L'eina en mans equivocades. Privacitat i vigilància en l'era digital

vista prèvia >

En plena societat de la informació, la privacitat afronta nous reptes. La seguretat de les dades personals sembla estar en entredit. Qui hauria de tenir-hi accés? Com es pot garantir que siguin secretes? L'amenaça terrorista ha imposat la necessitat d'incrementar la vigilància, posant en tensió el dret a la privadesa de les comunicacions, una eina bàsica per a qualsevol societat democràtica.

Ferran Esteve
Politòleg i periodista
@ferranesteve

Totes les societats i grups humans se sostenen en la creença que les normes que els regeixen són fruit d'un acord entre els seus membres, que s'han dotat per voluntat pròpia d'uns drets i deures vàlids per viure en comunitat. És el que en filosofia política s'anomena «contracte social». Malgrat que mai no ha estat redactat ni signat, un nou tipus de contracte social regeix la societat de la informació. Es basa en la presumpció que els usuaris d'internet entreguen de manera lliure tota mena de dades personals a tercers pel sol fet de fer servir la tecnologia o, de manera més acurada, per acceptar uns *terms of service*. L'ús d'aquesta informació per un petit grup d'empreses privades és inquietant, però pren un caire distòpic quan també els governs les empren per al control polític, tant en països democràtics com autoritaris.

La creença que els estats espien la seva pròpia ciutadania és un fet comú que s'accepta amb una inusitada normalitat, probablement per la falta de proves en el dia a dia. Aquesta sospita, però, és ja una certesa gràcies a les filtracions d'Edward Snowden (1983). El 2013, aquest consultor tecnològic dels EUA va revelar que la National Security Agency (NSA) estava emmagatzemant dades de comunicacions personals de tots els ciutadans del seu país.[1] No es tractava d'escoltes telefòniques, ni d'un seguiment de persones concretes, però sí de la recopilació massiva de metadades, incloent adreces de correu electrònic, números de telèfon, registres de trucades, data i hora de les comunicacions... Per si no fos prou, la filtració també va oferir detalls del programa PRISM —acrònim de Planning Tool for Resource Integration, Synchronization and Management— [Eina de planificació per a la integració, la sincronització i la gestió de recursos], a través del qual, la NSA monitoritzava habitants d'altres països a través de productes i serveis oferts per una desena d'empreses nord-americanes, sense respectar la legislació d'aquests estats.

Les revelacions d'Snowden van despertar crítiques arreu del món, esperonades en saber-se que altres governs democràtics tenien programes de vigilància semblants. Un fet que no va impedir tensions diplomàtiques, com la sorgida arran de les suposades escoltes —negades pels EUA— que la NSA havia fet a la cancellera alemanya Angela Merkel (1954). Tot i així, només cinc anys després d'aquell escàndol, aquests sistemes segueixen vigents, i la majoria d'estats inverteixen en tecnologies de vigilància similars als de la NSA, fent servir sovint l'amenaça terrorista com a excusa.

El mal del terror, el remei de la vigilància

La societat actual s'enfronta a un nou tipus de repte: el de l'enemic que no es presenta a la frontera en forma d'exèrcit sinó d'individu que es radicalitza dins el propi espai social. Aquesta nova amenaça només es pot neutralitzar amb prevenció i vigilància en xarxa, coneixent tant a les persones sospitoses, com per avançar-se als seus moviments. Per al politòleg alemany Herfried Münkler (1951), aquest escenari implica amenaces evidents per a la privacitat, però en cas de rebutjar-se, significaria assumir que els atacs terroristes

1 MACASKILL i DANCE, «NSA Files: Decoded. What the revelations mean for you».

La creença que els estats espien la seva pròpia ciutadania és un fet comú que s'accepta amb una inusitada normalitat, probablement per la falta de proves en el dia a dia

són inevitables. Per a això, afirma el professor de la Humboldt-Universität Zu Berlin, caldrien societats heroiques, capaces de sacrificar la seguretat per tal de salvaguardar la llibertat, però el món actual està regit per societats postheroiques, que no estan disposades a acceptar aquest tipus de violència.

Durant les dues darreres dècades, l'amenaça terrorista s'ha convertit en el motor de la indústria de la seguretat, tant en països democràtics com autoritaris. Els estats han afrontat aquest temor dotant de majors recursos als seus serveis d'intel·ligència i modificant les legislacions per tal de facilitar la seva tasca. Aquesta deriva securitària, però, s'ha convertit en una arma de doble tall, ja que sovint s'ha emprat com una eina contra la ciutadania i no contra aquells que amenacen l'estat.

En el cas dels països autoritaris o amb democràcies limitades, on les garanties judicials són més escasses, les conseqüències d'aquests nous marcs legals són especialment esfereïdores. Fent ús de lleis antiterroristes molt àmplies, aquests països imposen penes excessives per a l'activitat en línia, que tenen a veure més amb motius polítics que de seguretat nacional. Així, aquestes mesures, s'han fet servir contra activistes no violents i periodistes, com és el cas de Sayed Ahmed al-Mousawi, un guardonat fotoperiodista de Bahrain, que el 2015 va ser condemnat a deu anys de presó per repartir targetes SIM a manifestants «terroristes» i fotografiar protestes antigovernamentals.[2] En un altre cas destacat del mateix any, un tribunal rus va condemnar a cinc anys de presó al blogaire Vadim Tyumentsev (1980). Se l'acusava de publicar missatges animant a protestar de manera pacífica contra els preus del transport públic i de criticar la intervenció russa a Ucraïna.

En una tendència creixent i molt preocupant, fins i tot s'ha fet servir la legislació antiterrorista contra ciutadans comuns pel sol fet de publicar o difondre algun contingut crític, tal com ha alertat l'ONG Freedom House.[3] El 2016 al Pakistan, un home va rebre una condemna de tretze anys de presó només per fer «m'agrada» a un missatge de Facebook crític amb l'islam.[4] A l'Estat espanyol, des del 2014, l'anomenada «Operació Aranya» de la Guàrdia Civil ha detingut més de 70 persones acusades d'enaltiment del terrorisme i humiliació de les víctimes, en molts casos només per publicar acudits a Twitter. Malgrat dur-se a terme en una democràcia amb garanties judicials, les sentències derivades, algunes d'elles amb condemnes de presó, han suscitat crítiques per la desproporcionalitat i fonamenten les bases per promoure l'autocensura dels usuaris d'internet.

Més accés, més control

Fins fa tan sols uns anys, la capacitat d'alguns governs per dur a terme tasques de vigilància massiva era limitada. No obstant, a mesura que augmenta la penetració d'internet i la tecnologia es torna més assequible, la majoria de països del món ha anat accedint a aquestes eines de control.

2 INDEX OF CENSORSHIP, «Bahrain: NGOs express concern over arrest of photojournalist Sayed Ahmed Salman al-Mousawi».

3 FREEDOM HOUSE, *Freedom on the Net 2017*.

4 AGENCE FRANCE PRESS, «Pakistani jailed for 13 years for Facebook post».

La societat s'enfronta a un nou tipus de repte: el de l'enemic que no es presenta a la frontera en forma d'exèrcit sinó d'individu que es radicalitza dins el propi espai social

L'Aràbia Saudita, per exemple, va aixecar el 2017 la prohibició sobre les aplicacions que ofereixen serveis de veu i videotrucades, però prèviament havia contractat experts que els ajudessin a interceptar-les. A Egipte, els consellers del president Mohamed Mursi (1951) es van reunir amb el cap d'espies iranià el 2012 per demanar assistència en la construcció d'un aparell de vigilància. Fins i tot a la Líbia posterior a Moammar al-Gaddafi (1969-2011), informes de 2012 afirmaven que s'havien tornat a posar en marxa les eines de control de l'antic règim dictatorial.

Encara que alguns estats no puguin dur a terme inversions multimilionàries en vigilància, poden obtenir eines de control tecnològic amb certa facilitat. Algunes tècniques de *hacking,* com ara la intercepció d'SMS que contenen contrasenyes d'usuaris, són assequibles i permeten accedir a dispositius concrets d'una manera senzilla. En aquest camp destaca l'enviament de correus electrònics enganyosos per tal d'obtenir dades personals, l'anomenat *phishing*. A Egipte, una operació governamental anomenada «Nile Phish» va provar d'obtenir informació confidencial de les organitzacions de drets humans del país en el marc d'una onada repressiva que va començar el 2011.[5] Activistes de l'oposició política a Bahrain o Malàisia també han estat atacats amb programari maliciós i als Emirats Àrabs Units, un programa espia desenvolupat a Israel, es va fer servir contra el defensor de drets humans Ahmed Mansoor.[6] Cal remarcar que aquesta pràctica també ha estat emprada per governs democràtics, inclosos els dels EUA i Alemanya, per dur a terme investigacions criminals. En aquests casos, però, les actuacions policials acostumen a venir precedides d'una ordre judicial que les autoritza.

Afortunadament, hi ha governs que encara no han assolit un nivell d'alfabetització digital elevat, de manera que malgrat que existeix la voluntat de controlar la ciutadania, les tàctiques emprades no sempre ho fan possible. El cas més remarcable és el del Kazakhstan, on el 2015 el Govern va intentar establir un Certificat de Seguretat Nacional mitjançant una llei que obligava a tots els seus ciutadans a descarregar-se un programari i instal·lar-lo als seus dispositius, facilitant així l'espionatge.[7] La idea va sorgir de persones que probablement no comprenen com funciona internet, ja que confiaven que la manera més eficaç d'espiar la ciutadania és ordenant a milions de persones que s'instal·lin un sistema que permet trencar el secret de les seves comunicacions.

La batalla pel xifratge

Malgrat que la criptografia, la disciplina que estudia tècniques per a xifrar missatges, es remunta com a mínim a l'Antic Egipte, és en la societat de la informació quan aquest àmbit del coneixement s'ha tornat fonamental. Internet i la informàtica en general necessiten d'aquesta eina per garantir la seguretat de milions de processos i transaccions que succeeixen a diari, incloent les econòmiques.

5 SCOTT-RAILTON, «Nile Phish. Large-Scale Phishing Campaign Targeting Egyptian Civil Society».

6 AL JAZEERA, «Rights advocates call on UAE to release Ahmed Mansoor».

7 WOLF, «Kazakhstan's Unsettling New Cybersecurity Plan».

Durant les dues darreres dècades, l'amenaça terrorista s'ha convertit en el motor de la indústria de la seguretat, tant en països democràtics com autoritaris

Arran de les revelacions d'Edward Snowden, les empreses tecnològiques han mostrat un renovat interès per garantir la seguretat dels seus dispositius. La indignació popular per l'espionatge a escala massiva ha obligat les companyies a adoptar el xifrat per defecte com a eina essencial per protegir el seu model de negoci. Aquesta decisió, però, no ha estat percebuda com a beneficiosa per pràcticament cap govern del món, tampoc en democràcies avançades, que sovint entenen el secret de les comunicacions com un mecanisme per protegir l'activitat criminal.

Aquesta discrepància entre empreses i governs va tenir el seu cas més emblemàtic el 2015, quan un tribunal de districte dels EUA va ordenar a Apple que creés un nou programa per trencar les seves pròpies mesures de seguretat, de manera que les autoritats poguessin desbloquejar el telèfon del terrorista que havia atemptat a Califòrnia aquell mateix any. La companyia va negar-se a fer-ho per tal d'evitar un precedent legal perillós, però els serveis d'intel·ligència van aconseguir finalment accedir al dispositiu per si sols, de manera que no queda clar com es podria resoldre un litigi similar en el futur.

Al continent europeu, França i Alemanya han augmentat la pressió per reforçar els seus mecanismes de seguretat, i a l'agost de 2016 van fer una petició a la Comissió Europea per obligar els fabricants d'aplicacions xifrades a lliurar dades en casos de terrorisme. Juntament amb aquests dos, Bahrain, Cuba, Hongria, l'Índia, el Regne Unit, Tailàndia, Vietnam i la Xina han aprovat o impulsen lleis per limitar el xifratge o poder trencar-lo a demanda, oferint a l'estat el que s'anomena *backdoor access* [accés per la porta posterior], que els permetria consultar missatges privats de manera puntual. Malgrat que aquest recurs acostuma a reservar-se per a casos criminals, cal tenir en compte que en alguns d'aquests països la legislació es pot fer servir contra els defensors del drets humans i els periodistes, ja que les formes bàsiques d'expressió i dissidència són il·legals en moltes jurisdiccions.

Una atenció especial mereix el cas de Rússia, que s'ha convertit en un dels capdavanters en el camp de la vigilància tecnològica. El 2016, les autoritats d'aquest país van aprovar una llei antiterrorista que obliga els proveïdors d'internet a facilitar el desxifrat sempre que el Servei de Seguretat Federal, el successor del KGB, ho consideri necessari. També els exigeix que emmagatzemin les metadades dels usuaris durant tres anys, així com el contingut de les comunicacions —trucades, textos, imatges, vídeos i altres dades— durant sis mesos.

No cal deixar de banda el fet que, en aquestes tensions per trencar el xifratge, les empreses proveïdores d'internet són un actor necessari. Companyies com Microsoft han demandat els EUA per reclamar el seu dret a informar els clients si les seves dades estan sent consultades per les agències estatals. Però aquesta resistència és més limitada en països que no tenen institucions judicials lliures i independents, on les companyies tenen poques opcions: o bé compleixen amb les demandes estatals o les seves aplicacions poden ser bloquejades, els poden expulsar del país o fins i tot detenir el seu personal local. La pròpia Microsoft no ha lliurat batalla

La deriva securitària s'ha convertit en una arma de doble tall, ja que sovint s'ha emprat com una eina contra la ciutadania i no contra aquells que amenacen l'estat

a Tailàndia, per exemple, on ha estat acusada per l'organització Privacy International de facilitar l'espionatge del Govern militar al poder.[8]

La vulnerabilitat de les companyies és un tema de reflexió per a molts activistes i periodistes que fan servir els seus sistemes. Tot i que molts canals de comunicació són públics, només ho són fins allà on els seus propietaris ho permeten. Com escriu el professor del Massachusetts Institute of Technology Media Lab, Ethan Zuckerman (1973), cal entendre que allotjar un moviment polític en una xarxa social propietat d'una empresa privada «és com intentar organitzar una manifestació en un centre comercial. Sembla un espai públic, però no ho és».[9] Molts dels canals que es fan servir per a la discussió política en línia estan pensats en última instància per protegir els interessos dels accionistes i no de l'usuari, cosa que es fa evident quan un govern els obliga a complir les seves peticions.

8 PRIVACY INTERNATIONAL, «Who's that knocking atmMy door? Understanding Surveillance In Thailand».

9 ZUCKERMAN, «Public Spaces, Private Infrastructure – Open Video Conference».

L'anonimat digital, eina democràtica

Després d'uns primers anys d'eufòria en què usuaris de tot el món aprenien noves formes de socialització en línia, les xarxes socials han mostrat certes derives no desitjables, com ara la reproducció de comportaments discriminatoris que podríem agrupar sota el concepte de «discurs d'odi». La proliferació de missatges violents o que ataquen les minories, així com els que promouen comportaments delictius, han conduit a moltes persones a entendre l'anonimat amb què normalment actuen els agressors com a una eina perillosa que caldria eradicar d'internet. Malgrat que aquesta realitat no és desitjable i cal prendre mesures per corregir-la, la possibilitat de mantenir en secret la identitat té un fort vincle històric amb les llibertats d'expressió i polítiques. Des de fa segles, el dret a publicar sense revelar l'autoria ha permès la difusió de textos i obres polèmiques o crítiques amb el poder en els camps de l'art, la política, la literatura o el periodisme.

El cert és, però, que tot i que internet proveeix d'una sensació d'anonimat i llibertat en l'accés a la informació, cada cop es fa més evident la virtualitat d'aquesta privacitat. Les adreces IP, el número que identifica un dispositiu en una xarxa, es poden rastrejar i revelar quina ha estat la navegació de qualsevol individu. Mentre que el xifratge protegeix el contingut de les comunicacions, és a dir, els missatges, cal remarcar la importància de l'anonimat per garantir la privadesa de les metadades: qui es connecta, quan, quins webs visita, amb quins dispositius, durant quanta estona...

Per tal de defugir el control governamental o de terceres parts, existeixen eines capaces d'ocultar tècnicament les adreces IP i altres dades personals que revelen la identitat o la ubicació dels usuaris. És el cas de The Onion Router (TOR), un projecte de programari lliure que en lloc de generar connexions directes entre els navegadors i els servidors on hi ha els webs, els connecta de manera indirecta a través de diferents nodes. Això aconsegueix que l'IP real de l'internauta no es comuniqui mai directament amb la del proveïdor d'informació, fet que fa molt difícil rastrejar-la. Malgrat no ser infal·lible, periodistes i activistes polítics d'arreu del món fan servir aquesta

La indignació popular per l'espionatge a escala massiva ha obligat les companyies a adoptar el xifrat per defecte com a eina essencial per protegir el seu model de negoci

eina per garantir la seguretat de les seves comunicacions, especialment en països autoritaris. Probablement per aquest motiu, governs com els de Bielorússia, Egipte i Turquia han intentat bloquejar-lo. Per la pròpia natura distribuïda del sistema, aquestes mesures no poden eradicar-se de cap país, però sí que poden dificultar-ne l'accés al gran públic.

En els darrers anys també han cobrat importància les Virtual Private Network (VPN) [Xarxes Privades Virtuals], una tecnologia que permet connectar-se a internet a través de servidors remots, mantenint l'anonimat. Malgrat que sovint tenen un ús convencional, com ara permetre als empleats d'empreses accedir a fitxers corporatius des de casa, també s'utilitzen en països autoritaris com un mitjà per superar la censura. Això les ha convertit en un objectiu per als censors de països com —de nou— Bielorússia, Egipte i Turquia; on s'han aprovat legislacions que prohibeixen accedir a continguts censurats i permeten bloquejar els llocs web de proveïdors de VPN.

Les campanyes contra aquestes xarxes són impopulars i difícils d'aplicar, ja que moltes persones depenen d'elles per a dur a terme tasques legítimes, com ara consultar informació i notícies internacionals necessàries per al treball de científics, empreses o fins i tot de funcionaris governamentals. Per aquest motiu, cap país ha intentat prohibir completament les VPN, ja que es mouen cap a un sistema de dos nivells que autoritza l'ús d'eines aprovades pel govern, prohibint la resta. Aquest és el cas de la Xina, que ha exigit als proveïdors d'internet que bloquegin només les xarxes no autoritzades, ordre que ja ha obeït Apple despenjant-les de la versió xinesa de la seva Apple Store.

Altres exemples recents els trobem a països com els Emirats Àrabs Units, on noves esmenes a la llei de ciberdelinqüència prescriuen multes importants i possibles condemnes de presó pel mal ús de les VPN. A Rússia, per la seva banda, la prohibició de certes xarxes d'aquest tipus va venir acompanyada el 2016 de registres de les oficines i confiscació de servidors de l'empresa Private Internet Access. A l'Iran, les autoritats governamentals també han creat les seves pròpies xarxes privades oficials, que permeten als usuaris accedir a contingut restringit, però sotmetent totes les seves activitats a la supervisió estatal.

Responsabilitat i esperança en temps convulsos

Cal reconèixer que les mesures de control exposades dibuixen un panorama global en gran mesura desesperançador. És important, però, remarcar que existeixen possibilitats per tal de revertir-lo.

En primer lloc, cal exigir transparència. La ciutadania, especialment en països democràtics, té el dret a saber si els seus governants estan espiant-los a través de la tecnologia, i en cas que es consideri una mesura lícita, cal saber en quin grau i amb quines garanties es duu a terme. Tot i que moltes empreses privades poden determinar quines són les seves polítiques respecte a les dades, les administracions públiques no haurien de mantenir aquesta informació en secret, i en cas que això sigui necessari al tractar-se de registres criminals, ha d'estar justificat de manera raonada. Cal trencar

El dret a publicar sense revelar l'autoria ha permès la difusió de textos i obres polèmiques o crítiques amb el poder en els camps de l'art, la política, la literatura o el periodisme

amb la idea que les dades es poden recol·lectar massivament i emmagatzemar encara que no tinguin un ús concret, ja que la idea que algun dia podran ser útils per a la ciutadania no és un argument prou sòlid.

En segon lloc, cal ser crític amb les autoritats que fan ús de lleis de seguretat nacional per reprimir la dissidència a internet. Malgrat que alguns dels exemples exposats poden resultar llunyans al lector, el propi Estat espanyol és un exemple de la persecució cada cop més normalitzada de la llibertat d'expressió a xarxes socials com Twitter. Cal recordar que, malgrat que l'oposició ha demanat derogar alguns aspectes de la Llei de Seguretat Ciutadana, l'anomenada «llei mordassa», actualment aquesta polèmica norma encara està en vigor. Els seus preceptes afecten substancialment els drets de reunió, manifestació i llibertat d'expressió; a més a més, prohibeixen publicar imatges dels cossos policials a internet i convocar manifestacions a través de la xarxa.

D'altra banda, i en clau de responsabilitat individual, la ciutadania ha d'entendre els riscos als que s'enfronta en la seva activitat en línia, així com quines són les mesures de seguretat que pot prendre per evitar-los, actuant com a internautes conscients i responsables. Sense incidir en un discurs alarmista, cal que les persones coneguin què es fa amb les seves dades, per tal que triïn les seves pròpies configuracions de privacitat, protegeixin la seva informació personal i mantinguin una actitud proactiva per prevenir mals usos i evitar riscos.

Per últim, cal posar en valor les eines que garanteixen la privacitat en les comunicacions, malgrat que no siguin les majoritàries o les més accessibles en termes d'usabilitat. La tendència global a perseguir l'anonimat s'estén ràpidament i per exemple a finals del 2017, el portaveu del PP al Congrés, Rafael Hernando (1961), va anunciar que plantejarien a la resta de grups parlamentaris que s'estudiï un canvi de legislació per prohibir els comptes o perfils anònims a les xarxes socials. Un senyal d'alarma que reafirma que cal posar el focus en la importància de l'anonimat i el xifratge, que lluny de ser delictives, són eines que faciliten l'exercici dels drets democràtics. ■

Bibliografia

AGENCE FRANCE PRESS. **«Pakistani jailed for 13 years for Facebook post»** [en línia]. A *Daily Mail*, de 3 de març del 2016. Disponible a: <www.dailymail.co.uk>.

AL JAZEERA. **«Rights advocates call on UAE to release Ahmed Mansoor»** [en línia]. A *Al Jazeera*, de 28 de juny del 2017. Disponible a: <www.aljazeera.com/news>.

FREEDOM HOUSE. ***Freedom on the Net 2017*** [en línia]. Novembre del 2017. Disponible a: <wwwfreedomhouse.org>.

INDEX ON CENSORSHIP. **«Bahrain: NGOs express concern over arrest of photojournalist Sayed Ahmed Salman al-Mousawi»** [en línia]. Disponible a: <www.indexoncensorship.org>.

MACASKILL, Even i DANCE, Gabriel. **«NSA Files: Decoded. What the revelations mean for you»** [en línia] . A *The Guardian*, d'1 de novembre del 2013. Disponible a: <www.theguardian.com>.

PRIVACY INTERNATIONAL. **«Who's That Knocking At My Door? Understanding Surveillance In Thailand»** [en línia]. 2017. Disponible a: <www.privacyinternational.org>.

SCOTT-RAILTON, John (et al.). **«Nile Phish. Large-Scale Phishing Campaign Targeting Egyptian Civil Society»** [en línia]. A *The Citizen lab*, de 2 de febrer del 2017. Disponible a: <www.citizenlab.ca>.

WOLF, Josephine. **«Kazakhstan's Unsettling New Cybersecurity Plan»** [en línia]. A *Slate. Future Tense*, de 14 de desembre de 2015. Disponible a: <www.slate.com>.

ZUCKERMAN Ethan. **«Public Spaces, Private Infrastructure – Open Video Conference»** [en línia]. A *Ethan Zauckerman*, d'1 d'octubre del 2010. Disponible a: <www.ethanzuckerman.com>.