De Yahoo al cas Snowden: deixeu d'espiar-nos a internet!

Dani Vilaró / @danivilaro

L'estrena aquesta setmana d'"**Snowden**', 'biopic' cinematogràfic d'**Oliver Stone** sobre l'antic analista de la NSA que va revelar l'abast global de la vigilància massiva de les comunicacions a Internet, hauria de reobrir el debat sobre els drets que estem disposats a deixar enrere en nom de la seguretat i la lluita contra el terrorisme.

La setmana passada saltava una notícia que fa temps hauria escandalitzat mig món però que avui dia ni sorprèn: **Yahoo havia espiat en secret els missatges de correu electrònic dels seus clients** seguint ordres dels serveis d'intel·ligència dels Estats Units d'Amèrica. Abans de 2013 la revelació potser hauria obert informatius i ocupat primeres planes dels diaris. Aquesta vegada, però, no se n'ha fet gaire sang perquè és conegut que vivim en els temps de la vigilància massiva de les comunicacions a Internet: l'espionatge de tot el que fem a la xarxa és una pràctica generalitzada de molts governs.

Edward Snowden obria el meló quan el juny del 2013 denunciava l'omnipresència del programa de vigilància de l'Agència Nacional de Seguretat (NSA, en anglès), on treballava. Snowden revelava com, sense cap supervisió judicial, les agències de seguretat estatals utilitzen programes de vigilància massiva per emmagatzemar i analitzar en secret, sense transparència ni escrutini públic, milions de comunicacions privades de persones de tot el món, en una pràctica il·legal que viola drets fonamentals. Empreses com Facebook, Google o Microsoft acceptaven lliurar informació dels seus clients seguint ordres secretes de la NSA. Molts vam passar de les típiques informacions 'conspiranoiques' que sempre han envoltat Internet a una realitat que se'ns feia evident: ens espiaven.

De què parlem quan parlem de vigilància massiva?

Si utilitzem Internet o un telèfon mòbil, molt probablement ens estan espiant. Els governs utilitzen programes que accedeixen a dades de les grans empreses tecnològiques i a cables de fibra òptica que mouen les comunicacions globals per les xarxes. Les emmagatzemen i analitzen els **historials de navegació a internet, cerques d'informació, correus electrònics o trucades telefòniques**. També busquen metadades (dades sobre dades); això és, que no es preocupen tant del contingut (de què s'hi diu), com de les hores de les trucades, la ubicació, qui són els destinataris de les comunicacions, etc. Tot això, diuen, en nom de la seguretat, buscant patrons de conducta que ajudin a detectar i prevenir accions terroristes.

Les dades s'emmagatzemen i potents algoritmes informàtics completen cerques ràpides per analitzar la informació. El sistema, liderat per les agències de seguretat dels anomenats **"Cinc Ulls" (EUA, la Gran Bretanya, el Canadà, Austràlia i Nova Zelanda)**, ha estat compartit amb agències d'intel·ligència de fins a 41 països. Una autèntica teranyina global que empetiteix les històries d'espionatge 'artesanal' de la Guerra Freda: per complexa i pel volum de dades que gestiona.

> Sol funcionar un raonament com el que segueix: atemptats al cor d'Europa. Tenim por. Conseqüència? Barra lliure per a les agències de seguretat

Però, quin és l'abast del problema? Espien molt? Poc? Les xifres esborronen: cada dia els EUA recullen 5.000 registres d'ubicació de telèfons mòbils. Amb el Regne Unit, els EUA comparteixen prop de 200 milions de missatges de text diaris. En un sol mes, la NSA captura prop de 42.000 milions de registres d'Internet, com cerques o historials de navegació. Segons les revelacions d'Snowden, en un mes els EUA van interceptar fins a 60 milions de trucades telefòniques només a Espanya.

Potser algú pensarà que ja li va bé. Encara sol funcionar un raonament com el que segueix, i disculpeu l'esquematisme: atemptats al cor d'Europa. Tenim por. Conseqüència? Barra lliure: les agències de seguretat han de treballar per la nostra seguretat i ser més efectives en la prevenció i lluita contra un terrorisme que colpeja cada cop més ràpid. Vivim immersos en una amenaça global que ja no requereix de grans operatius ni d'anys de preparació (tipus 11S). Avui pot passar qualsevol cosa i arreu; per tant, que ens espiïn a tots.

Aquest pensament és perillós i obre dubtes molt seriosos des d'una perspectiva de drets humans: el primer és que **aquestes pràctiques només són legals quan són selectives, és a dir, quan es fan basant-se en indicis o proves suficients** de conducta delictiva i quan això es determina, per exemple, a través d'una ordre judicial. Mai no poden ser pràctiques indiscriminades, massives (com ho són). Mai no poden ser discrecionals per l'única decisió d'un cos policial o d'un organisme de seguretat estatal perquè és una pràctica il·legal que vulnera drets fonamentals, com la intimitat, la privacitat o la mateixa llibertat d'expressió. Què deixem de fer o dir a la xarxa si ens sentim espiats, si sabem que a l'altra banda hi ha algú que emmagatzema informació? **La vigilància indiscriminada simplement ens converteix a tots en presumptes delinqüents i les nostres activitats, en sospitoses**. Tenint, com tenim sobre la taula, reformes legislatives recents que limiten la llibertat d'expressió o de manifestació (lleis mordassa) o bé que amplien els delictes de terrorisme de manera molt ambigua (reforma del Codi Penal: recordeu els titellaires o l'operació Pandora?), això, com a mínim, és inquietant.

Espiar tothom és eficaç en la lluita contra el terrorisme?

El segon problema que presenten les pràctiques de vigilància massiva és la **suposada eficàcia en la lluita contra la terrorisme**. D'acord, els governs han de garantir la seguretat i lluitar contra el terrorisme. Des dels governs se'ns llancen contínuament missatges sobre l'amenaça "real" del terrorisme i ens diuen que necessiten més instruments i més poder per prevenir atemptats. Però realment han estat eficaces aquestes pràctiques? Els fets ens diuen que no i que, malauradament, la vigilància massiva ni ha portat més seguretat ni ha permès prevenir atemptats com els que, per exemple, han afectat França o Bèlgica l'últim any.

> "Si no he fet res dolent, per què em tracten com un criminal en potència i vulneren els meus drets?"

Algú encara pot seguir pensant: "Si no he fet res dolent no tinc res a amagar i ja va bé que m'espiïn". La pregunta hauria de ser la inversa: «Si no he fet res dolent, per què em tracten com un criminal en potència i vulneren els meus drets?". La majoria de governs occidentals ens enfronten a un fals dilema binari: seguretat o llibertat. Hem de triar. Doncs no. En un estat de dret, on les lleis haurien d'equilibrar tots dos conceptes, les persones són innocents fins que es demostra el contrari i tenen el dret que se'ls respecti la vida privada. Per tant, abans de violar aquest dret, els governs han de tenir indicis clars que s'està cometent un delicte. No poden buscar proves aleatòriament. Per posar un símil marítim: no poden passar la xarxa d'arrossegament pel fons marí fent-lo malbé, a veure què pesquen, si peixos grossos o petits.

I encara una tercera pega. **Què passa amb les dades emmagatzemades? Com sabem que no seran utilitzades contra nosaltres en un futur?** Quina certesa tenim que les dades no acabaran a mans d'algú que les utilitzarà amb finalitats diferents a les que ens asseguren? Amb l'excusa de la seguretat, de l'interès o la defensa nacional o del que toqui en aquell moment, es podrien utilitzar les dades personals per atacar periodistes o perseguir i assenyalar públicament activistes socials.

Això no és ciència ficció perquè ja passa en alguns països. A **Bahrain, Egipte, Aràbia Saudita, Bielorrússia o Etiòpia**, els seus governs ja han utilitzat aquesta vigilància de les comunicacions per detectar i empresonar activistes o dissidents. Al Marroc, un grup de periodistes i activistes conegut com Mamfakinch va ser espiat amb programes distribuïts per les mateixes autoritats. Van enviar-los un document simulant una primícia que, en clicar-se, instal·lava el codi maliciós per poder accedir a tot allò que escrivien i a les seves fonts.

L'africtivisme, l'esclat esperançador de l'activisme africà a les xarxes, fa temps que també pateix l'escomesa de governs que temen l'efecte multiplicador (i mobilitzador) d'Internet en les capes més joves i informades de la població. **Cal dir que, com passa amb el comerç d'armes, els principals fabricants d'aquest programari són empreses occidentals?** Algunes són empreses petites o mitjanes britàniques, alemanyes, italianes… que aconsegueixen notorietat per la venda d'aquests programes a governs repressius, i després hi ha les empreses més grans, transnacionals, que també fabriquen aquest tipus de tecnologia, com **Lockheed-Martin, BAE Systems o Raytheon**.

> A Catalunya el Cesicat va recollir dades d'activistes socials, també personals, més enllà de la seva activitat pública

Més evidències. La Unió Americana per les Llibertats Civils (ACLU) ha denunciat recentment que la policia nord-americana utilitza programari de vigilància de les xarxes socials per monitoritzar l'ús d'etiquetes com **#BlackLivesMatter** o **#PoliceBrutality** per identificar activistes que protesten contra la mort de persones negres a mans d'agents de policia. El 2014 a Catalunya també es va saber que el Cesicat havia recollit dades d'activistes socials, també les personals, més enllà de la seva activitat pública a la xarxa.

És un fet, doncs, que els governs (tots) volen aprofitar la conjuntura de la por, del debat sobre la seguretat i el terrorisme global perquè acceptem que no tenim drets, o que els perdem, quan ens situem a Internet. Que acceptem sense rondinar que quan utilitzem el mòbil o el correu electrònic, tot el que fem o diem els pertany. Oi que no toleraríem aquest grau d'intrusió en la nostra vida fora de la xarxa? Per què hem de permetre'l dins? L'any passat, governs com els del Pakistan, França, Polònia, Suïssa o Regne Unit van impulsar reformes legislatives per augmentar l'abast de la vigilància i tenir més poder intrusiu en les comunicacions. L'ofensiva és global: en governs del nord i del sud, en democràcies formals i dictadures.

Vigilar el vigilant

La tecnologia actual proporciona als governs un poder sense precedents per observar tot el que fem a Internet. Ens cal, doncs, un mecanisme independent, fiscalitzador, que controli els vigilants per evitar els abusos de poder. Però avui són poques les lleis que realment ens protegeixen d'aquestes pràctiques i ja hem vist més amunt com la tendència ara és justament la contrària: debilitar encara més la protecció.

A títol individual podem recórrer a **tecnologia de protecció** com el xifrat i l'encriptació dels

nostres missatges i rastre a la xarxa per garantir el nostre anonimat quan ens movem per Internet. Moltes persones tenim una idea clara sobre quina informació sensible voldríem protegir i el pas següent ha de ser formar-se i començar a reflexionar sobre la seguretat a les xarxes amb realisme i sentit comú: encriptació de dades i navegació segura són unes primeres passes bàsiques i necessàries.

Els instruments individuals de protecció, però, no són la panacea i cal apuntar molt més alt i en dues direccions. Per molt que ens protegim individualment perquè coneixem un amic o amiga 'hacker' que ens aconsella, res no ens protegirà més que un marc legal fort contra aquestes pràctiques governamentals i també una responsabilitat més forta, crítica i activista si voleu, com a consumidors.

Per una banda, **aprofundir en la via legal**. El dret internacional de drets humans protegeix els drets a la intimitat i a la llibertat d'expressió i els estats tenen l'obligació legal de protegir-los. Aquí encara hi ha camp per recórrer, tant en legislació que revoqui les pràctiques que s'han fet fins ara emparades en l'opacitat i la manca de transparència, com en el paper de les autoritats judicials per interpretar que el que ja s'ha fet viola drets fonamentals i per tant es pot perseguir. Des que Snowden va destapar els fets, alguna cosa s'ha mogut. Als EUA s'ha aprovat una llei que revoca algunes de les pràctiques antigues de la NSA, com les escoltes telefòniques sense autorització judicial. Recentment un jutge federal a Alemanya ha ordenat la destrucció d'una base de dades construïda amb pràctiques de vigilància indiscriminada.

L'altra via per desfer el que s'ha perdut és el nostre paper actiu com a **consumidors crítics d'empreses tecnològiques**. Pensem-nos bé a què accedim quan donem el nostre consentiment a una empresa. Hem vist com les empreses tecnològiques han jugat un paper fosc, quan no directament de cooperador necessari, en tota aquesta història. Exigim que els nostres aparells siguin segurs, demanem més encriptació (whatsapp no ho feia i ara ho fa), qüestionem les empreses quan ens demanin segons quines dades sensibles i preguntem per a què les volen, on es desen, si les destrueixen o no i quan… **Qüestionem i denunciem aquestes empreses quan creguem que no ho fan bé**. Apple, fa uns mesos, va mantenir un litigi amb l'FBI per mantenir l'encriptació del seu iPhone. Sense saber del cert si va tractar-se d'una operació cosmètica, el gegant tecnològic va plantar cara a una ordre del govern nord-americà que obria una porta molt perillosa. Aquest pot ser un camí: que les empreses, descoberta la seva connivència amb els governs per poder dur a terme la vigilància massiva, ara se sentin qüestionades pels seus clients i, en certa manera, es vegin obligades a fer passes enrere, siguin sinceres o no, guiades per l'ètica o pel compte de resultats.

Protegir els filtradors

I acabo amb una qüestió no menys important, i torno a Edward Snowden. **Cal protegir les persones que denuncien irregularitats, les filtradores o informants, quan destapen abusos greus als drets humans**. La persecució que pateix Snowden per haver contribuït al coneixement global d'abusos de poder és repugnant. Tothom hauria de poder denunciar abusos contra els drets humans o informacions d'interès públic en condicions de seguretat, sense por a patir presó o a ser considerat un traïdor o un espia.

Snowden, que viu a Rússia, s'enfronta a una amenaça real de molts anys de presó si decideix tornar als EUA però també té molts problemes per aconseguir asil en un altre país per les pressions diplomàtiques i econòmiques dels EUA. Ni traïdor, ni segurament un heroi, Snowden ens va destapar un món de clavegueres governamentals que amenaça drets i llibertats fonamentals. Es fa difícil preveure que passarà en el futur perquè en l'àmbit de la tecnologia i les xarxes tot es mou molt ràpid, potser massa, però el que és important és que no ens rendim. Cal que participem en el debat públic, col·lectiu, i sotmetem els governs a escrutini i denúncia de les pràctiques de vigilància

indiscriminada perquè justament el que volen és que ens cansem i abandonem. Seria servir-los el nostre cap, el de tothom de fet, en safata de plata.

Dani Vilaró és periodista.