REPRESSIÓ DIGITAL: EL CONTROL ESTATAL DE LA POBLACIÓ AMB MESURES DIGITALS

STEVEN FELDSTEIN
Investigador sènior al Programa de Democràcia, Conflicte i Governança, Carnegie Endowment for International Peace

IRIS FIONA BRAUER
Investigadora James C. Gaither al Programa de Democràcia, Conflicte i Governança, Carnegie Endowment for International Peace

Elena Kostiutxenko sabia que havia de ser prudent. Com a col·laboradora de *Nóvaia Gazeta*, una de les últimes publicacions russes obertament crítiques amb el president Vladímir Putin, estava familiaritzada amb la repressió del Kremlin contra els mitjans de comunicació independents. A causa de la seva cobertura antibèl·lica, la censura russa va obligar aquest diari a abandonar Internet, bloquejant el seu lloc web per als lectors russos habituals i obligant Kostiutxenko a fugir del país. A Alemanya, Kostiutxenko se sentia més segura i amb més llibertat per escriure contra Putin i la guerra. Per això, quan de sobte es va veure greument afectada per una malaltia en aparença impossible de diagnosticar, va tardar diversos mesos a acceptar que probablement havia estat enverinada per agents russos. Havia donat per fet que residir a Berlín li proporcionaria certa protecció, però s'equivocava; les forces de seguretat russes havien arribat fins on era, probablement a través del seu compte de Messenger. La història de Kostiutxenko revela fins a quin punt el Govern rus està disposat a reprimir la dissidència, especialment en el tema de la guerra a Ucraïna.

Les autoritats russes utilitzen diferents eines digitals per intimidar els activistes i estendre la por entre la població. Els agents de seguretat fan servir la tecnologia de reconeixement facial (FRT, per la seva sigla en anglès) per identificar i detenir manifestants (vegeu l'article de Lena Masri, «Facial recognition is helping Putin curb dissent with the aid of U.S. tech», *Reuters*, 2023), i la policia hi recorre per rastrejar i assenyalar els insubmisos. Es tracta d'una tecnologia molt habitual a Moscou –on la trobem present en càmeres, a peu de carrer o en l'escaneig biomètric del metro–, i que s'està estenent ràpidament a altres àrees del país. A més del reconeixement facial, el Kremlin fa servir el Sistema per a Activitats d'Investigació Operativa (SORM, en la seva sigla en rus) per monitorar els dispositius dels ciutadans, un sistema que ha demostrat ser particularment útil per rastrejar la dissidència i que ha permès a les autoritats recopilar gran quantitat de dades sobre els crítics al règim. SORM és només una peça del projecte rus de censura en línia, gran part del qual s'executa a través de Roskomnadzor, l'agència responsable de la supervisió i el control d'Internet. Les tàctiques d'aquesta agència inclouen el bloqueig de llocs web que publiquin contingut contra la guerra i la restricció d'accés a plataformes occidentals com Facebook. Recentment, Roskomnadzor ha començat a bloquejar també els serveis de VPN (xarxa privada virtual), per tallar les últimes vies d'accés a la Internet externa. Aquest recurs de Rússia a les eines digitals per a la vigilància i la censura és un reflex d'una tendència mundial més àmplia. A tot el planeta, els conflictes i la inseguretat política van en augment i cada vegada hi ha més governs que recorren a eines digitals per reforçar la repressió i incrementar la seva seguretat.

Un bon exemple són, en aquest sentit, les mesures implementades per l'Iran. El règim

ha fet ús amb freqüència dels talls i les restriccions d'Internet per limitar l'accés a la Internet global, ha criminalitzat l'ús de les VPN i ha bloquejat l'accés dels usuaris a les botigues d'aplicacions, obligant els seus ciutadans a ingressar a la Xarxa Nacional d'Informació, controlada per l'Estat. Per monitorar la seva població –per exemple, a l'hora de fer que les dones compleixin les lleis del vel obligatori– l'Iran utilitza cada vegada més tant l'FRT com la biometria (vegeu l'article de Mahsa Alimardani, «Aggressive New Digital Repression in Iran in the Era of the Woman, Life, Freedom Uprisings», a *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*, Carnegie 2023), integrats en sistemes de vigilància més amplis. Encara que l'abast i la capacitat de seguiment biomètric del Govern no estan clars, la incertesa i la por creades per l'amenaça d'aquesta tecnologia il·lustren els efectes esgarrifosos de la repressió preventiva; les eines de vigilància digital limiten la dissidència sense necessitat d'arrestar ni castigar la població.

Els conflictes i la inseguretat política van en augment i cada vegada hi ha més governs que utilitzen eines digitals per reforçar la repressió i incrementar la seva seguretat

També Myanmar permet il·lustrar aquesta situació. Arran del cop d'Estat de 2021, la junta militar va bloquejar immediatament l'accés a les xarxes socials, va prohibir les VPN i va autoritzar el tancament complet d'Internet (encara que, ja abans del cop d'Estat, el Govern elegit democràticament també havia tallat Internet en zones en conflicte, demostrant que aquestes tàctiques no només les utilitzen els governs autoritaris). L'exèrcit de Myanmar, que no disposa de l'aparell de vigilància centralitzat que té Rússia, va recórrer al hackeig telefònic d'empreses russes, estatunidenques, europees i xineses per supervisar i castigar els dissidents.

Tant a Myanmar com a Rússia, les empreses de telecomunicacions i proveïdores d'Internet que no s'han doblegat a les demandes de l'Estat, o bé han estat expulsades, o bé han quedat sota control governamental. L'intent d'establir una Internet nacional completament controlada per l'Estat i aïllada de la Internet global és, de fet, una tendència que creix als països autoritaris. En el cas de la Xina, les autoritats van iniciar el control estatal sobre Internet amb el «Gran Tallafoc», un sistema de censura que bloqueja llocs i plataformes internacionals, supervisa i elimina continguts, alhora que difon propaganda (vegeu l'informe «Freedom on the net, China» *Freedom House*, 2023). I són molts els països que proven d'emular el model xinès. Rússia i Xina han demostrat, en successives reunions, l'existència d'una cooperació creixent en tàctiques de repressió digital entre les dues potències; els funcionaris xinesos han compartit recomanacions sobre com impedir l'ús de les VPN, desxifrar el trànsit xifrat i regular les plataformes. En paral·lel, l'esforç rus per crear una Internet pròpia, controlada i aïllada, va donar lloc a una llei que, el 2019, va establir les bases d'una «RuNet» sobirana, amb gestió estatal centralitzada i la instal·lació obligatòria d'equips per al control del trànsit i el servei (vegeu Zak Doffman, «Putin's 'Internet Kill Switch' Suddenly Gets Real», *Forbes*, 2024).

En el seu afany per controlar totalment Internet, els estats no titubegen a l'hora de bloquejar les empreses i plataformes globals. Per exemple, després de la invasió d'Ucraïna, Rússia va bloquejar Facebook i Twitter per considerar-los extremistes. La realitat és que aquests llocs poden oferir un accés crític a notícies i a la comunicació i el seu bloqueig

permet a l'Estat exercir un control més gran. Tanmateix, l'alternativa pot ser fins i tot més preocupant, si les empreses que romanen en entorns en els quals hi ha repressió sobre Internet, i davant de la possibilitat de perdre quota de negoci, es tornen complaents amb les demandes i pressions dels governs. Un exemple d'això va tenir lloc abans de les eleccions turques de 2023, quan Twitter va eliminar publicacions crítiques amb el president Recep Tayyip Erdogan a petició del Govern. I una situació semblant va passar a la Xina, on la funció AirDrop d'Apple es va utilitzar per compartir imatges de protestes i missatges crítics amb Xi Jinping i amb el Partit Comunista Xinès (els activistes a favor de la democràcia a Hong Kong van compartir, per exemple, de forma anònima, lemes de protesta amb turistes de la Xina continental). La funció AirDrop havia eludit amb èxit les eines xineses de censura, motiu pel qual Apple va reduir ràpidament la seva capacitat, probablement a causa de la pressió de les autoritats xineses.

Les mesures digitals coercitives no són exclusives dels països autoritaris, com demostren els exemples d'Israel i l'Índia. Israel ha acaparat l'atenció aquests últims mesos per l'ús que ha fet de la tecnologia de reconeixement facial, que va començar a desplegar abans de l'actual conflicte a Gaza. Durant anys, l'exèrcit israelià ha utilitzat dades biomètriques per identificar els palestins a Gaza i Cisjordània, però, segons alguns informes, disposa d'un programa nou i més ampli que ha permès a les forces de seguretat recollir i catalogar dades de centenars de palestins sense el seu consentiment per a un programa experimental de vigilància massiva a fi de supervisar persones determinades. La recopilació de dades s'ha ampliat encara més a causa de l'ús de càmeres equipades amb FRT per part dels soldats, més enllà dels *checkpoints* i a la mateixa Franja de Gaza. Segons els informes de *+972* i *Local Call*, l'aparell de vigilància d'Israel està alimentant un nou sistema basat en IA que produeix objectius per a atacs militars (vegeu Yuval Abraham, «"Lavender": The AI machine directing Israel's bombing spree in Gaza», *+972 Magazine*, 2024).

A l'Índia, ha crescut l'ús de la vigilància d'alta tecnologia al mateix temps que ho feia la llarga pràctica de talls i restriccions d'Internet. Mitjançant el desplegament de drons i càmeres de vigilància durant les protestes, el Govern indi ha utilitzat l'FRT per identificar i arrestar manifestants i ha instal·lat càmeres permanents per descoratjar la dissidència entre les minories i castigar les protestes quan es produeixen.

Aquests exemples en llocs diferents demostren l'atractiu en augment que té la tecnologia digital per als governs que estan decidits a frenar la dissidència i consolidar el control sobre les seves poblacions. Són mesures que cada vegada són més efectives a l'hora de limitar la dissidència tant en línia com al món físic.