REPRESIÓN DIGITAL: EL CONTROL ESTATAL DE LA POBLACIÓN A TRAVÉS DE MEDIDAS DIGITALES

STEVEN FELDSTEIN
Investigador sénior en el Programa de Democracia, Conflicto y Gobernanza, Carnegie Endowment for International Peace

IRIS FIONA BRAUER
Investigadora James C. Gaither en el Programa de Democracia, Conflicto y Gobernanza, Carnegie Endowment for International Peace

Elena Kostyuchenko sabía que debía ser prudente. Como colaboradora de *Novaya Gazeta*, una de las últimas publicaciones rusas abiertamente críticas con el presidente Vladímir Putin, estaba familiarizada con la prolongada represión del Kremlin contra los medios de comunicación independientes. Debido a su cobertura antibélica, la censura rusa obligó a este periódico a abandonar Internet, bloqueando su sitio web para los lectores rusos habituales y obligando a la propia Kostyuchenko a huir del país. En Alemania, Kostyuchenko se sentía más segura y con más libertad para escribir contra Putin y la guerra. Por eso, cuando de pronto cayó gravemente enferma de una dolencia en apariencia imposible de diagnosticar, tardó varios meses en aceptar que probablemente había sido envenenada por agentes rusos. Había dado por hecho que residir en Berlín le proporcionaría cierta protección, pero se equivocaba; las fuerzas de seguridad rusas habían dado con ella, probablemente a través de su cuenta de Messenger. La historia de Kostyuchenko revela hasta qué punto está dispuesto a llegar el Gobierno ruso para reprimir la disidencia, especialmente en lo que respecta al disenso sobre la guerra en Ucrania.

Las autoridades rusas están utilizando diferentes herramientas digitales para intimidar a los activistas y extender el miedo entre la población. Los agentes de seguridad emplean la tecnología de reconocimiento facial (FRT, por su sigla en inglés) para identificar y detener a manifestantes (véase el artículo de Lena Masri, «Facial recognition is helping Putin curb dissent with the aid of U.S. tech», Reuters, 2023), y la policía recurre a ella para rastrear y señalar a los insumisos. Se trata de una tecnología muy extendida en Moscú –donde está presente en cámaras, a pie de calle, y hasta en el escaneo biométrico del metro–, y que se está extendiendo rápidamente a otras áreas del país. Además del reconocimiento facial, el Kremlin emplea el Sistema para Actividades de Investigación Operativa (SORM, por su sigla en ruso) para monitorizar los dispositivos de los ciudadanos, un sistema que ha demostrado ser particularmente útil para rastrear la disidencia y que ha permitido a las autoridades recopilar gran cantidad de datos sobre los críticos al régimen. SORM es solo una pieza del proyecto ruso de censura en línea, gran parte del cual se ejecuta a través de Roskomnadzor, la agencia responsable de la supervisión y el control de Internet. Las tácticas de esta agencia incluyen el bloqueo de sitios web que publiquen contenido contra la guerra y la restricción de acceso a plataformas occidentales como Facebook. Recientemente, Roskomnadzor ha empezado a bloquear también los servicios de VPN (red privada virtual), para cortar las últimas vías de acceso al Internet externo. Este recurso de Rusia a las herramientas digitales para la vigilancia y la censura es un reflejo de una tendencia mundial más amplia. En todo el planeta, los conflictos y la inseguridad política van en aumento y cada vez más son los gobiernos que recurren a herramientas

digitales para reforzar su represión e incrementar su seguridad.

Las medidas implementadas por Irán constituyen en este punto un buen ejemplo. El régimen ha recurrido con frecuencia a los cortes y restricciones de Internet para limitar el acceso al Internet global, a lo que ha añadido la criminalización de las VPN y el bloqueo del acceso de los usuarios a tiendas de aplicaciones, obligando así a sus ciudadanos a ingresar en la Red Nacional de Información, controlada por el Estado. Para monitorizar a su población –por ejemplo, a la hora de hacer cumplir a las mujeres con las leyes del velo obligatorio– Irán utiliza cada vez más tanto el FRT como la biometría (véase el artículo de Mahsa Alimardani, «Aggressive New Digital Repression in Iran in the Era of the Woman, Life, Freedom Uprisings», en *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*, Carnegie 2023), integrados en sistemas de vigilancia más amplios. Aunque el alcance y la capacidad del seguimiento biométrico del Gobierno no están claros, la incertidumbre y el miedo creados por la amenaza de esta tecnología ilustran los efectos escalofriantes de la represión preventiva; las herramientas de vigilancia digital limitan la disidencia sin necesidad de arrestos ni castigos.

Los conflictos y la inseguridad política van en aumento y cada vez más son los gobiernos que usan herramientas digitales para reforzar su represión e incrementar su seguridad

También Myanmar permite ilustrar esta cuestión. A raíz del golpe de Estado de 2021, la junta militar bloqueó inmediatamente el acceso a las redes sociales, prohibió las VPN y autorizó el cierre completo de Internet (aunque ya antes del golpe el Gobierno elegido democráticamente también había cortado Internet en zonas en conflicto, demostrando que estas tácticas no solo las utilizan los gobiernos autoritarios). Al carecer del aparato de vigilancia centralizado de Rusia, el ejército de Myanmar recurrió al *hackeo* telefónico de empresas rusas, estadounidenses, europeas y chinas para supervisar y castigar a los disidentes.

Tanto en Myanmar como en Rusia, a las empresas de telecomunicaciones e Internet que no se han plegado a las demandas estatales, o bien se las ha expulsado, o bien han sido puestas bajo control gubernamental. El intento de establecer un Internet nacional completamente controlado por el Estado y aislado del Internet global es, de hecho, una tendencia creciente en los países autoritarios. En el caso de China, las autoridades iniciaron el control estatal sobre Internet con el «Gran Cortafuegos», un sistema de censura que bloquea sitios y plataformas internacionales, supervisa y elimina contenidos, a la vez que difunde propaganda (véase el informe «Freedom on the net, China», *Freedom House*, 2023). Y son muchos los países que tratan de emular el modelo chino. Rusia y China han dado muestras, a través de sucesivas reuniones, de una creciente cooperación entre las dos potencias en tácticas de represión digital; los funcionarios chinos han compartido recomendaciones sobre cómo impedir el uso de VPN, descifrar el tráfico cifrado y regular las plataformas. En paralelo, el esfuerzo ruso por crear un Internet propio, controlado y aislado, dio lugar a una ley que, en 2019, sentó las bases para una «RuNet» soberana, con gestión estatal centralizada y la instalación obligatoria de equipos para el control del tráfico y el servicio (véase Zak Doffman, «Putin's 'Internet Kill Switch' Suddenly Gets Real», *Forbes*, 2024).

En su empeño por controlar totalmente Internet, los estados no titubean a la hora de

bloquear a las empresas y plataformas globales. Por ejemplo, tras la invasión de Ucrania, Rusia bloqueó los sitios de Facebook y Twitter por considerarlos extremistas. La realidad es que estos sitios pueden ofrecer un acceso crítico a noticias y a la comunicación y que su bloqueo permite un mayor control por parte del Estado. Sin embargo, la alternativa puede ser incluso más preocupante, si las empresas que permanecen en entornos en los que existe represión sobre Internet, y ante la posibilidad de perder cuota de negocio, se tornan complacientes con las demandas y presiones de los gobiernos. Un ejemplo de ello tuvo lugar antes de las elecciones turcas de 2023, cuando Twitter eliminó publicaciones críticas con el presidente Recep Tayyip Erdogan a petición del Gobierno. Y algo parecido sucedió en China, donde la función AirDrop de Apple se utilizó para compartir imágenes de protestas y mensajes críticos con Xi Jinping y con el Partido Comunista Chino (los activistas a favor de la democracia en Hong Kong compartieron, por ejemplo, de forma anónima, lemas de protesta con turistas de la China continental). La función AirDrop había eludido con éxito las herramientas chinas de censura, motivo por el cual Apple redujo rápidamente su capacidad, probablemente debido a la presión de las autoridades chinas.

Las medidas digitales coercitivas no son exclusivas de los países autoritarios, como demuestran los ejemplos de Israel e India. Israel ha recibido una mayor atención en los últimos meses por su uso de la tecnología de reconocimiento facial, que empezó a desplegar antes del actual conflicto en Gaza. Durante años, el ejército israelí ha utilizado datos biométricos para identificar a los palestinos en Gaza y Cisjordania, pero existen informes que apuntan a un programa nuevo y más amplio, en el que las fuerzas de seguridad han recopilado y catalogado datos de cientos de palestinos sin su consentimiento para un programa experimental de vigilancia masiva con el fin de supervisar a ciertas personas de interés. La recopilación de datos se ha ampliado aún más debido al uso de cámaras equipadas con FRT por parte de los soldados, más allá de los *checkpoints* y en la propia Franja de Gaza. Según los informes de *+972* y *Local Call*, el aparato de vigilancia de Israel está alimentando un nuevo sistema basado en IA que produce objetivos para ataques militares (véase Yuval Abraham, «"Lavender": The AI machine directing Israel's bombing spree in Gaza», *+972 Magazine*, 2024).

En India, el uso de la vigilancia de alta tecnología ha crecido a la par que su larga práctica de cortes y restricciones de Internet. Mediante el despliegue de drones y cámaras de vigilancia en las protestas, el Gobierno indio ha utilizado el FRT para identificar y arrestar a manifestantes y ha instalado cámaras permanentes, con el propósito de desalentar la disidencia entre las minorías y castigar las protestas cuando estas se producen.

Estos diferentes ejemplos demuestran el creciente atractivo de la tecnología digital para los gobiernos que tienen puesto su empeño en frenar la disidencia y consolidar el control sobre sus poblaciones, y son medidas que demuestran ser cada vez más efectivas a la hora de limitar la disidencia tanto en línea como en el mundo físico.