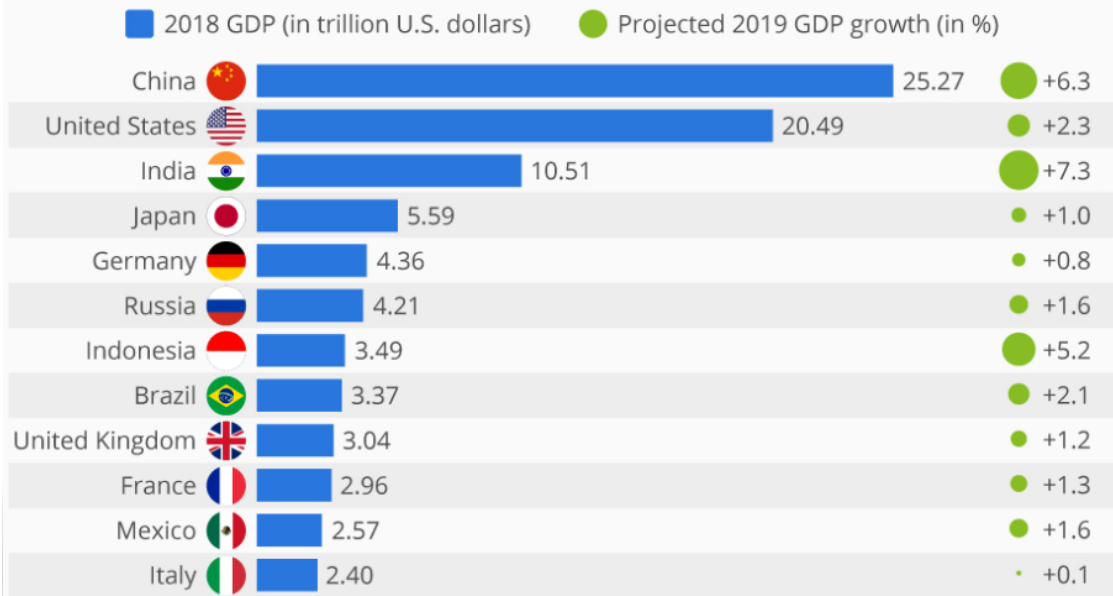


En definitiva; los gobiernos de todo el globo están reforzando el control sobre Internet y la tarea respecto las siguientes páginas radicarán en dibujar un diagnóstico adecuado. Para ello, tal y

como se anuncia anteriormente, se ha procedido a analizar pormenorizadamente tres grandes estudios de caso que por su influencia internacional son capitales para abordar esta cuestión: China, Rusia e Irán.

The Biggest Economies in the World

Countries with the biggest GDPs in the world and their growth outlooks



2.1 China

El resurgimiento de la Rusia post-comunista, la creciente tensión entre China –potencia emergente- y Estados Unidos –potencia todavía dominante-, la profunda transformación de Oriente Próximo a causa de las intervenciones militares occidentales y del germen sembrado por las Primaveras Árabes, los Estados Fallidos y la aparición de actores no estatales –como las organizaciones terroristas o las grandes multinacionales digitales- prueban que no hubo “Fin de la Historia”.

Por el contrario, como señala Manuel Montobbio, hoy vivimos una era de cambio y un cambio de era, determinado por la globalización de la Sociedad de la Información y sus efectos, así como por el desplazamiento del centro de gravedad global hacia Asia-Pacífico y la emergencia simultánea de China y la India.

La República Popular fundada bajo el liderazgo de Mao Tse-tung en 1949 celebró el pasado 1 de octubre de 2019 su 70º aniversario, siendo su potencial a escala global indudable, pues en palabras de Martin Wolf “cuando China estornuda la economía mundial se enfría”. No obstante,

mientras detenta una posición privilegiada en el ascenso hacia el liderazgo económico y tecnológico, existe una percepción generalizada sobre que la llegada al poder de Xi Jinping ha producido una involución en lo que se refiere a la evolución política, los Derechos Humanos y las Libertades Civiles, retrocediendo incluso en la reforma iniciada en 1978 bajo el impulso de Deng Xiaoping para poner en marcha un proceso de separación paulatina entre el Estado y el Partido.

Debido a ello, recientemente China ha sido definida por la Comisión Europea en su Informe de 12 de marzo “EU-China-A strategic Outlook”- preparatorio para el Consejo Europeo del 21 y 22 de marzo-, como “un competidor económico en busca de liderazgo tecnológico” y “un rival sistémico que promueve modelos alternativos de gobernanza”; conceptos que definen su ascenso hacia el liderazgo internacional económico y tecnológico mientras plantea dudas en la consolidación de su identidad global al no tratar de activar procesos de democratización.

En este contexto, el ciberespacio se ha establecido como una dimensión configurada para ejercer poder, convirtiéndose en otra herramienta geoestratégica del autoritarismo chino. Tras un exhaustivo análisis se ha observado que existen 4 grandes formas de influencia:

- Desarrollo de infraestructuras en otros países: A través de la iniciativa *Belt and Road*, China está suministrando a muchos países no solo carreteras y ferrocarriles, sino también infraestructura avanzada, como redes de banda ancha y centros de datos. En febrero, el gigante tecnológico chino Huawei abrió su primer centro de datos en la nube en Egipto. Mientras tanto, en Marruecos, China está ayudando a construir la muy esperada ciudad inteligente *Tangier Tech*, que albergará a 200 empresas chinas. Queda patente, entonces, que China no sólo está desarrollando una política de expansión tecnológica, sino que trata de exportar una visión global de cómo debería funcionar Internet en la totalidad de los Estados; defendiendo la soberanía cibernética o digital como reflejo del derecho de cada país a elegir cómo gobernar su Internet.
- Los ataques cibernéticos que desarrolla hacia otros Estados u Organizaciones, como por ejemplo el descubierto en 2009 por el Information Warfare Monitor -iniciativa canadiense formada por SecDevGroup y Citizen Lab-, denominado *GhostNet*.
- La obligación de las empresas tecnológicas chinas a facilitar la información obtenida al gobierno –como señalaba Robert Strayer, Subsecretario Adjunto de Cibercomunicaciones, Comunicaciones Internacionales y Política Informativa de la Oficina de Asuntos Económicos y Empresariales del Departamento de Estado de EE.UU., el pasado 26 de febrero de 2019, en el Mobile World Congress celebrado en Barcelona.

- La censura que promueve China dentro de su soberanía, conducente a la construcción de un Estado digital autoritario, apoyado complementariamente en un sistema de crédito social, y en la que nos centraremos específicamente debido a la temática particular de este trabajo.

Así, el primer elemento al que debemos aludir, es el técnico:

La evolución desde la implementación del primer proyecto piloto de Internet en China en 1989, pasando por su expansión nacional en 1994 hasta la actualidad, donde cuenta con 730.723.960 usuarios según datos proporcionados por la CIA, ha sido larga y compleja.

En 1997, Beijing promulgó sus primeras leyes relativas a la penalización de contenido en línea considerado perjudicial para la seguridad nacional o los intereses del Estado, y poco después inició el Proyecto *Golden Shield*, centrado en mejorar la seguridad de la red; cuyo desarrollo proporcionaría las bases del posterior *Great Firewall of China*. Si bien múltiples figuras políticas se mostraron escépticas ante la idea de prohibir la influencia de las creencias occidentales en la ideología comunista a través de este instrumento –llegando a ser comparado con “tratar de clavar gelatina en la pared” por Bill Clinton- en la actualidad podemos afirmar que el Gran Cortafuegos Chino, ha supuesto la construcción de un mundo virtual propio, limitando los flujos de información entre el interior y el exterior y, por lo tanto, determinando el abanico de fuentes a los que la ciudadanía china puede acceder.

Asimismo, en la actualidad el Gobierno de China controla a todos los proveedores de Internet a través de su autorización y control por el Ministerio de Industria y Tecnología de la Información, tanto en el interior como en el exterior del país. Bajo el Gran Cortafuegos Chino se utilizan técnicas como el filtrado de URLs –bloqueando las webs que contienen palabras clave como “Tiananmen”-; el envenenamiento de DNS ejecutando la inaccesibilidad a determinadas webs; la autocensura tanto de las personas a título individual como de empresas u otras organizaciones; el bloqueo de redes privadas virtuales (VPNs) –como en la muerte del ganador del Premio Nobel de la Paz Liu Xiaobo en julio de 2017 o durante el XIX Congreso Nacional del Partido Comunista de China en octubre de 2017-; o la aplicación manual o automatizada de monitoreo de contenido en línea.

En este sentido James Griffiths, autor de *The Great Firewall of China*, considera que es el sistema más sofisticado del mundo dedicado a la vigilancia y la censura en línea, pues no sólo bloquea el propio contenido que se considera “perjudicial” sino que de forma automatizada puede bloquear las herramientas que tratan de obviar dicha censura. Así, afirma, a nivel local, Beijing confía en las empresas tecnológicas nacionales para censurar y encuestar a los propios usuarios. Están obligados legalmente a entregar datos a las autoridades cuando se les solicite, y se espera que sigan reglas no escritas y eviten líneas rojas invisibles sobre qué censurar, lo que significa más error por el lado de la censura excesiva para que no sean castigados”.

El segundo de los elementos a analizar son los motivos actuales que han llevado a China a no sólo mantener su Gran Cortafuegos, sino a hacerlo más eficaz a través de la Inteligencia Artificial. En este sentido, las declaraciones realizadas alrededor del 19º Congreso Nacional del Partido Comunista de China y traducidas por la fundación *New America* revelan que el régimen chino concibe como una sola entidad la seguridad informática y la información, así como una planificación, implementación y promoción unificada.

No obstante, se puede aludir a los dos principales motivos subyacentes que coexisten bajo la dialéctica gubernamental:

- I. Teniendo en cuenta que en las regiones rurales e inestables como Xinjiang, los medios de comunicación en línea son muy analizados en comparación con las ciudades desarrolladas, como con Shanghai –entorno económico chino por excelencia-, se puede deducir que existe un amplio CONTROL POLÍTICO interesado en evitar posibles conflictos cuyo flujo de comunicación es Internet.

Como muestra de ello, se puede señalar el bloqueo de Facebook, Twitter, o Bing, entre otras aplicaciones por parte del gigante asiático a raíz de una movilización pacífica iniciada por una minoría musulmana que se propagó por redes sociales, se convirtió en masiva, y terminó en una manifestación sangrientamente reprimida en Xinjiang en 2009.

De igual modo, este control político a través de la censura digital está configurado para dominar el discurso por parte del Gobierno chino frente a la diversidad de actores de la Sociedad Civil. Sirva de ejemplo el cierre de a Youtube en marzo de 2008, después de que grupos tibetanos colgasen material gráfico de la represión de las protestas de Lhasa, capital de Tibet; mientras que las televisiones chinas difundían imágenes de grupos tibetanos atacando tiendas y quemando coches de policía.

- II. Paralelamente, se encuentran los motivos derivados del CONTROL SOCIAL, pues tras la obstrucción a los sitios de redes sociales extranjeras, la ciudadanía china adopta nuevas herramientas –esta vez de corte local- como Youku y Sina Weibo, donde la censura y la propaganda pueden ser fácilmente reforzadas. En este sentido, en enero de 2018, la plataforma Weibo suspendió varios de sus programas más populares después de que las autoridades le ordenaran que limpiara información “mal orientada” y “vulgar”, mientras que en abril cerró Neihan Duanzi, una aplicación de parodias con más de 38 millones de usuarios mensuales.

Finalmente, el tercer elemento en el que se debe incidir es el estado actual de la cuestión y cuáles son las posibles posturas al respecto. Si bien algunos autores proponen un modelo de *decoupling* que abogaría por la separación radical entre los grandes sistemas económicos y

tecnológicos aislados entre sí, lo cierto es que esta idea camina lejos de la interacción económica entre las naciones como fuente de crecimiento y del multilateralismo que el mundo espera de los líderes del futuro.

En esta línea, Tuo Zhen, portavoz temporal de la fuerza política que gobierna desde 1949 afirmó en el 19º Congreso Nacional del Partido Comunista de China que “no copiarán ni replicarán modelos de otros países” pero que mantendrán la apertura económica. Esta poderosa idea, sustentada en el concepto de desarrollo modernitario –modernización impulsada por regímenes autoritarios- es peligrosamente compartida por Rusia, y parece que se consolidará como uno de los grandes reto a enfrentar desde la óptica occidental del globo para esta nueva década que empieza. Pues, como nos recuerda Enrique Fanjul, gestionar el ascenso de China, facilitar su acoplamiento en el mundo, es posible e imprescindible para la estabilidad del mismo.

2.2 Rusia

1.3.1 Aparición y evolución de Runet

Rusia Runet es el término común que se utiliza para referirse a la parte de Internet dedicada a usuarios rusoparlantes.

En términos generales, en Rusia la industria de Internet se ha desarrollado de forma autosuficiente e independiente de las grandes compañías de tecnología estadounidenses. Empresas como Google o Facebook tienen una presencia notable en el país, pero no han llegado a dominar el mercado y son empresas rusas las que copan las herramientas de búsqueda, las redes sociales y los correos electrónicos.

La presión ejercida durante la primera década del siglo XXI contra los medios de comunicación tradicionales (televisión, radio, prensa,...) provocó que los medios digitales ganaran influencia, ya que era el único espacio en el que la prensa tenía posibilidades de ser libre. Buenos ejemplos de esta situación fueron Gazeta.ru o Lenta.ru, Odnoklassniki y Vkontakte².

Desde su creación, Runet ha sido un espacio libre e independiente, pero al comienzo de la década el poder político decidió actuar y ejercer su control, limitando la libertad de la red, coartando cualquier posibilidad de disentir y creando todo un compendio normativo que bajo una apariencia garantista, permitiera restringir la capacidad informativa.

² En mayo de 2014, Vkontakte tenía más de 250 millones de usuarios registrados y 60 millones de visitantes únicos al día, un éxito que hizo que la red fuera traducida a más de 50 idiomas. Era la red de la gente joven, interesada en política.

Como señala Zvereva, las medidas de control del Estado ruso sobre Runet tenían dos objetivos, por un lado se intenta controlar las corrientes de información para prevenir una posible revolución interna y por otro lado limitar la influencia extranjera sobre Runet.

En 2008, Facebook entró en el panorama de las redes sociales rusas con su versión en idioma ruso. Las redes sociales ganaron importancia como agentes del debate político, dando poder a la ciudadanía. La respuesta político-estratégica de Rusia fue desarrollar un Internet propio – Runet– que pudiera funcionar independientemente de servidores extranjeros, con el propósito de defender al país de posibles ataques cibernéticos. Tal como lo expresó el senador Andrey Klishas del Partido Rusia Unida, “Estados Unidos tiene la capacidad técnica de desconectar a Rusia de los servidores principales; en otras palabras, Internet dejaría de funcionar en Rusia, y como Estados Unidos cree que no tiene límites cuando se trata de sus intereses nacionales, Rusia como Estado soberano debe dotarse de los recursos técnicos para contrarrestar esas amenazas (France24, 18/05/2019).

La intervención del Gobierno ruso empezó en diciembre de 2011, cuando se celebraron las elecciones parlamentarias de Rusia. Las redes sociales se llenaron de vídeos y fotos que mostraban fraudes masivos, organizándose, a través de las redes sociales (Facebook y Vkontakte), acciones de protesta que tuvieron lugar a lo largo del siguiente año y medio.

De forma progresiva el gobierno ruso fue aprobando una serie de medidas legislativas dirigidas a ampliar el control de la red:

- Enmiendas al Código Administrativo y la Ley de Reuniones, Mítines, Manifestaciones, Marchas y Piquetes. El documento multiplicó las multas por acciones de protesta masivas.
- Ley de bloqueo de sitios webs, que permitía al Gobierno ruso el bloqueo inmediato de contenidos relacionados con “pornografía infantil”, “propaganda de drogas” y “suicidio”. Las webs con contenido prohibido, según la ley, debían ser incluidas en la “lista negra”, después de que el proveedor tuviera 24 horas para informar el propietario de la página y demandarlo. Desde ese momento, el propietario tenía otras 24 horas para eliminar el contenido sospechoso. Si no lo ejecutaba, pasado ese tiempo, el proveedor debía bloquear la página prohibida. De esta manera, la ley permitía bloquear un sitio web en tres días.
- Entrada en vigor de la “lista negra”, en la dirección zapret-info.gov.ru. Muchos periodistas lo llamaron el “cortafuegos ruso” y sospecharon que, con el pretexto de protección contra la pedofilia, la ley sería utilizada para bloquear toda clase de sitios webs.
- Normativa que coartaba la libertad digital, penando con hasta cinco años de prisión opiniones críticas con la anexión de Crimea, tendiendo –en palabras de Volkov- al modelo chino.

7 de febrero de 2020

- Enmiendas a la ley sobre información, que permitían al Gobierno poder restringir el acceso a una amplia gama de recursos informativos, entre ellos, sitios webs en los que *“se propaguen llamamientos a los disturbios, actividades extremistas y participación en actos públicos masivos”*. El bloqueo de las páginas podría ser realizado en tan solo 15 minutos: las enmiendas liberaron al Gobierno de la necesidad de esperar una decisión judicial, como ocurría anteriormente, para impedir que se usara Internet con fines “extremistas”. Utilizando esta normativa se bloquearon el medio digital Lenta. ru. , las páginas webs de carácter opositor Grani. ru, Kasparov.ru y Ej.ru. y diversos blogs.
- Ley de información personal, que con el pretexto de la lucha antiterrorista, introdujo medidas de control del ciberespacio, con dos innovaciones importantes, una de las cuales estaba relacionada con el control de los usuarios rusos en plataformas extranjeras, exigiendo a los “organizadores de la difusión de la información en la web” guardar la información sobre “los hechos de la recepción, transmisión, entrega y procesamiento de voz, escritura, imágenes, sonidos u otros modos de mensajes digitales”, así como información sobre los propios usuarios, durante los seis meses posteriores a su creación en el territorio ruso. Los medios de comunicación interpretan las nuevas enmiendas como el paso hacia el control de las publicaciones en Facebook, Google y Twitter.

La segunda innovación introducida por las enmiendas afectaba directamente a los blogueros y su libertad de expresión. La ley iguala a los blogs con más de 3.000 visitantes diarios con los medios de comunicación. Así, la página de cualquier bloguero podría ser cerrada por las mismas razones que los medios: información extremista, propaganda de homosexualidad, información sobre suicidio o drogas.

- Ley de responsabilidad penal contra “la exaltación del nazismo y la divulgación de informaciones falsas sobre la actuación de la Unión Soviética en la Segunda Guerra Mundial”. La nueva norma preveía la imposición de multas para quienes profanen monumentos relacionados con la gloria militar y efemérides de la Federación de Rusia.

Los cambios legislativos se realizaron tanto para controlar la información hacia el exterior, como la información hacia el interior, estableciendo los medios de comunicación como un sector estratégico orientado a “la defensa del país y la seguridad del Estado” (Sánchez y Tarín, 2018).

En este sentido, el gobierno ruso trató de desarrollar y fomentar Runet como un medio encargado de difundir la cultura y la lengua rusa en Internet, detallando que: “...el establecimiento del control estatal sobre ella [Runet], es necesario para crear lo que las autoridades rusas consideraban un Internet «seguro»”.

En resumen, podemos citar el artículo publicado por el periódico Kommersant, el 29 de abril de 2014, en el que mantenía que “Runet está siendo preparado para el control total, ya que las

autoridades rusas se encuentran en proceso de elaboración de un paquete de herramientas de control para los proveedores web. Quieren controlar los contenidos digitales en todos los niveles y prohibir la posibilidad de localizar los servidores DNS del dominio .ru fuera de Rusia”.

1.3.2 Tipos de control en Runet

De este modo, todas las medidas legislativas desarrolladas por el gobierno ruso han permitido la materialización de los siguientes tipos de control:

➤ **Control de Primera Generación:**

Los controles de primera generación se centran en negar el acceso a recursos específicos de Internet, bloqueando directamente el acceso a servidores, dominios, palabras clave y direcciones IP.

Este tipo de filtrado generalmente se logra mediante el uso de software especializado o implementando instrucciones manualmente en enrutadores.

Los controles de primera generación se practican monitoreando la red y desarrollando listas de bloqueo, que luego se transmiten a los ISP individuales que implementan el bloqueo contra los recursos específicos o nombres de dominio.

Una segunda práctica asociada con el bloqueo de primera generación es la vigilancia de cibercafés., que deben notificar los usuarios que intentan acceder a sitios prohibidos.

➤ **Controles de segunda generación**

Los controles de segunda generación tienen como objetivo negar el acceso a los recursos de información cuando sea necesario, especificando las condiciones bajo las cuales se puede denegar el acceso.

Las capacidades técnicas típicas de los controles de segunda generación están orientadas a desarrollar sus efectos "justo a tiempo" contra contenidos o servicios seleccionados (por ejemplo, durante las elecciones o manifestaciones públicas).

Estas tecnologías, a veces, pueden ser difíciles de verificar, ya que pueden parecer errores técnicos y se suele recurrir a ellas utilizando como pretexto la Seguridad Nacional, sobre todo en momentos de disturbios sociales para bloquear contenidos y servicios específicos de Internet.

Una de las técnicas más comunes implica solicitudes formales e informales a los ISP, de tal forma que estén bajo presión constante para cumplir con las solicitudes del gobierno, bajo amenaza de enfrentarse a posibles sanciones si no lo hacen o incluso la revocación de sus licencias. Tales presiones los hacen vulnerables a las solicitudes de las autoridades, especialmente las que se transmiten informalmente.

Cabe destacar que en Rusia, el nivel superior de los ISP está en manos de grandes compañías de telecomunicaciones, como Trans-TeleKom y Rostelecom, con fuertes lazos con el gobierno. Estos proveedores dan respuesta a solicitudes informales para hacer que cierto contenido sea inaccesible, según le interese al Estado, alegando cuestiones técnicas.

Otros medios técnicos menos sutiles pero efectivos incluyen la limitación de acceso a contenidos, así como servicios de telecomunicaciones seleccionados, como servicios de telefonía móvil y, especialmente, servicios de mensajería móvil o cortes temporales de Internet.

Las técnicas de segunda generación también hacen un uso extensivo de los ataques a la red informática, especialmente el uso de ataques distribuidos de denegación de servicio (DDoS), que pueden abrumar ISP y sitios seleccionados, y que dificultan el rastreo de los perpetradores, ya que los ataques son vendidos como diseñados por "hackers".

➤ **Controles de tercera generación**

A diferencia de las dos primeras generaciones de controles de contenido, los controles de tercera generación requieren un enfoque multidimensional altamente sofisticado para mejorar el control estatal sobre ciberespacio nacional.

Los controles de tercera generación incluyen mejorar la jurisdicción sobre el ciberespacio nacional, expandiendo los poderes de vigilancia estatal.

La característica clave de los controles de tercera generación es que la atención no se centra en negar el acceso, sino en desarrollar campañas efectivas de contrainformación, que abrumen, desacreditan o desmoralizan a los oponentes.

Los controles de tercera generación también se centran en el uso activo de vigilancia y minería de datos, como medios para confundir a los oponentes e incluyen el monitoreo sin orden judicial de usuarios de Internet.

La nueva legislación desarrollada en Rusia permite controlar todo el tráfico de Internet y el uso personal sin necesidad de orden judicial. Desde 2008, Rusia amplió los poderes previamente establecidos que obligaba a los ISP a comprar e instalar equipos que permitan la supervisión de la actividad de Internet de usuarios específicos.

Otros aspectos de los controles de tercera generación son difíciles de documentar, ya que utilizan vigilancia, interacción y acción física directa para lograr una interrupción de redes objetivo. La fuente final de estas campañas también es difícil de atribuir y solo puede establecerse mediante una cuidadosa investigación o conocimiento interno, ya que están diseñados para esconder el papel de los actores estatales.

El objetivo de estas campañas es efectuar cambios cognitivos en lugar de negar el acceso a línea de información o servicios.

Estas técnicas incluyen el empleo de " Brigadas de Internet " para involucrar, confundir o desacreditar a personas o fuentes. Dicha acción puede incluir la publicación de propaganda y desinformación a través de blogs masivos y participación en encuestas de Internet.

1.3.3 Evaluación de los controles

Las tres generaciones de controles no son excluyentes y pueden coexistir varias actualmente.

La confluencia de los controles de segunda / tercera generación y la legitimación de la vigilancia están contribuyendo a desarrollar un ciberespacio más regulado y menos espontáneo que el que existía en el pasado.

El crecimiento de los controles de segunda y tercera generación se ha producido como consecuencia de la creciente importancia de la seguridad cibernética como un dominio de acción militar.

A parte de la posibilidad de desarrollar mayores técnicas de control directo, existe un riesgo mayor de que los controles deriven hacia estrategias que buscan competir y dominar a los oponentes a través de campañas de desinformación, intimidación y otras tácticas diseñadas para dividir, confundir, y deshabilitar.

Rusia, China y los Estados Unidos han desarrollado todas las doctrinas y capacidades para la operar en el ciberespacio y esto incluye ataques a la red informática, así como operaciones diseñadas para dar forma al dominio a través del filtrado selectivo, denegación de acceso a la información y el compromiso de información.

2.3 Irán

La República Islámica de Irán contaba con 56,7 millones de internautas en 2017, el 69,1% de su población, y 40 millones de usuarios de Facebook. Según datos de la Unión Internacional de Telecomunicaciones el 72,8% de las familias iraníes tienen acceso a Internet.

Desde que el primer nodo de Internet se implantara en Irán en el año 1993, el uso de Internet ha ido creciendo paulatinamente, siendo sólo superado en la actualidad por Israel en términos de penetrabilidad y acceso a Internet en el conjunto de la región de Oriente Medio.

Dado que gobierno iraní históricamente se ha caracterizado por llevar a cabo prácticas limitadoras de la libertad de prensa y de la información en general, son muchos los usuarios que vieron una oportunidad para superar el bloqueo en esta nueva herramienta. Por ello, a partir de 2006, Irán empezó a restringir el acceso y desarrollar la censura informativa también en Internet.

7 de febrero de 2020

Actualmente, la regulación de Internet en Irán es extremadamente compleja e involucra un amplio abanico de actores. El ya mencionado Gobierno, el poder judicial, los líderes religiosos, los partidos políticos, las empresas, los activistas opositores, entre otros, ejercen presión para bloquear o desbloquear determinadas redes sociales. Asimismo, el Consejo Supremo del Ciberespacio - dentro del poder judicial- define y determina el contenido criminal en la web.

Por su parte, las instituciones sociales más islámicas y conservadoras del establishment iraní se decantan por políticas más restrictivas. El ayatolá Ali Khamenei desarrolla una profunda observación sobre el tráfico digital y aboga por fuertes políticas de censura.

Ello ha conllevado la existencia de un amplio mercado cuyo producto son VPNs y productos análogos para poder superar los bloqueos.

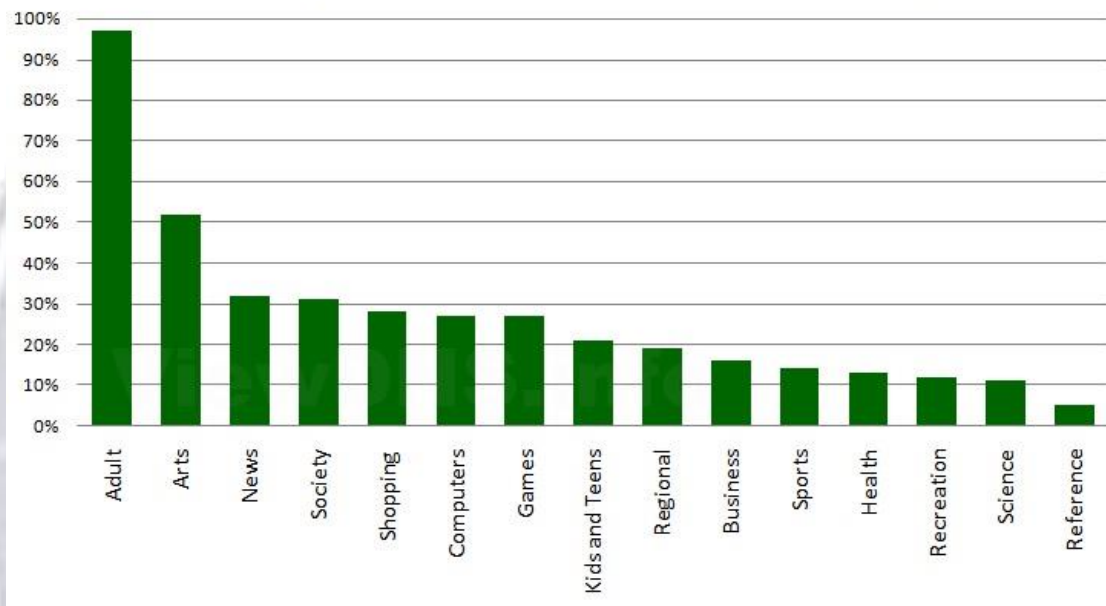
Asimismo, desde el 15 de noviembre del pasado año se vienen produciendo manifestaciones y protestas en las principales ciudades del país, encendidas a raíz del aumento del precio de los combustibles y que han desembocado en la crítica hacia el gobierno de Hasán Rohaní, así como en la ampliación de demandas hacia una mayor libertad política. El derribo del vuelo 752 de Ukraine International Airlines el 8 de enero alimentó dicho descontento social, sumado al malestar causado por la situación económica y al poder desmesurado que la Guardia Revolucionaria Iraní ejerce a lo largo del territorio y en una amplitud de esferas del Estado iraní.

Si bien esta oleada de movilizaciones no es nueva, sino que viene procedida por las de 2016 –la llamada Revuelta del Día de Ciro el Grande- las de 2017 y 2018, así como por las huelgas generales de los últimos dos años, en este último ciclo 2019-2020 la violencia ha aumentado, reprimiendo las marchas y concentraciones con mayor contundencia. Ejemplo de ello, son los disparos con munición real efectuados contra los manifestantes en ciudades como Isfahan, Behbahan y Shiraz, o el encarcelamiento de más de 6.000 opositores. En este sentido se ha pronunciado Ebrahim Raisi, presidente del Tribunal Supremo, quien ha advertido de que el peso de la ley se aplicará con severidad, incluyendo la pena de muerte. En la misma línea se han pronunciado otras autoridades, entre ellas Abdolreza Rahmani Fazli –ministro de Interior-, Mahmoud Alavi –ministro de Inteligencia-, y Mohammad Javad Azari Jahromi –ministro de Información y Tecnologías de la Comunicación; ambos tres agentes activos en el ahogamiento del movimiento opositor iraní.

Así, su modelo de represión y censura combina tácticas en el ciberespacio y en el terreno tradicional, combinando tres niveles de control: el policial, el judicial y el informativo. Desde la óptica policial, Abdolreza Rahmani Fazli y Hossein Ashtari se ocupan de las detenciones en las manifestaciones así como del uso de la violencia encaminada a disolverlas. Gholamreza Soleimani es quien lidera el apoyo de los voluntarios Basij, ya movilizados para dispersar las movilizaciones de 2009. Paralelamente, desde el plano de la información son los Servicios de Inteligencia iraníes los que se infiltran en los círculos de opositores tanto en el exilio como en el interior del país. Una forma de proceder que se complementa con inteligencia de señales, tanto para captación, como para bloquear información o rastrear opositores.

Por ahora, la figura clave de los bloqueos en Internet es Azari Jahromi, cuya política de acceso a la información incluye imposibilitar la entrada a plataformas digitales y redes sociales, así como la prohibición de usar la tecnología necesaria para sortear los filtros y muros de la Red Nacional de Información de Irán –denominada NIN–, que funciona como una intranet centralizada y redirige el tráfico de Internet a través de servidores nacionales operados por empresas de telecomunicaciones controladas. De esta forma, la Administración y las terminales mediáticas pro-régimen pueden seguir conectadas mientras que los opositores pierden un canal fundamental que se convirtió en una herramienta clave de la Sociedad Civil a partir de las Primaveras Árabes.

Percentage of Websites Blocked in Iran by Category



3. Motivos de la censura y el bloqueo en Internet

La concatenación de los tres grandes casos presentados, junto al examen -en menor nivel- de 15 países adicionales ha permitido establecer una primera clasificación de los motivos para censurar Internet. En todo caso, se debe puntualizar que la exposición de los siguientes motivos no supone que sean excluyentes, puesto que numerosas ocasiones concurren con simultaneidad en el mismo territorio nacional.

3.1 Censura y bloqueo en relación a la Comunidad LGBTI:

La cancelación del estreno de la película *la Bella y la Bestia* en Malasia por parte de Disney en 2017 por negarse a la censura exigida por el presidente de la Junta de Censura de Películas, Abdul Halim Abdul Hamid, o la eliminación de una imagen mostrando un beso entre dos hombres en la edición del *International New York Times* distribuida en Pakistán, son dos de los ejemplos de la limitación de la libertad de expresión relativa a la Comunidad LGBTI y de la filtración de información neutral o positiva a la población.



Esta censura varía de grado según el Estado analizar; si bien tiene una mayor penetración en las regiones de Oriente Medio, Asia y África, según indica el Informe “Homofobia de Estado” en su edición 2019, publicado por la *International Lesbian, Gay, Bisexual, Trans and Intersex Association* (ILGA). En términos generales hay 70 Estados Miembro de la ONU (35%) que penalizan los actos sexuales consensuales entre personas adultas del mismo sexo, además de otras 3 jurisdicciones que no son Estados Miembro pero criminalizan tales actos, en Gaza, las Islas Cook y ciertas provincias de Indonesia.

De este modo, cuando se analiza la censura y bloqueo en relación a la Comunidad LGBTI, no puede limitarse a observar los bloqueos de contenidos pornográficos, sino que se debe examinar el acceso libre –o no- a páginas de noticias y cultura LGBTI, información sobre organizaciones de defensa y promoción de los Derechos de dicha Comunidad, webs de organizaciones sobre VIH/SIDA, u aplicaciones de citas para personas del mismo sexo.

Debido a la pluralidad de los casos particulares resulta complejo elegir ejemplos concretos que puedan extrapolarse y servir de modelo general. No obstante, se considera oportuno

exponer por lo menos uno, que permita la visualización a grandes rasgos del funcionamiento de la censura LGTBI en Internet:

1. LÍBANO :

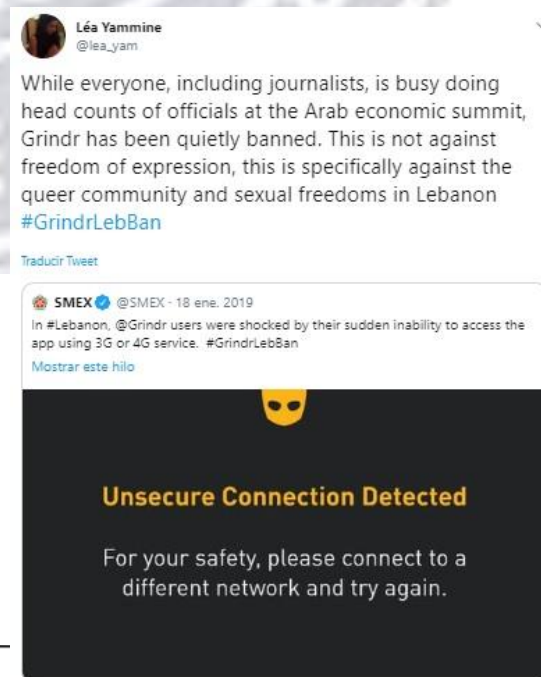
La República Libanesa está sumida actualmente en una fuerte crisis económica y política, dejando al país sin gobierno durante más de dos meses desde que el ex primer ministro Saad Hariri renunció el 29 de octubre cediendo a la presión popular.

Mientras, se han sucedido importantes protestas en el marco de la denominada “Semana de la Ira”, con el bloqueo de las principales carreteras del país -desde Beirut hasta Trípoli-, así como cortes de energía y manifestaciones contra la corrupción institucional y el estancamiento para la formación del nuevo Ejecutivo.

En el ámbito LGTBI, desde que en 2008 ondeara la bandera arcoiris en la primera manifestación LGTBI de su Historia y durante varios años, Líbano ha progresado paulatinamente en la aceptación y visibilidad de la comunidad, si bien en los dos últimos años la situación se ha bloqueado. Si bien durante unos años se había convertido en uno de los países más permisivos del mundo árabe por tolerar de facto la homosexualidad tras varias resoluciones judiciales, por otra parte siguen estando vigentes los artículos del Código Penal Libanés que velan por la “ética y moral públicas”, incluyendo entre ellos el artículo 534 que condena “cualquier acto sexual contrario al orden natural”.

Ninguno de estos supuestos es desarrollado con detalle en el propio Código Penal, pero de facto se han venido produciendo hechos consecutivos que se encaminan hacia un endurecimiento de la situación de la Comunidad LGTBI en Líbano como el arresto en mayo de 2018 del organizador del festival anual del Orgullo en Beirut -lo que obligó a cancelar el evento-, o la detención de Georges Azzi, director ejecutivo de la Fundación Árabe para las Libertades y la Igualdad, quien organizaba anualmente la conferencia NEDWA.

Este contexto ha tenido su reflejo en el ámbito virtual, pues Internet ha sido una de las herramientas utilizadas por el Gobierno para la represión. Así, Lea Yammine, subdirectora de Lebanon Support, anunciaba el bloqueo de Grindr en enero de 2019 por orden del Ministerio de Telecomunicaciones. Si bien este fue un corte efímero, según datos del Informe



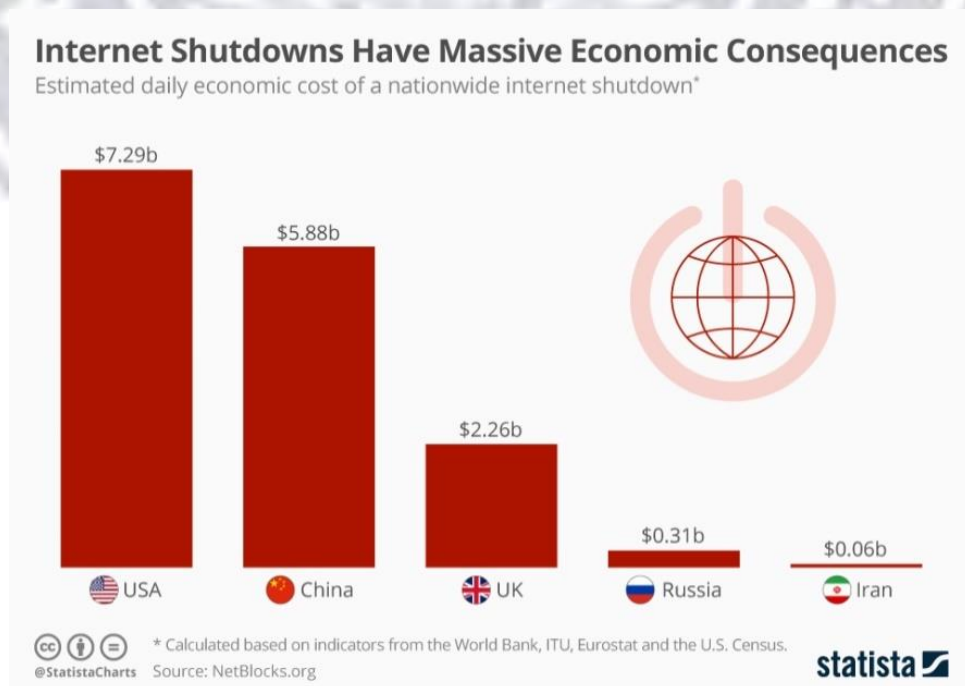
“Homofobia de Estado: Actualización del panorama global de legislación” de la International Lesbian, Gay, Bisexual, Trans and Intersex Association en mayo de 2019 el Ministerio Público ordenó a OGERO (propietario y administrador de red fija del estado libanés) bloquear Grindr. Poco después se anunció que todos los proveedores de servicios de Internet en el país harían lo propio. Las autoridades libanesas reconocieron su decisión de prohibir la aplicación, si bien nunca ofrecieron una explicación para ello, como señala Richard Hall.

Otros países que limitan por este motivo: Singapur; Marruecos, Etiopía, Arabia Saudí, Indonesia; especialmente en África, Oriente Medio y la región de Asia-Pacífico.

3.2 Censura y bloqueo por motivos económicos:

Los cortes de Internet tienen un fuerte impacto en la Economía, puesto que los flujos de comunicación son un factor estratégico de la misma. De este modo, la Institución Brookings – un centro de investigación económica sin ánimo de lucro situado en Washington – alega que el principal perjuicio se produce sobre las economías en desarrollo, en la medida que tratan de lograr una estabilidad financiera difícil de prever empresarialmente con los cortes de Internet gubernamentales.

En este sentido se pronunció un informe del Consejo Indio para la Investigación en Relaciones Económicas Internacionales (ICRIER), quien alegó que las 16.315 horas de desconexión llevadas a cabo por el Gobierno indio generaron pérdidas por valor de 3.040 millones de dólares.



Por otro lado, para algunos Estados como China –quien opta por la desconexión sistémica del “Internet global”- el factor económico es mayoritariamente un elemento persuasorio; pues disuade a las empresas extranjeras al generar excesivos elementos de incerteza y desconocimiento, y provoca un crecimiento del nicho de mercado para las empresas nacionales. Ejemplo de ello son el surgimiento y actual dominio de gigantes chinos como Baidu, Alibaba, Tencent o BAT.

No obstante es difícil encontrar múltiples ejemplos de cómo el bloqueo y la censura en Internet constituyen un factor positivo para la Economía de un Estado.

3.3 Censura y bloqueo cuyo motivo es limitar la exposición a la información exterior y promulgación de los valores nacionales:

1. COREA DEL NORTE

La República Popular Democrática de Corea, conocida como Corea del Norte, es un país de Asia oriental, que ha consolidado como uno de los regímenes más autoritarios del planeta. Se caracteriza por ser notoriamente hermético y aislado, si bien su actual dirigente Kim Jong-un, se diferencia de sus antepasados por entender la importancia de los beneficios de una comunidad virtual limitada.

En términos generales, el acceso a Internet sin filtros -según fuentes humanas que han desertado del régimen norcoreano- suele estar reservado para burócratas de alto rango, miembros de organizaciones no gubernamentales, algunos embajadores extranjeros y diplomáticos y grupos de asistencia externos. El resto de la población, accede bajo una Intranet llamada *Kwangmyong*, iniciada en el año 2000 y administrada por el único proveedor de servicio de Internet existente, de propiedad del Gobierno, por lo que este modelo de soberanía digital conlleva la limitación total de la exposición de la población norcoreana a información del exterior, y la promulgación y exaltación de los valores del régimen, a través de las 28 páginas web oficiales.

Asimismo, también han desarrollado su propio sistema operativo, denominado Estrella Roja con una versión adaptada de Firefox, conocida como Naenara, nombre que comparte con el único portal existente.

3.4 Censura y bloqueo cuyo motivo es paralizar la movilización de la Sociedad Civil controlando el relato político:

Si bien suele aludirse públicamente a razones de Seguridad Nacional, o al corte de la propagación de noticias falsas, son múltiples los casos que esconden apagones o bloqueos por esta razón.

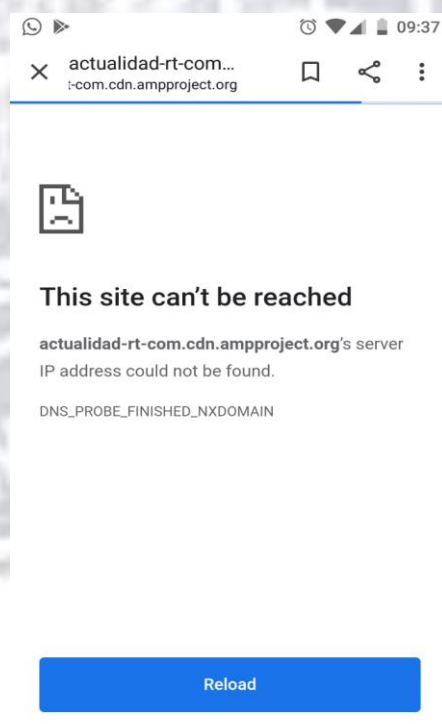
1. ECUADOR

La República del Ecuador, considerada en el Índice de Democracia (Democracy Index) de la Unidad de Inteligencia de The Economist como una Democracia Imperfecta (meter link?) es un reflejo del contexto latinoamericano actual, el cual se caracteriza por una creciente inestabilidad política y social de cara a 2020.

Su mayor punto crítico en la reciente crisis se alcanzó en los meses de octubre y noviembre de 2019, a raíz de la aprobación del Plan de Ajuste -llamado “paquetazo”- exigido por el Fondo Económico Internacional-, y a través del cual se desarrollaban medidas como la bajada salarial en contratos temporales del sector público, la reducción de vacaciones para los empleados públicos, o la eliminación de los subsidios a los combustibles. Las consecuencias de la implantación de estas medidas, junto el hartazgo social, los niveles de corrupción y la polarización exacerbada entre Gobierno y oposición- encabezada por Rafael Correa-, conllevaron huelgas en el sector educativo y en el transporte público, bloqueos, y movilizaciones cuyo fin era terminar con el mandato de Lenin Moreno.

Para tratar de limitar dicha presión social el Gobierno decretó el jueves 3 de octubre el Estado de Excepción con el que quedó limitado el derecho de reunión, la libertad de tránsito y se desplegó a la policía y a las Fuerzas Armadas por todo el país. Asimismo, organizaciones como Netblocks señalaron que se produjeron bloqueos parciales de Internet. Ejemplo de ello sería la alteración del servicio a través del operador CNT el lunes 7 de octubre, o el bloqueo de Claro, el proveedor líder de telecomunicaciones en Ecuador, el 12 de octubre.

De la misma forma, aún hoy el contenido de determinadas webs es censurado de acuerdo a las políticas implementadas en relación al Estado de Excepción. Ejemplo de ello, es el bloqueo de la emisión de canal 778, correspondiente a RT en Español.



Asimismo, el uso de Internet como herramienta de los Gobiernos para alterar las movilizaciones de la comunidad andina no es exclusivo de Ecuador. Varias organizaciones de

la Sociedad Civil que promueven los Derechos Humanos en el mundo digital, como AccesNow, la Asociación para el Progreso de las Comunicaciones, o la Fundación Karisma, informan de numerosos incidentes entre los cuales destacan la restricción de cuentas en redes sociales dedicadas a la difusión de información sobre las protestas en Bolivia con el fin de censurar contenidos relevantes, la confiscación de equipos periodísticos por parte de las fuerzas de seguridad, el envío de mensajes SMS que disuadían la participación a los paros convocados en Colombia, por parte de los abonados al servicio de telefonía móvil; o el monitoreo de las redes sociales de determinados activistas en Chile.

2. SUDÁN

Tras gobernar durante 30 años la República de Sudán, Omar al-Bashir fue depuesto por una revolución pacífica en 2019, dando lugar el 21 de agosto a la designación de Abdallah Hamdoug como primer ministro y constituyéndose el Consejo Soberano de Sudán, como parte de un acuerdo para compartir el poder y guiar a Sudán en los tres años de transición, hacia un gobierno civil, según el Estatuto Constitucional para el Período de Transición 2019.

Si bien según datos de la CIA sólo el 28% de los habitantes de Sudán son usuarios de Internet, esta conectividad se ha visto permanentemente alterada debido a la inestabilidad política y económica del país. Ejemplo de ello fue el bloqueo de septiembre de 2019 por el cual el Consejo Militar Transitorio ordenó el bloqueo por razones de seguridad, tratando de impedir la publicación de información referida a la represión llevada a cabo por las fuerzas de seguridad y militar durante la masacre de Jartum, y fruto de la cual se produjeron más de cien muertes.

Pero los bloqueos de Internet en Sudán no son extraños, pues pese a la numerosa normativa internacional que trata de garantizar el acceso a la Sociedad de la Información, como por ejemplo la resolución del Consejo de Derechos Humanos de Naciones Unidas en julio de 2016 por la cual se condenaban los bloqueos a Internet, las leyes sudanesas como la Ley de Regulación de Telecomunicaciones de 2018 permite a la autoridad regulatoria el derecho a interrumpir toda comunicación y telecomunicación de facto.

De este modo, los cuatro proveedores de servicio de telecomunicaciones en Sudán –Zain Sudan, subsidiaria del grupo kuwaití Zain y con el 48% de la cuota de mercado; MTN Sudán; Sudani, controlado por el Gobierno; y CANAR, son habitualmente obligados a bloquear Internet, con el objetivo de impedir el acceso a redes sociales y aplicaciones como Facebook o Twitter.

3. INDIA

7 de febrero de 2020

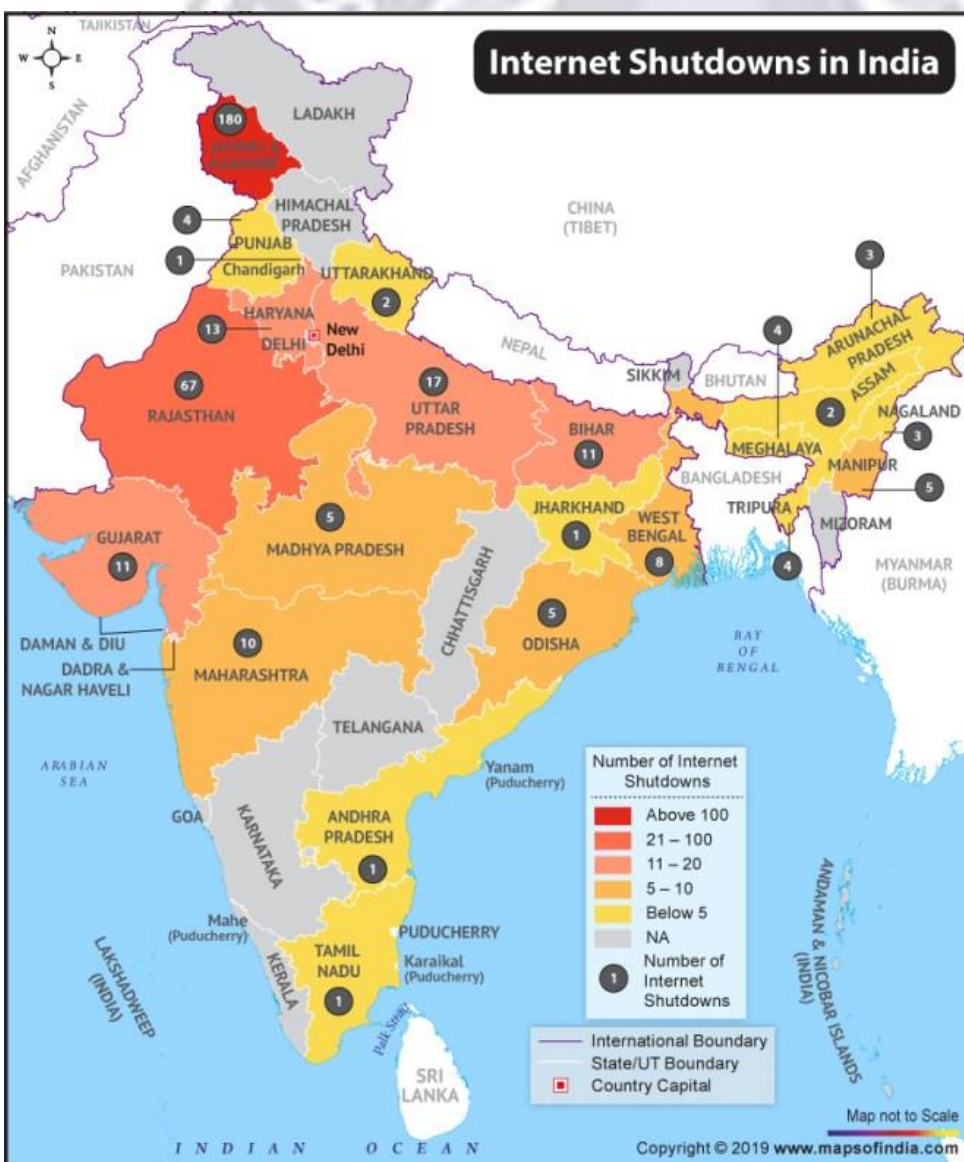
Hace 70 años, la India aprobaba una nueva Constitución, fruto de su independencia y tenían lugar las primeras elecciones. En aquel momento nadie creía que fuera capaz de sobreponerse a sus complicadas circunstancias –un extenso territorio, su densidad demográfica, su diversidad étnica, o a las altas tasas de pobreza y analfabetismo, entre otras-; no obstante como señalan autores como Josep M^a Colomer –político y economista de la Georgetown University- paulatinamente se introdujeron cambios institucionales y políticos cuyo resultado fue la consolidación de la democracia más poblada del mundo.

El pasado año 2019 Narendra Modi renovó su mayoría absoluta –ganando 303 de los 543 escaños en el *Lokh Sabha* (parlamento)- en las elecciones celebradas entre el 11 de abril y el 19 de mayo, abriéndose ante él un largo mandato de 5 años.

En este contexto, a finales de diciembre de 2019, el Gobierno de la India cortó toda la comunicación móvil (incluyendo mensajes, llamadas e Internet) en diversas áreas de Nueva Delhi y otras ciudades del país con el objetivo de contrarrestar las multitudinarias protestas

callejeras contra la polémica Ley de Ciudadanía; por la cual Narendra Modi y su partido –el nacionalista hindú Bharatiya Janata Party- pretenden poder conceder permisos a inmigrantes irregulares de países vecinos siempre que no profesen el Islam.

En términos concretos, según la página web Netblocks, el superintendente de policía de Saharanpur expuso: “Para evitar la propagación de rumores hemos decidido cerrar los servicios de Internet



hasta mañana y hemos enviado una carta al respecto a los proveedores de servicios de telecomunicaciones". No obstante, las razones reales son el limitado apoyo público a las iniciativas propuestas y su rechazo generalizado.

Asimismo, la región de Cachemira es desde la óptica de los *shutdowns* la más perjudicada, pues su territorio sufre repetidas desconexiones y en diciembre de 2019 batieron el récord de estar más tiempo apagados, llegando a los 137 días. Ello es debido a dos motivos principales confrontados a la política nacionalista de Modi: a) Cachemira es la única región de mayoría musulmana en la India, b) es una región constantemente disputada con Pakistán. Debido a esto el Gobierno ha retirado su autonomía especial, ha dividido el Estado en dos territorios regidos por Delhi, y la mantiene incomunicada con el resto del país y del mundo.

Sin embargo, Cachemira no es el único territorio apagado, pues AccesNow cifra en 159 las veces que India ha suspendido Internet en todo el país en los últimos 3 años - ocupando el 67% de las suspensiones totales en el mundo, sin incluir China ni Corea del Norte-, mientras que el Centro para el Derecho y la Libertad de Software ha contabilizado en 373 las veces que la India ha llevado a cabo un corte de Internet regional. Igualmente, en diciembre, tras el anuncio de la Ley de Ciudadanía, bloqueó Internet en siete Estados en respuesta a las marchas convocadas contra esta ley considerada discriminatoria.

3.5 Censura y bloqueo cuyo motivo es distorsionar la celebración de elecciones libres:

En ocasiones se llevan a cabo bloqueos parciales que afectan a un período temporal concreto, en el que suele tener lugar un evento determinado en el que gubernamentalmente se quiere influir. Un ejemplo de ello es el caso de Bielorusia:

1. BIELORUSIA

El Parlamento de la República declaró la soberanía de Bielorrusia el 27 de julio de 1990 y tras el colapso de la Unión Soviética, Bielorrusia fue independiente a partir del 25 de agosto de 1991. No obstante la evolución de Bielorrusia hasta la actualidad ha sido dispar: mientras por un lado ha experimentado un alto crecimiento en el Índice de Desarrollo Humano de la Organización de Naciones Unidas, y cuenta con un sistema público sólido -especialmente en el ámbito educativo y sanitario-; por otra parte su sistema político está lejos de convertirse en una democracia y la ausencia de Derechos Civiles y Libertades Públicas es notoria.

Respecto a las últimas elecciones, los observadores de la OSCE determinaron que las elecciones legislativas no fueron libres ni imparciales, y el escrutinio fue problemático en numerosos lugares. Los candidatos pro-Lukashenko arrasaron tras el registro de más de 500

irregularidades en el proceso, por lo que internacionalmente se ha atestiguado que Bielorrusia no cumple con los estándares democráticos.

Si bien a partir de la anexión de Crimea en 2014 por parte de Rusia, el antiguo satélite ruso ha mostrado signos de querer acercarse a sus vecinos europeos, por otra parte aún es el único país de Europa que mantiene la pena de muerte, ejerce un control férreo sobre los oponentes políticos, impone severas restricciones a la libertad de prensa y mantiene en el poder a Aleksandr Lukashenko, Presidente desde 1994.

Estas dinámicas también se reflejan en la Red, pues aunque en términos generales Bielorrusia no tiene un Internet fuertemente limitado sí se producen cortes en momentos estratégicamente vitales en la Historia del país. Ejemplo de ello es el ataque de denegación de servicio al medio opositor Charter 97 durante el período de la elección presidencial de diciembre de año. Según la información recogida por varias organizaciones de la Sociedad Civil los internautas que trataban de acceder a dicha web fueron redirigidos hacia webs falsas, por lo que tuvo una incidencia crítica en los procesos de información de los electores y en consecuencia no se celebran elecciones libres.



4. Conclusión

Tras examinar las cuestiones planteadas a lo largo de este informe podemos concluir que verdaderamente es preciso analizar las nuevas formas de interrelación que la red está propiciando y cómo estas inciden en el comportamiento del Estado.

Internet es oportunidad y amenaza al mismo tiempo. Desarrollado a partir de los años 60, fue diseñado con el propósito de facilitar el intercambio de conocimientos e ideas; hoy, sin embargo, la quiebra de los pilares de esta filosofía está en riesgo.

La globalización ha provocado que se desdibujen los límites entre lo interno y lo externo, potenciándose la existencia de comunidades transnacionales de prosumidores, que escapan de la esfera territorial tradicional y que cada vez cuentan con mayor capacidad de interactividad en tiempo real.

En este contexto, por una parte, algunos Estados consideran que supone un elemento demasiado sólido como herramienta de contrapoder; mientras que a su vez, las grandes corporaciones –especialmente de telecomunicaciones– buscan favorecer sus intereses comerciales sin valorar la protección de datos.

En todo caso, queda patente que existe un debate abierto sobre la gobernanza de Internet entendida como el conjunto de principios, normas, reglas, procesos de toma de decisión y actividades que, implementados y aplicados de forma coordinada por gobiernos, sector privado, Sociedad Civil y comunidad técnica, definan la evolución y el uso de la Red. Hoy por hoy, no existe una parametrización hegemónica, sino que los Estados-Nación legislan y actúan en función de sus intereses.

En este marco se puede afirmar que tal y como se planteaba en la hipótesis el régimen político de un país es una variable fundamental que incide en una mayor o menor censura. Los Estados democráticos ejecutan filtrados menos evidentes debido al riesgo reputacional interno y externo que les supone, mientras que varios de los Estados más autocráticos del globo planean desconexiones que permitan a los Gobiernos limitar la exposición de la información a su ciudadanía. No obstante, dicha regla general también comprende casos excepcionales como la India.

En todo caso, si se quiere incentivar la propagación de los valores democráticos a lo largo del globo, este será un asunto sobre el que será esencial desarrollar políticas institucionales coordinadas.

* * *

Bibliografía

- Abuín Vences, N. y Vinader Segura, R. (2011). El desarrollo de la World Wide Web en España: una aproximación teórica desde sus orígenes hasta su transformación en un medio semántico. *Razón y Palabra*, (75)
- Association for Progressive Communications, Humanist Institute for Cooperation with Developing Countries. (2015). *Global Information Society Watch 2015: Sexual rights and the internet*. Recuperado de <https://giswatch.org/sites/default/files/gw2015-full-report.pdf>
- Association for Progressive Communications, International Development Research Centre. (2016). *Global Information Society Watch 2016: Economic, social and cultural rights and the internet*. Recuperado de https://www.giswatch.org/sites/default/files/Giswatch2016_web.pdf
- Barcelona Centre for International Affaires. (2019). *El mundo en 2020: diez temas que marcarán la agenda global*. Recuperado de https://www.cidob.org/publicaciones/serie_de_publicacion/notes_internacionales/n1_220/el_mundo_en_2020_diez_temas_que_marcaran_la_agenda_global
- Candón Mena, J.I. (2012). Soberanía tecnológica en la era de las redes. *Revista Internacional de pensamiento político*. vol. 7, 73-92
- Castells, M. (2006). Internet y la sociedad red. *Contrastes*. (43), 111-113
- Committee for Protect Journalists. (2011). *Las diez herramientas de los opresores de Internet*. Recuperado de <https://cpj.org/es/2011/05/las-10-herramientas-de-los-opresores-de-internet.php>
- Deibert, R. y Rohozinski, R. (2008). "¿Bueno para la libertad, malo para la seguridad? Sociedad Civil Global (MIT Press). 123-147. Recuperado de https://tavaana.org/sites/default/files/Access%20Denied,%20Chapter%206%20Good%20for%20Liberty,%20Bad%20for%20Security%20-%20PDF%20-%20English_0.pdf
- Fernández, P. (2014). Neutralidad de la red: tensiones para pensar la regulación de internet. *Question*, 1 (42), 69-84, Recuperado de: <https://perio.unlp.edu.ar/ojs/index.php/question/article/view/2131>
- Frosini, T. E. (2018). Internet y Democracia. *Revista de derecho constitucional europeo*. (30).

- Gaafar, R., Shawkat, O. (2019). *Las mujeres sudanesas, en el corazón de la Revolución*. Recuperado de <https://www.africaye.org/las-mujeres-sudanesas-en-el-corazon-de-la-revolucion/>
- Global Voices. (2020). *Mayor interrupción de internet en estado Rakáin de Myanmar fija peligroso precedente*. Recuperado de <https://es.globalvoices.org/2020/01/02/mayor-interrupcion-de-internet-en-estado-rakain-de-myanmar-fija-peligroso-precedente/>
- Gozzer, J.C. (1999). Internet y Estado: aproximaciones a la globalización desde el ciberespacio. Entre lo real y lo virtual. Colombia Internacional. (47), 51-71
- International Lesbian, Gay, Bisexual, Trans and Intersex Association. (2019). *Homofobia de Estado: Actualización del panorama global de la legislación*. Recuperado de https://ilga.org/downloads/ILGA_World_Homofobia_de_Estado_Actualizacion_Panorama_global_Legislacion_diciembre_2019.pdf
- Kyriakopoulou, K. (2011). Authoritarian states and internet social media: Instruments of democratisation or instruments of control?. Human Affairs, 21(1). doi: 10.2478/s13374-011-0003-y
- Leighton-Dore, S. (2019). *Grindr has reportedly been banned in Lebanon*. Recuperado de <https://www.sbs.com.au/topics/pride/agenda/article/2019/01/23/grindr-has-reportedly-been-banned-lebanon>
- Lozada, M. (2001). Estudios Latinoamericanos sobre cultura y transformaciones sociales en tiempos de globalización 2. (Capítulo: Política en red y democracia virtual: la cuestión de lo público. Recuperado de: <http://bibliotecavirtual.clacso.org.ar/clacso/gt/20100914034214/10lozada.pdf>
- Li, J. (2014). Internet Control or Internet Censorship? Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice. Pittsburgh Journal Of Technology Law And Policy, 14(1), 1-43. doi: 10.5195/tlp.2013.131
- Liu, Y. (2014). Competitive political regime and Internet control (1st ed.).
- Marín, J.L. (2018). Apagar internet, o como suprimir derechos en la red. Estudios de Política Exterior.
- Martínez Jiménez, C. (2015). "El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de Estados Unidos y Rusia". (Trabajo fin de grado, Universidad Pontificia de Comillas, Madrid. Recuperado de <https://repositorio.comillas.edu/xmlui/handle/11531/1222>
- Merino, A. (2019). Access Now

- Newman, L. (2020). How Iran's Government Shut Off the Internet. Retrieved 17 December 2019, from <https://www.wired.com/story/iran-internet-shutoff/>
- Olea, Andrea. (2019). *Beirut, un refugio para la comunidad LGBT en el mundo árabe*. Recuperado de <https://www.pikaramagazine.com/2019/03/beirut-un-refugio-para-la-comunidad-lgbt-en-el-mundo-arabe/>
- Paganini, P. (2020). RuNet – Russia successfully concluded tests on its Internet infrastructure. Retrieved 27 December 2019, from <https://securityaffairs.co/wordpress/95564/security/russia-runet-tests.html>
- Peris Blanes, A. (2010). Internet e identidad nacional: Estado, Dominios y Comunidades virtuales. *IC Revista Científica de Información y Comunicación*. (7), 221-254
- Polyanskaya, A., Krivov A. y Lomko, I. (30 de abril de 2003) "Comisarios de Internet: El FSB", *Vestnik Online*, 320(9). Recuperado de: http://www.vestnik.com/issues/2003/0430/win/polyanskaya_krivov_lomko.htm.
- Puyosa, I.. (2015). Control político de internet en el contexto de un régimen híbrido Venezuela 2007-2015. *Revista Teknokultura*, Vol. 12(3), 501-526. doi: 10.5209/rev_TK.2015.v12.n3.50392
- Puyosa, I. y Chaguaceda, A. (2017). Cinco regímenes políticos en Latinoamérica, libertad de internet y mecanismos de control. *Retos: Revista de Ciencias de la Administración y Economía*, VIII (14), 11-37
- Ramírez Plascencia, D. (2007). Conflicto de leyes y censura en internet: el caso Yahoo!. *Comunicación y Sociedad*. 8, 155-178
- Reporteros sin Fronteras. (2019). *Sudán: Las autoridades de transición mantienen la política de censura a los medios, meses después del derrocamiento de Omar Al-Bashir*. Recuperado de <https://rsf.org/es/noticias/sudan-las-autoridades-de-transicion-mantienen-la-politica-de-censura-los-medios-meses-despues-del>
- Rodríguez Prieto, R. (2017). De la «neutralidad» a la «imparcialidad» en la red. Un análisis crítico de la política de la UE sobre internet y algunas propuestas de mejora. *Cuadernos Europeos de Deusto*. Núm. 57. doi: <http://dx.doi.org/10.18543/ced-57-2017pp217-246>
- Sabiguero, A., Nieves, M., Ibarra, V., Jackson, M., Messano, F., & Esnal, G. (2016). Relaciones entre soberanía y tecnología en los tiempos de Internet. *Revista De La Facultad De Derecho*, (41), 259-286. <https://doi.org/10.22187/rfd2016211>

- Sanjuán Santonja, M. (2015). Nuevas formaciones políticas crecidas en Internet y su entrada en las Elecciones Europeas 2014: el caso de Movimiento RED, Podemos, Recortes Cero y Partido X. Dígitos. Revista de Comunicación Digital. (1), 71-89
- Software Freedom Law Center. (2018). *Living in Digital Darkness: A Handbook on Internet Shutdowns in India*. Recuperado de <https://sflc.in/sites/default/files/reports/Living%20in%20Digital%20Darkness%20-%20A%20Handbook%20on%20Internet%20Shutdowns%20in%20India%2c%20May%202018%20-%20by%20SFLCin.pdf>
- Stadnik, I. (2019). Internet Governance in Russia – Sovereign Basics for Independent Runet. SSRN Electronic Journal. doi: 10.2139/ssrn.3421984
- Sierra Castro, H. (2015). El Derecho a la privacidad y el Intervencionismo de Estado en la era digital. Red Universitaria sobre Derechos Humanos y Democratización para América Latina. (7), 73-93
- Vercelli, A. (2014). Repensando las regulaciones en la era digital: ¿Llegó la hora de (re)regular Internet? Voces en el Fenix, Revista de la Facultad de Ciencias Económicas de la Universidad Buenos Aires. (5), 15
- Vercelli, A. (2015). Repensando las regulaciones de internet. Análisis de las tensiones políticas entre no-regular y re-regular la red-de-redes. Chasqui. Revista Latinoamericana de Comunicación, 129, 95-112.
- Wakefield, J. (2020). Russia 'successfully tests' its unplugged internet. Retrieved 27 December 2019, from <https://www.bbc.com/news/technology-50902496>
- Zayas Rosell, A. (2018-19). Injerencias Occidente-Rusia: Rusofilia versus Rusofobia. (Trabajo fin de grado, Universidad de Alicante) Recuperado de https://rua.ua.es/dspace/bitstream/10045/93501/1/Injerencias_entre_Occidente_y_Rusia_Rusofilia_versus_Rus_Zayas_Rosell_Andres.pdf