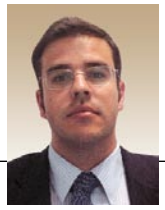
La ciberutopía en la era WikiLeaks

La web y los medios cibernéticos se han convertido en mecanismos para la libertad de expresión, la cultura y la política. Sin embargo, los gobiernos totalitarios emplean las mismas herramientas para coartar la libertad de expresión de sus ciudadanos, ejecutar campañas de información, y reforzar sus regímenes. En este artículo se analizan las luces, sombras y "claroscuros" relativos a esta realidad y su relación con la ciberseguridad, prestando especial atención a la influencia que Internet tuvo en la "primavera árabe", al uso de internet que hacen los gobiernos totalitaristas y grupos terroristas, así como la transformación de internet en una herramienta radicalizadora.



Enrique Fojón Chamorro / Adolfo Hernández Lorente

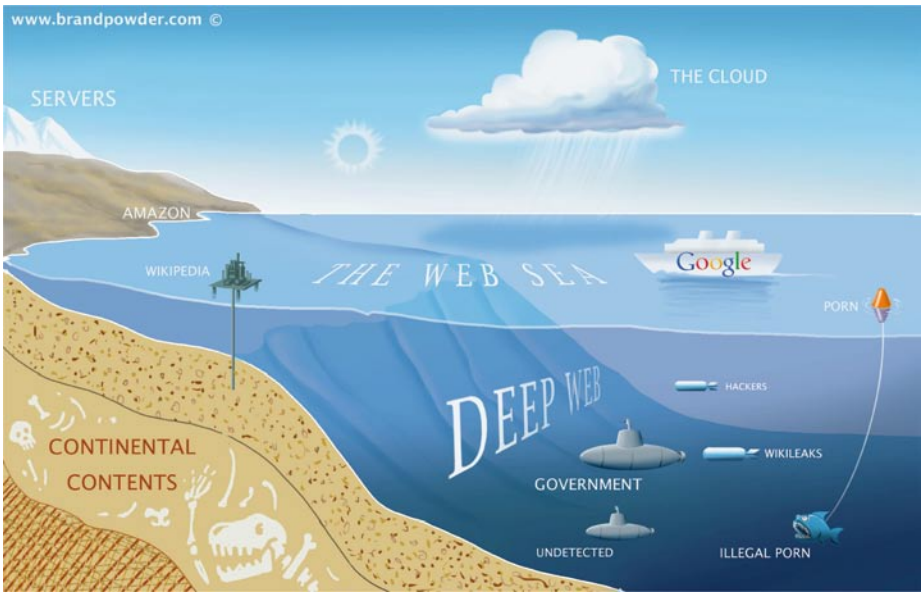
Internet y la primavera árabe

A principios de 2011, la inmolación del joven tunecino Mohamed Bouazizi fue el detonante de una revolución social que venía fraguándose en Túnez y que culminó con la caída del régimen de Zine El Abidine Ben Ali. La revolución tunecina sirvió de inspiración y se extendió a la mayoría de los países musulmanes del norte de África y Oriente Medio. Esta revolución fue bautizada por los medios de comunicación como "la primavera árabe", cuyo "espíritu" está todavía vigente, y que, hasta la fecha, ha propiciado la caída del ya mencionado régimen de Ben Ali en Túnez, así como los de Hosni Mubarak en Egipto, Muamar el Gadafi en Libia y Ali Abdullah Saleh en Yemen. Además, ha provocado cambios de gobierno en Marruecos, Omán y Jordania e importantes protestas sociales en Argelia, Mauritania y Siria, desencadenando en este último país una guerra civil que hoy en día continua.

Pero, ¿qué papel ha jugado Internet en este tipo de revoluciones? Sin lugar a dudas, Internet ha tenido un papel importante, aunque no decisivo, en el desencadenamiento inicial de estas revoluciones, a pesar de la opinión contraria de muchos internet-centristas –aquellos que, según Evgeny Morozov, tienen la tendencia a explicar todo en base a convertir internet en el punto de partida y el principal actor de la explicación– que confirieron a Internet un papel casi único en el origen de la "primavera árabe".

Herramientas anticensura

Sin embargo, Internet ha coadyuvado, de manera decisiva, a la difusión, apoyo y consolidación de las revoluciones. Los regímenes musulmanes del Norte de África y Oriente Medio se han caracterizado y caracterizan por una censura severa en el acceso y uso de Internet. Por ello, durante años el Consorcio para la Libertad Global de Internet (GFIC, sus siglas en inglés), una organización financiada en parte por el Departamento de Estado de los Estados Unidos, ha estado desarrollando herramientas anticensura como Freegate, Ultrasurf o Dynaweb. Estas herramientas fueron diseñadas e implementadas con el objeto de proporcionar apoyo a los ciberactivistas chinos e iraníes, pero su uso se ha extendido para dar cobertura a los ciberactivistas tunecinos, egipcios y libios, entre otros. Estas herramientas anticensura no sólo permiten a los ciberactivistas comunicarse con el exterior y dar a conocer su realidad diaria sin ser censurados por sus gobiernos, sino que a su vez les permite conocer la realidad internacional y organizar acciones futuras. Durante las revoluciones, los gobiernos de Egipto, Libia o Siria, sabedores del patrocinio de GFIC así como del apoyo de otros gobiernos y organizaciones, realizaron numerosos y largos cortes en el acceso a internet aprovechando el control que ejercen sobre la infraestructura de Internet en sus países. Con las revoluciones en pleno apogeo los videos y testimonios que los cibernautas tunecinos, libios, egipcios o sirios compartieron en la red sirvieron para que los medios de comunicación internacionales ejerciesen, y ejerzan, un papel de "altavoz" que permita dar a conocer la situación de estos países, provocando la condena internacional e incluso la intervención militar en Libia por parte de una coalición de países liderada por Francia y Reino Unido y en la cual participó España.



Dos caras de la misma moneda: usos de internet con fines totalitaristas y terroristas

A principios del siglo XXI, muchos expertos políticos predijeron que Internet sería, sin duda, el medio que catalizaría el proceso de democratización de aquellos países sometidos a regímenes totalitarios. Nada más lejos de la realidad.

Un caso interesante es el uso huxleyano de Internet que hace el gobierno chino al proporcionar a sus cibernautas todos aquellos servicios que demandan (correo electrónico, redes sociales, webs de entretenimiento o pornografía). Servicios que inicialmente estaban siendo proporcionados, en su inmensa mayoría, por empresas extranjeras, como Google o Facebook, están siendo sustituidos por productos *Made in China*, como Baidu o Weibo. Esta "condescendencia" del gobierno chino viene acompañada, por un lado, de una "censura selectiva", que les permite eliminar o tergiversar todo aquello que pueda suponer un elemento de desestabilización para el régimen y, por otro lado, de una "cultura panopticista" donde los internautas chinos saben y se sienten cibervigilados por su gobierno. El hecho de que menos del 0,5% de los cibernautas chinos hagan un uso regular de herramientas anticensura o que más de 87% de los adolescentes chinos desconozcan la existencia de los acontecimientos de la plaza de Tianamen de 1989 ejemplarizan el "éxito" de la política china sobre Internet.

Irán decidió en 2009, tras la "revolución verde" –también conocida como "revolución Twitter"– crear Iran-Net, un internet específico iraní. A pesar del fracaso de la revolución, que tenía como objetivo derrocar al gobierno electo de Mahmud Ahmadineyad, el uso de redes sociales "occidentales", en este caso Twitter, fue el mejor argumento para que el gobierno iraní comenzase la construcción de la Iran-Net, que tiene como objetivo llevar a cabo un control orwelliano del ciberespacio iraní. El descubriendo del gusano Stuxnet en 2010 aceleró la ejecución del proyecto, endureciendo sus requisitos censores. Hoy en día, la Iran-Net se encuentra en

una fase de pre-producción con algunos servicios ya operativos. Irán, al igual que China, dispone de unidades militares cibernéticas que tienen como objeto la penetración en redes enemigas y la sustracción de información sensible. La situación geopolítica de Irán ha provocado que el gobierno iraní preste apoyo cibernético a gobiernos amigos como Siria y al grupo terrorista chií Hezbolá.

La naturaleza heterogénea de Al-Qaeda confiere a Internet un papel protagonista en sus actividades de financiación, inteligencia, propaganda y captación. Estas actividades son llevadas a cabo por miembros de Al-Qaeda formados en el uso "maligno" de las nuevas tecnologías o cibergangs, que realizan tareas especificas sin conocer, en la mayoría de los casos, que el cliente final es una organización terrorista. Durante este año, en España se han producido dos detenciones de miembros de Al-Qaeda que explotaban las capacidades de Internet. Faisal Errai, un marroquí de 26 años, reclutaba a través de foros yihadistas a muyahidines que luego eran enviados a zonas de conflicto como Afganistán y Chechenia. Mudhar Hussein Almalki, también conocido como el ´bibliotecario´ de la Red Ansar Al Mujahideen -Red de partidarios de los Mujahidines o RAAM-, aparato de propaganda de apoyo a Al-Qaeda, fue detenido tras publicar en un foro islamista los nombres de un conjunto de políticos como objetivos de la Ýihad´. Entre estos políticos se encontraban George Bush, Bill Clinton, José María Aznar o Javier Solana.

Internet como herramienta radicalizadora

Dicho lo anterior, foros, *blogs*, webs, chats y redes sociales se han convertido en un crisol de de ideas, ideologías y posturas religiosas.

Hasta hace unas décadas, personas con intereses y problemáticas diversas no tenían relativa facilidad de entrar en contacto entre sí. Sin embargo, Internet ha roto las barreras geopolíticas e idiomáticas, permitiendo el flujo de ideas y la aparición de relaciones entre personas con intereses poco comunes.

Es en este intercambio de ideas virtual donde se manifiesta un fenómeno que en psicosociología se conoce como *polarización grupal*, demostrada empíricamente y profusamente explicada en diversos ensayos (*Stoner, Cass Stein*).

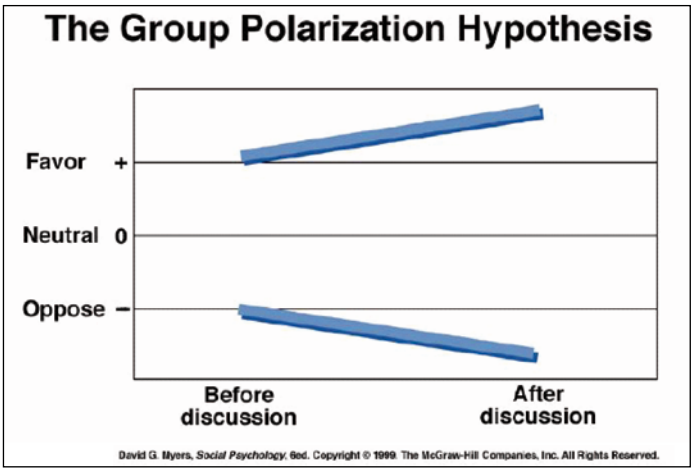
La polarización grupal es la tendencia que sufren las opiniones de las personas de un grupo, homogeneizándose y desplazándose al extremo más afín, llegando a opinar y realizar actos a los que esas mismas personas individualmente no se atreverían (asumiendo más riesgos). En otras palabras, la discusión tiende a **fortalecer** la inclinación inicial del grupo. Además, se refuerzan los argumentos que defienden la postura ideológica del grupo, y se desarrollan contraargumentos ante las posturas contrarias, conocido como influencia informacional.

Mediante el análisis de este fenómeno, se detectan patrones comunes de compartimiento en los grupos polarizados:

• **Búsqueda de un enemigo común**. Los grupos polarizados suelen encontrar un contrario en el que descargar su ira, creando un vínculo de cohesión y autoafirmación muy potente.

• Potencialmente contienen una **gran violencia contenida** que se desata en comportamientos irracionales, ya sea de forma velada o abierta.

• **Fuerte sentimiento de pertenencia a un grupo**. Para defenderse de tensiones, rechazos y exclusiones, los componentes del grupo no buscan ni se atreven a exponer ideas contradictorias a las comunes del conjunto. Cuando el interés por evitar conflictos y disputas internas crece, el grupo pierde contacto con la realidad, apareciendo el denominado *pensamiento grupal*.



• **Creencia de poseer a verdad absoluta**, lo que lleva a no contrastar la información ni a cuestionarse las posturas tomadas, repitiendo los mismos corolarios e hipótesis, creando una espiral que se retroalimenta favoreciendo la radicalización.

Como ya se ha indicado, este fenómeno es una herramienta eficaz empleada por extremistas políticos y religiosos en internet para captar y radicalizar ya que, además, permite un acceso virtualmente libre a argumentos, imágenes y relatos que apoyan ideologías extremistas, brindando la oportunidad de comunicarse con individuos y grupos radicales creando, de esta forma, un círculo de validación social.

Cabe recordar el caso del Mayor de la Armada norteamericana Nidal Malik Hassan, que asesinó en la base tejana de Fort Hood a 13 soldados como protesta al apoyo americano a Israel y las guerras en Irak y Afganistán. Su captador e incitador, el imán norteamericano Anwar al-Aulaqi, considerado el "Bin Laden de internet", era un auténtico líder regional de al-Qaeda por su labor de captación y entrenamiento a través de internet y su involucración directa en los atentados del 11 de septiembre. Al-Aulaqi, ingeniero y profesor de formación, fue una persona brillante y conocedora de la potencia de Internet como herramienta sin parangón de influencia socio-política, de propaganda, adiestramiento, movilización, reclutamiento y comunicación con fines de mando y control.

Conclusiones

La ausencia de una gobernanza global de Internet está alimentando el cibermaniqueísmo. Muchos gobiernos se escudan en esta ausencia de gobernanza para radicalizar sus posturas y justificar el modo en el que dirigen, gestionan, operan y controlan su ciberespacio específico.

La era de la ciberutopía –por la cual se minimizaban los rasgos represivos de las nuevas tecnologías y se consideraba que todos los actores involucrados en el ciberespacio eran democráticos– hace tiempo que quedó atrás.

Si bien Internet no es la única herramienta determinante en los procesos de radicalización y reclutamiento de extremistas y terroristas, es innegable el efecto catalizador y expansivo que la red de redes supone para la difusión de ideas y creación de *pensamientos grupales polarizados*.

La ausencia de una gobernanza global de Internet está alimentando el cibermaniqueísmo. Muchos gobiernos se escudan en esta ausencia de gobernanza para radicalizar sus posturas y justificar el modo en el que dirigen, gestionan, operan y controlan su ciberespacio específico.

Su potencia en este sentido viene reforzada por ampliar su marco de referencia, las ambiciones, el radio y campo de acción de los grupos radicales a la medida de un mundo globalizado, haciendo emerger identidades, ideologías, proyectos extremistas transnacionales y globales, y adaptando sus estructuras y actividades mediante el aprovechamiento de las funcionalidades ofrecidas por internet.

En la casuística concreta comentada, intentar controlar los flujos de información en internet a fin de dividir los grupos radicales, se antoja una tarea hercúlea. El control efectivo contra el radicalismo en internet, independientemente de las medidas técnicas adoptadas, pasa por el desarrollo de una actitud individual imparcial, animando el pensamiento crítico, cuestionando la información recibida y buscando críticas externas a las propias. ■

Enrique Fojón Chamorro
Ingeniero Superior en Informática
efojonc@gmail.com

Adolfo Hernández Lorente
Ingeniero Superior en Informática
ahernandez@gmail.com

SPANISH CYBER SECURITY INSTITUTE (SCSI)