

Nuevas (y viejas) formas de censura de la información en internet

China es una incubadora de un gran número de técnicas de restricciones de contenidos en internet que después se aplican por **todo el planeta**. La censura y los ataques a la libertad de expresión e información en la red también ocurren en **España** y en países de nuestro entorno.

ANTONIO DELGADO

El 10 de octubre de 2014, el usuario @VictorUgas de la red social Twitter publicó las fotos del cadáver del diputado venezolano Robert Serra en la morgue. Este diputado de 27 años fue asesinado diez días antes en su casa de Caracas. Lo encontraron maniatado y amordazado, con 50 puñaladas. También mataron a una mujer que estaba con él.

La publicación de las imágenes causó un revuelo entre los venezolanos. Mientras usuarios de esta red social pedían el linchamiento público del usuario que las había publicado, otros se dedicaron a darle difusión desde sus propias cuentas¹. Unos días más tarde, fue detenido junto con otros usuarios.

El medio argentino Infobae se hizo eco de esta polémica y publicó una versión

editada de las imágenes del cadáver de Serra en un artículo en su página web². A las pocas horas, Delcy Rodríguez, ministra de Comunicación e Información de Venezuela, utilizó la misma red social para comunicar que la página web de Infobae había sido bloqueada en Venezuela³: “Por mancillar el honor de nuestro joven diputado Robert Serra e irrespetar la integridad de su familia, ha sido bloqueado el portal web Infobae”.

Desde ese momento, era imposible acceder al dominio Infobae.com. El mecanismo de censura utilizado por Venezuela consistió en aplicar una ley que obliga a los proveedores de acceso a internet (ISP) a bloquear direcciones web a requerimiento del Gobierno. Los ISP ejecutan un proceso para que no se re-

Antonio Delgado (@adelgado) es periodista especializado en periodismo de datos, tecnología y sociedad.

1.- <http://adb.li/apm1> 2.- <http://adb.li/apm2> 3.- <http://adb.li/apm3>

suelvan las DNS del nombre de un dominio determinado. Es decir, se manipula el mecanismo que posibilita que, cuando alguien escribe una dirección en su navegador, automáticamente se apunte a la dirección IP del servidor donde se encuentra la página web.

Infobae tardó seis días en construir una herramienta para saltarse la censura. Básicamente, consiste en un *software* que cada pocos segundos envía una petición de información (*ping*) a la página web de Infobae. Esta petición se realiza utilizando un *proxy*, o servidor intermedio, que simula estar navegando desde una dirección IP de Venezuela. Si la página web no está disponible, se activa un nuevo dominio de forma automática. Compraron más de 100 dominios de diferentes extensiones y lanzaron el primero: Infobae.press. A las pocas horas, este dominio también fue bloqueado⁴. Automáticamente se activó Infobae.media. Al mismo tiempo que se sucedía esta lucha entre el ratón y el gato, una amplia y heterogénea red formada por periodistas, tuiteros venezolanos, comunidades y foros de todo tipo, medios internacionales, activistas, gente de Anonymous y hasta la Universidad de Stanford utilizaban las redes sociales y sus diferentes canales de comunicación para correr la voz con cada nueva dirección de la web para que llegara a las pantallas del máximo número de venezolanos.

La reacción frente al intento de censura hizo que se amplificara el contenido

censurado. El tráfico a la página web de Infobae desde Venezuela se multiplicó por tres durante esos días. Internacionalmente se conoció más la información del asesinato del diputado Serra, así como las imágenes de su cuerpo en la morgue. El Gobierno de Maduro ya no censuró Infobae.media. La repercusión de la campaña de censura hizo que las imágenes y el propio medio de comunicación fueran mucho más conocidos tanto en el ámbito nacional como en el internacional.

Efecto Streisand: cuando se amplifica una información al censurarla

El efecto que ocurre al censurar una información y conseguir lo contrario –es decir, su amplificación– se le conoce como efecto Streisand⁵. En 2003, la página web Pictopia.com publicó una foto aérea de la costa de California en la que se veía la casa de Barbara Streisand. La actriz estadounidense denunció a la web y al fotógrafo Kenneth Adelman por violación de la privacidad. La página y el fotógrafo argumentaban que la imagen donde aparecía la casa era parte de un trabajo en el que se denunciaba la erosión de la costa. La polémica surgida por este intento de censura fue ampliamente recogida por medios de todo el mundo. Las imágenes aéreas de la casa

4.- <http://adb.li/apm4> 5.- <http://adb.li/apm5>

de Streisand se publicaron en miles de blogs, foros y medios de comunicación. La actriz había conseguido el efecto contrario. Las imágenes de su casa tuvieron mayor impacto mediático que si la denuncia no se hubiera producido.

La única manera que tiene el Gobierno de Venezuela de bloquear Infobae es cortando el acceso a la red a todo el país. Y eso es lo que hizo Egipto en enero de 2011. En medio de las multitudinarias protestas en El Cairo, amplificadas y promovidas gracias a las redes sociales, el Gobierno de Hosni Mubarak decidió desconectar Egipto de internet⁶ y bloquear los servicios de telecomunicaciones como una forma de parar las protestas. No sirvió de nada y perjudicó a la economía del país. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) calculó que el bloqueo de internet durante cinco días tuvo un coste directo de al menos 90 millones de dólares⁷, al estimar que el sector de internet y las telecomunicaciones representan entre el 3 y 4 % del producto interior bruto (PIB) del país. Hoy en día, desconectar un país de internet supone un alto impacto sobre la economía y la sociedad. En Irán, el régimen ha limitado el ancho de banda para no hacer sencillo el uso de la red y desincentivar las críticas en redes sociales y la publicación de vídeos e imágenes. No ha funcionado y ahora se plantean aumentar la velocidad de acceso en las licencias de móvil 3G y 4G⁸.

Ataque de denegación de servicio

A veces, la censura se realiza a través de ataques informáticos. Eso es lo que ocurrió en España en febrero de 2008. El popular blog de tecnología Genbeta, propiedad de la empresa de medios Weblogs SL, caía por un ataque de Denegación Distribuida de Servicio (DDoS)⁹. Este tipo de ataques consiste en realizar millones de peticiones de acceso a un servidor desde otros tantos ordenadores y servidores hasta colapsarlo. Para ello, los delincuentes alquilan redes de ordenadores infectados (*botnets*) con *malware* o se aprovechan de vulnerabilidades en servidores de internet para tomar el control de las máquinas. Utilizan toda la potencia de estas máquinas zombis para desconectar por fuerza bruta un sitio web.

Bloqueo de internet cinco días en Egipto: coste de unos 90 millones de dólares

Todo comenzó en noviembre de 2007 con la publicación de una entrada en el blog en el que se alertaba sobre algunos servicios como Quienteadmite.com, sitios que se ofrecían a los usuarios para saber quién les había borrado de su lista de amigos en la aplicación de mensajería instantánea Messenger, pero que en realidad lo que hacían era quedarse con el nombre y contraseña del usuario para fines maliciosos. Este *post* quedó varios meses en

6.- <http://adb.li/apm6> 7.- <http://adb.li/apm7> 8.- <http://adb.li/apm8> 9.- <http://adb.li/apm9>

el olvido hasta que empezó a ocupar las primeras posiciones en buscadores frente a determinadas búsquedas genéricas. Por culpa de este ataque, el blog estuvo una semana fuera de combate.

Rápidamente, otros sitios de internet se solidarizaron republicando el contenido. También fueron objeto de los ataques. Entre ellos, el conocido sitio de agregación de contenidos Menéame. Esta plataforma se convirtió en el nuevo objetivo de los delincuentes. Ricardo Gallir, uno de los fundadores de este servicio, publicó en su blog, alojado en la popular plataforma WordPress.com, una serie de entradas en las que denunciaba los hechos y se hacía eco de sus investigaciones sobre quiénes estaban detrás de los ataques. La reacción fue lanzar un ataque de múltiples gigabits por segundo y decenas de millones de paquetes por segundo contra WordPress.com, lo que afectó a tres de sus centros de datos y dañó seriamente el rendimiento general de la plataforma de alojamientos de blogs más grande de internet.

El ‘copyright’ y la amenaza judicial

En países democráticos, la censura en internet es mucho más sutil. El bloqueo de artículos, vídeos informativos o críticas frente a instituciones o grandes empresas se realiza utilizando otros mecanismos como ampararse en supuestas violaciones de la propiedad intelectual. Es habitual el envío de cartas de re-

querimiento por infracción de marca o derechos de autor para eliminar contenidos críticos de internet. Grandes plataformas de alojamiento de contenidos como YouTube dispone de mecanismos semiautomatizados para resolver estas disputas. Debido a las quejas de los grandes proveedores de contenido por la piratería, el contenido se retira inmediatamente y luego se hacen las preguntas. Una vez eliminado o bloqueado, el usuario afectado puede hacer las alegaciones pertinentes. El proceso puede durar semanas.

En países democráticos,
la censura en internet
es mucho más sutil

BuzzFeed, uno de los medios digitales norteamericanos con mayor crecimiento en los últimos años, denunció en un artículo¹⁰ cómo el servicio de alojamiento de textos Scribd eliminó documentos secretos relacionados con un programa de espionaje en Ecuador. Este medio los había publicado para apoyar un reportaje de investigación. En los documentos se mostraba un acuerdo entre la agencia de inteligencia de Ecuador y un intermediario de Estados Unidos para comprar equipos de espionaje a empresas israelíes. Scribd decidió eliminar el documento sin preguntar primero al recibir una reclamación por infracción de

10.- <http://adb.li/apm10>

copyright, según la normativa antipiratería “Digital Millennium Copyright Act” (DMCA) de Estados Unidos. De nada sirvieron las alegaciones. Desde entonces, para alojar documentos, BuzzFeed utiliza el servicio de DocumentCloud, un proyecto pensado por y para periodistas y medios. Esta web permite subir y compartir documentos de trabajo dentro de las redacciones, además de realizar búsquedas estructuradas. Esta plataforma periodística también recibió posteriormente un requerimiento de violación de *copyright*, pero no lo tuvieron en cuenta. En la actualidad, medios como *The New York Times*, ProPublica o, en España, ELDiario.es han subido más de medio millón de documentos a DocumentCloud.

Detrás de este intento de censura a BuzzFeed se encuentra la empresa española Ares Rights. En su página web se publicitan como un servicio orientado a combatir la piratería en internet. Igualmente, esta empresa, fundada en 2008, es conocida también por la eliminación de un documental¹¹ y vídeos críticos con la gestión del Gobierno del presidente ecuatoriano Rafael Correa¹², mediante la reclamación de violación de *copyright*¹³. En estos vídeos se utilizan pequeños fragmentos de imágenes de Correa transmitidas por la televisión pública Ecuador TV, algo que forma parte del uso justo amparado por la convención de Berna de derechos de

autor. Este supuesto uso de imágenes no autorizadas es la argumentación exhibida para, en nombre de sus titulares, realizar una reclamación de *copyright* a plataformas como YouTube y Vimeo.

La amenaza de abrir un procedimiento judicial como forma de conseguir la eliminación de un contenido crítico es otra de las formas más habituales de ejercer la censura en internet¹⁴. Una amenaza de denuncia firmada por un gran despacho de abogados en nombre de una multinacional es una de las fórmulas más comunes en España y países de nuestro entorno para eliminar contenidos críticos en la red. Empresas periodísticas de medio o gran tamaño disponen de recursos para poder hacer frente a un proceso judicial, pero, en el caso de medios pequeños o blogueros, este tipo de amenaza supone de facto un ataque directo a su libertad de expresión y sostenibilidad económica. La mayoría suele optar por eliminar el contenido.

Este tipo de procedimientos también se utilizan para conseguir censurar opiniones críticas vertidas en los comentarios de las noticias por parte de los lectores, aunque no siempre las empresas de medios están dispuestas a defender a sus lectores. El pasado mes de octubre, la empresa de medios Weblogs SL ganó una demanda¹⁵ a un empresario que reclamaba la eliminación de dos hilos de respuestas en uno de sus blogs. En ellos, un usuario se quejaba de que

11.- <http://adb.li/apm11> 12.- <http://adb.li/apm12> 13.- <http://adb.li/apm13> 14.- <http://adb.li/apm14> 15.- <http://adb.li/apm15>

un teléfono que había adquirido en una tienda no se correspondía con lo que había pedido. El dueño de la tienda entró en una disputa en los comentarios y finalmente demandó a la empresa Weblogs SL por intromisión al honor. La sentencia¹⁶ absolvió de todos los cargos al medio imponiendo las costas al demandante. En su escrito, el juez argumenta que en tales comentarios no se realiza una intromisión al honor del demandante y que, por encima de este, prevalece la libertad de expresión del usuario al comentar en internet.

China: incubadora de restricciones

China es una incubadora de todo tipo de restricciones de internet¹⁷ que después se aplican por todo el planeta. En la actualidad, 645 millones de chinos están conectados a internet, lo que representa casi el 50 % de la población total. Este país cuenta con tecnología propia y de empresas privadas –muchas de ellas occidentales–, así como un ejército de personas para controlar, censurar e incluso manipular contenidos en medios y redes sociales que no son del agrado del Gobierno. La maquinaria se detiene cuando las críticas de los ciudadanos van dirigidas a la oposición o contra países extranjeros.

El Gran Cortafuegos Chino es el nombre con el que se conoce la tecnología más utilizada por la censura china. Este cortafuegos está presente en todos los

niveles dentro de una red: desde enrutadores a redes troncales, pasando por los proveedores de acceso a internet (ISP). Así, se controla y bloquea tanto la IP de un servidor web como las DNS de un dominio asociado a dicha dirección. Otra técnica que se aplica consiste en limitar la banda ancha en determinados momentos; de esta forma, se estrangula la navegación por internet o por determinadas webs, haciendo complicado acceder a diversos servicios o fuentes de información. Este filtrado incluye un análisis profundo del tráfico, lo que permite que la censura se realice de forma automática en función de diversas palabras clave. Al usuario se le muestra un mensaje en blanco, de error o cualquier otro contenido. También se suelen recopilar los datos de los usuarios que están intentando acceder a contenido prohibido para ordenar su detención.

En China es habitual censurar medios internacionales. En 2013, las webs de medios como *New York Times*, Bloomberg, *El País* y el Consorcio Internacional de Periodistas fueron bloqueadas en China por publicar investigaciones sobre la acumulación de riqueza de las principales familias chinas y el uso de paraísos fiscales.

Asimismo, la censura china suele bloquear aplicaciones y servicios de gran éxito internacional. En el hueco de mercado que dejan surgen equivalentes locales que cumplen con los requisitos del Gobierno chino. Sitios

16.- <http://adb.li/apm16> 17.- <http://adb.li/apm17>

como Sina Weibo, QQ y Tencent. Por ejemplo, el buscador Baidu no solo elimina contenidos considerados “ilegales” por el Gobierno, sino que también manipula los resultados de búsquedas para ofrecer en los primeros lugares las informaciones aprobadas por el Estado frente al publicado por fuentes no oficiales o extranjeras.

La censura pierde efectividad al mismo ritmo que un tema de debate se viraliza

Las empresas internacionales que operan en el país también pasan por el aro. Yahoo, Google y Apple son algunas de las empresas que se han autocensurado y han incorporado en mayor o menor medida los requerimientos del Gobierno chino. Se trata de un gran mercado que no están dispuestos a perder. Por ejemplo, no muestran información sobre las protestas de la Plaza de Tiananmén de 1989. Incluso Siri, el agente virtual más parlanchín de Apple, se calla cuando los usuarios chinos preguntan por estas cuestiones.

En el artículo científico titulado “*The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions*”¹⁸, publicado en agosto de 2013, se explica el funcionamiento de la censura china en internet en el servicio Weibo, una red de mensajería instantánea y *microblogging* similar a Twitter. En este estudio se ana-

lizan las diferentes técnicas de censura utilizadas durante 2012. En el periodo analizado, esta red social contaba con 300 millones de usuarios y cada día se publicaban unos 100 millones de mensajes. El 30 % de los mensajes se borra entre cinco y 30 minutos después de su publicación. En las primeras 24 horas se borra casi el 90 % del total de los mensajes censurados.

En Weibo, los censores utilizan diferentes métodos. Desde suprimir de forma temporal o permanente cuentas y mensajes a técnicas mucho más sutiles como eliminar un *post* de un usuario pero dejarlo visible solo para él. De esta manera, el responsable del mensaje cree que el resto de la red también puede leerlo. A pesar de todas estas medidas, en muchas ocasiones no se puede parar la difusión de mensajes o rumores, lo que pone en alerta al Gobierno chino y hace que exija a los directivos de estas empresas un mayor control de los usuarios.

También existen censores humanos. Miles de ellos. Se encargan de realizar aquellas tareas que las máquinas aún no hacen bien. Como captar ironías o mensajes en clave en blogs, redes sociales, foros o cualquier otra forma desarrollada para compartir información en internet. Pueden acceder además a mensajes de correo electrónico, instantáneos o llamadas de teléfono.

Otra forma de manipulación y control de la información se lleva a cabo mediante

18.- <http://adb.li/apm18>

la propaganda. Desde hace una década, existen unidades dedicadas a diseminar en internet contenidos a favor del Gobierno. Esta técnica conocida como *astroturfing* es habitual también en países occidentales como una forma de *marketing* a favor de empresas o intereses particulares.

La censura no siempre funciona

A pesar de la ingente cantidad de recursos que dedica China a controlar los mensajes de sus ciudadanos, la censura no siempre es posible. Los usuarios de Weibo obligaron al Gobierno a empezar a abordar el problema de la alta contaminación en las principales ciudades chinas. También se han denunciado casos de corrupción y abuso por parte de jefes del partido. La censura pierde efectividad al mismo ritmo que un tema de debate se viraliza.

La censura tampoco sabe actuar cuando las críticas se realizan en forma de sátiras, eufemismos o chistes. El uso de palabras neutras o crear una jerga propia es complicado de filtrar.

En las elecciones generales francesas de 2012, los usuarios de Twitter de este país utilizaron mensajes satíricos o en clave de humor¹⁹ para eludir la normativa que prohíbe la publicación de resultados parciales o sondeos electorales antes del cierre de los colegios electorales. La violación de esta norma supone multas de hasta 75.000 euros. Los sondeos fueron publicados en webs de medios francófonos en Suiza y Bélgica

y amplificadas en clave de humor en las redes sociales con mensajes del tipo “el gouda se vende entre 52,5 y 53 euros” o “el tomate está maduro”, junto con la etiqueta #RadioLondres, como referencia a la emisora de radio que utilizaba la resistencia francesa para coordinarse durante la II Guerra Mundial.

Protección de la libertad de expresión

Internet, por sus características, permite a las personas buscar, recibir y distribuir información e ideas de forma instantánea. Es un gran facilitador de derechos humanos como la libertad de expresión y opinión. Impulsa el desarrollo económico y social de la humanidad. La red tiene un lugar esencial en la educación de las personas. Por estos motivos, la Organización de las Naciones Unidas (ONU) considera que el acceso a internet es un derecho humano y hay que protegerlo y promover su uso²⁰. Cortar el acceso a los ciudadanos supone un atentado al derecho de libertad de expresión y opinión recogido en el artículo 19 de la Declaración Universal de Derechos Humanos.

Los mecanismos de bloqueo o filtrado por parte de los Gobiernos para censurar en internet y la falta de transparencia a la hora de ejecutar estas medidas son una de las principales preocupaciones de la ONU. En caso de que sea necesario, Naciones Unidas recomienda que la decisión del bloqueo nunca debe estar en manos de una empresa privada y los

19.- <http://adb.li/apm19> 20.- <http://adb.li/apm20>

Estados tienen que proporcionar un listado de los sitios bloqueados, así como una explicación individual. Además, estas medidas deben ser tomadas por un juez y en un proceso transparente tanto para el usuario involucrado como para el resto de la sociedad.

Formas individuales de protección

Muchos de los mecanismos que utilizan los Gobiernos para censurar contenidos en internet son las mismas armas que se han desarrollado en la lucha contra la piratería. Esta disputa contra las redes de pares y las páginas con contenido no autorizado han supuesto el desarrollo de técnicas y herramientas de eliminación de contenidos que ahora se utilizan para censurar por motivos políticos, económicos o religiosos.

De igual modo, las técnicas más habituales que los usuarios utilizan para saltarse estas restricciones también pueden ser aprovechadas para esquivar este tipo de censura.

El uso de redes privadas virtuales (VPN) permite generar una conexión cifrada a través de diferentes servidores alojados en el extranjero. Es la opción más recomendada a la hora de visitar países como China: saltarse restricciones de contenido por *copyright* o aumentar la seguridad de periodistas y activistas en situación de riesgo. También es recomendable el uso de *proxys*

de servidores extranjeros, aunque estos ofrecen menores niveles de seguridad y privacidad. En menor medida, se utilizan técnicas de camuflaje de textos en archivos multimedia o difusión de contenidos a través de redes punto a punto (P2P, por sus siglas en inglés).

Lucha activa contra la censura

¿Qué pueden hacer los medios? Pablo Mancini, director de estrategia digital de Infobae, considera que el episodio de censura de su medio por parte del Gobierno de Venezuela debe servir para que la comunidad internacional tome un papel activo contra este tipo de ataques a la libertad de expresión e información. Mancini cree que sería necesario poner en marcha una alianza global por la libertad de la prensa en internet en la que estuvieran actores importantes, desde Naciones Unidas a grandes empresas del sector como Google, Facebook y Twitter²¹. Esta gran coalición debería ser capaz de desarrollar una especie de “refugio técnico” que posibilite que cualquier medio de comunicación *online*, independientemente de su tamaño, cuente con el respaldo y ayuda de la comunidad. Infobae, de momento, pondrá a disposición de otros medios o blogueros que sufran una acción similar la tecnología desarrollada para saltarse este tipo de ataques a la libertad de expresión. La difusión de contenidos, para bien o para mal, nunca se para. ■

21.- <http://adb.li/apm21>