Cómo defenderse de la represión digital

Raquel Jorge Ricart

Getty Images

He aquí un repaso a los mecanismos de respuesta frente a las acciones represivas que se llevan a cabo en la esfera virtual.

¿Qué pasaría si, en un día de jornada electoral, todo un país se quedara sin acceso a Internet? No es una sorpresa. Esto –y más– ha ocurrido, y con bastante frecuencia.

En solo cinco meses, desde enero a mayo de 2021, se han registrado más de 50 apagones intencionados de Internet en 21 Estados. 24 de estos 50 afectaron a todo un país al completo, o al menos a la mayoría de regiones de él.

En la región de Yamú y Cachemira, territorio limítrofe de tensiones militares entre India y Pakistán, las autoridades produjeron la caída de Internet al menos en 16 ocasiones solo durante 2021. Pese a que los servicios de 4G volvieron a su normalidad en febrero, desde entonces el Gobierno continúa limitando el acceso a la conectividad móvil. Los argumentos son que representa una medida preventiva ante posibles operaciones militares, o para garantizar el orden público. No cabe olvidar que en esta región se produjo el apagón de Internet más largo de toda la historia, desde agosto de 2019 hasta marzo de 2020. Otros casos son el de Birmania, en donde desde el golpe militar que tuvo lugar en febrero de 2021, la Junta está dando de forma selectiva acceso a la fibra óptica y al cable fijo de Internet a ciertas instituciones, empresas e individuos, y continúa bloqueando el acceso a servicios móvil en ciertas regiones del país.

Represión digital a geometría variable

Ahora bien, no hay una única forma de hacerlo. Tantos otros escenarios adquieren el significado de represión digital: además de los apagones intencionados de Internet (en días de protesta o jornadas electorales), están el control estatal de la información que circula de manera online, la creación de leyes que criminalizan a activistas online protegidos, la persecución extralegal de activistas de redes sociales, el bloqueo de plataformas y páginas web, o ciberataques que van dirigidos a grupos de la sociedad civil y activismo social.

Lo cierto es que la represión digital no es algo particular de una región. En las jornadas electorales de 2021 en Uganda, el presidente Yoweri Musevení decidió bloquear Facebook después de que la plataforma eliminara una red de cuentas vinculadas al Gobierno que difundían información falsa. Caso similar ocurrió en Rusia, donde el Ejecutivo intentó limitar el tráfico de Twitter ante la negativa de la empresa de eliminar ciertas cuentas que el Kremlin pidió borrar.

La represión digital tampoco se limita a países no democráticos. Sucede también en "democracias imperfectas", tal y como las cataloga *The Economist Intelligence Unit*. Entre otros ejemplos está el caso de México, donde un grupo importante de periodistas recibieron ciberataques, concretamente *malwares* (que buscaban infectar sus sistemas) y ataques *DDoS* (para denegar sus servicios de forma distribuida en las redes conectadas de periodistas), dos semanas antes de las elecciones presidenciales de 2018. Un patrón común ha sido que buena parte de estos periodistas han recibido el ciberataque por la misma vía: Pegasus, un *spyware* que se mantenía oculto mientras registraba información. Mientras, Polonia aprobaba en 2016 una nueva ley de vigilancia y de antiterrorismo en la que la definición de "amenaza para la seguridad nacional" recibió críticas, y la ley permitía bloquear páginas web y telecomunicaciones, así como limitar la libertad de asamblea, si se estimaba oportuno.

Menor número, pero mayor vulnerabilidad

Si se miran los datos en un vistazo, se podría decir que 2021 ha sido positivo en comparación a año anteriores. En 2019 se registraron 115 apagones de Internet; en 2020, 60; y en los primeros cinco meses de 2021, 50. Sin embargo, lo cierto es que esto no augura mejoras. Aunque es verdad que el número de apagones de Internet –sin contar las otras expresiones de represión digital– se ha reducido recientemente, estos casos tienden a ser más severos en sus consecuencias para los derechos humanos así como para la propia estabilidad y seguridad de los países.

¿Por qué? Son cada vez más prolongados en el tiempo. La falta generalizada de conocimiento sobre los impactos de la tecnología hace que el camino sea más llano a la hora de instaurar medidas y leyes de control estatal de la información. A ello se une que normalmente en los países con economías menos fuertes no existen tantas personas formadas en ciberseguridad, lo cual hace que, aunque cada vez más personas de Estados empobrecidos se conecten a Internet, no hay infraestructuras ni empresas privadas de ciberseguridad que realmente puedan proteger sus entornos virtuales.

La pandemia causada por la COVID-19 ha llevado a nuevos espacios para la represión digital. La mayor conectividad de las personas a servicios de pago digitales, el comercio electrónico, las aplicaciones de notificaciones de salud, las videollamadas o *simplemente* la creación de una cuenta en una red social para hablar con personas allegadas ha hecho que haya mayor acceso a datos personales, se puedan trazar mejor los movimientos, y que activistas de la sociedad civil que anteriormente se organizaban en persona, ahora se hayan visto obligados a utilizar medios digitales.

Mecanismos de respuesta ante la represión digital

Se podría argumentar que en países donde el grado de conectividad a redes de Internet es bajo no pueden sufrir más represión digital. Sin embargo, el panorama es en realidad otro. Pese a que en los países de África Subsahariana menos del 30% de la población tiene acceso regular a Internet y los propios gobiernos tienen deficiencias cibernéticas críticas para su infraestructura, algunas formas de represión digital –como la extensión de campañas de desinformación– empiezan en lo virtual, pero rápidamente acaban propagándose en el espacio de lo físico, que es donde tiene un impacto significativo.

Los propios grupos que directamente sufren represión digital lo saben, y es por ello que desde hace años han empezado a implantar mecanismos de respuesta.

Algunas comunidades auto-organizadas crean sus propios **sistemas paralelos** a los gestionados por el gobierno y lo expanden a lo largo de la población para que lo use, aunque buena parte de esta en realidad no lo haga con un objetivo político. En Uganda, se descubrió que el 57% de la ciudadanía utiliza aplicaciones de VPNs alternativas para evitar pagar impuestos. Su tráfico en Internet solo queda registrado en una red privada vinculada a un servidor remoto que cifra los datos en tránsito, lo que permite que ninguna empresa ni gobierno pueda rastrear a qué aplicaciones o páginas web se accede. Estas VPNs alternativas fueron creadas por un grupo de personas especializadas en seguridad digital y profesores de escuela y universidad que concienciaban a la población de los riesgos de desinformación en las redes sociales tradicionales.

También surgió como contrarrepuesta a un impuesto sobre las redes sociales que el Gobierno de Uganda implantó en 2018 para bloquear el acceso a plataformas como WhatsApp,Facebook y Twitter. Este impuesto sigue vigente, no se ha reclamado su eliminación por partede ninguna organización civil, y mientras casi dos tercios de la población ugandesa seautoorganizan en redes privadas.

Otros grupos no se autoorganizan, sino que se apoyan en **redes internacionales de apoyo y protección técnicas.** Este caso suele ser frecuente con las diásporas procedentes de países donde su comunidad es vulnerable.

Un ejemplo interesante es la creación de *TibCERT*, el primer Equipo de Respuesta para Emergencias Informáticas para la diáspora tibetana, y cuyos miembros provienen de todo el mundo. Entre noviembre de 2018 y mayo de 2019, un grupo importante de altos cargos de la Administración Central Tibetana, el Parlamento del Tíbet y personas vinculadas tanto al Dalai Lama como a organizaciones de derechos humanos de esta región recibieron enlaces maliciosos en mensajes de WhatsApp de personas que aparentaban ser periodistas de medios de comunicación internacionales o trabajadores de ONG conocidas. Al pulsar sobre el enlace, automáticamente un *spyware* se infiltraba en los móviles de estas personas, interceptando una gran cantidad de información. En esta campaña, llamada *Poison Carp*, todavía no se ha podido atribuir fehacientemente la autoría, pese a la existencia de ciertos patrones.

Las diásporas tibetanas por cuenta propia no tenían el conocimiento suficiente para organizarse. Sin embargo, la alta visibilidad mediática que el Tíbet en general tiene a través de ONG internacionales permitió que se creara con bastante rapidez un CERT para esta región, apoyado por especialistas de todo el mundo desde sus hogares y de forma voluntaria. En él, las comunidades tibetanas se equiparan de mejores ciberdefensas a nivel técnico, su madurez y protección en ciberseguridad ha crecido, y se realizan talleres de concienciación sociales para prevenir gestos, como es abrir un correo sospechoso.

Las campañas de denuncia e incidencia desde el extranjero son otro mecanismo, quizás no para dar respuesta, pero sí para dar visibilidad y reclamar un cambio. Concretamente, la campaña global #KeepItOn, liderada por AccessNow y que representa a 258 organizaciones de 106 países en el mundo, coordina desde una gran organización internacional toda una serie de pequeñas acciones sobre el terreno, como son formar a personas para que monitoreen manifestaciones de represión digital y lo traduzcan en datos, o hacen presión a gobiernos extranjeros para que no presten financiación a gobiernos donde se reprime digitalmente a activistas o se bloquea el derecho a la información.

Otras organizaciones financian la creación de **nuevas secciones tecnológicas dentro de sus organizaciones de incidencia.** Si bien es cierto que al principio no va a suponer grandes campañas de denuncia, poder empezar a hacer investigación permite a las organizaciones entrar en contacto con activistas sobre el terreno de una forma mucho más cercana. En este sentido, el European AI Fund se encarga de analizar solicitudes para finalmente dotar de cantidades importantes de dinero a ONG temáticas para la creación de secciones de incidencia en temas tecnológicos. Un caso parecido ocurre con Digital Freedom Fund, que financia litigios en materia de derechos digitales o aporta presupuesto para poder hacer investigaciones antes de entrar en fase judicial.

Algunos programas para la promoción de la democracia empiezan a desplegar acciones para situaciones de represión digital. Tal y como se observa a partir de los datos del *Election Watch in the Digital Age* realizado por The Freedom House, para cada forma de represión

digital se necesitan mecanismos de respuesta específicos.

En ese sentido, destaca el caso de la Unión Europea, que ya ha preparado cinco líneas de trabajo para abordar la represión digital en aquellos países no pertenecientes a la Unión con quienes ha trabajado habitualmente para la promoción de la democracia, cooperación al desarrollo o seguridad.

Así, a través del tradicional Instrumento Europeo para la Democracia y los Derechos Humanos (EIDHR), las misiones de observación electoral (EOMs) y las misiones de seguimiento electoral (EFMs) ya incorporan un eje sobre distorsiones online de los procesos electorales. Empezó con Kenia y Sri Lanka en 2018, y sigue hasta el momento.

Garantizar el pluralismo de los medios de comunicación tampoco es sencillo en lo digital. Así, el proyecto Media4Democracy, que se despliega en las Delegaciones Diplomáticas de la UE en el extranjero, tiene como prioridades combatir la violencia y amenazas a la libertad de expresión online, proteger el derecho a la información veraz y fortalecer el derecho a la privacidad, entre otros.

Por otra parte, también se trabaja en la protección y fomento del activismo online. Las iniciativas Supporting Democracy y CivicTech4Democracy destinan financiación para talleres en donde se promueve que el activismo social en países no democráticos pueda hacerse en lo digital, y además de forma segura. En caso de necesitar proteger a activistas a nivel legal, el mecanismo ProtectDefenders.eu da formaciones sobre cómo protegerse digitalmente, y también permite la reubicación temporal de personas para poder apoyar en procedimientos judiciales sobre este aspecto.

Finalmente, la alfabetización digital es otro aspecto relevante en el que el European Endowment for Democracy trabaja para hacer que los *bloggers* sepan protegerse de forma muy específica y puedan construir redes de apoyo a nivel local.

Un reto de gran calibre

Aunque existan mecanismos de respuesta integrales, el reto mayor es conocer su impacto real y conducir a que realmente las manifestaciones de represión digital disminuyan. A veces se dice que estas existen porque hay unos proveedores que ofrecen los sistemas para hacerlo. Sin embargo, la represión digital no es más que la continuación de la represión física que ya ocurría en tiempos pasados. Lo online ha acelerado y diversificado tanto las formas de represión como también las de movilización política y social. Ha generado espacios de exclusión al mismo

tiempo que ha abierto nuevos espacios de posibilidad.

Reconfigura las fronteras de lo virtual, y también de lo físico. Pero, sobre todo, transforma la manera en que pensamos nuestra “libertad cognitiva”. ¿Seremos capaz de identificar las consecuencias positivas y negativas de lo digital como un desafío real, material, diario, en nuestra forma de entender nuestra individualidad?

Fecha de creación
13 julio, 2021