Fer-se transparent a la xarxa

Les empreses fan negoci de les nostres dades mentre els estats controlen la nostra activitat a internet. Cada vegada, però, en són més els qui alerten d'aquests perills.

Reportatge de ***Cristian Reche***

L'ús de les noves tecnologies i l'enorme dependència que en tenim resulta evident. La nostra vida quotidiana apareix reflectida a Facebook, i els nostres pensaments més intranscendents, a Twitter. En definitiva, cada dia aboquem a la xarxa una bona part del que som, hi quedem exposats. Ara bé, fins a quin punt són segures aquestes pràctiques?

"Quan ets a dins de Facebook, tens una sensació de seguretat enorme, però aquesta sensació és completament falsa", assegura James Vasile, director de l'Open Internet Project Tools, una entitat internacional sobre seguretat a la xarxa que, entre més esdeveniments, recentment va participar a l'organització del Circumvention Tech Festival, a València. L'objectiu? Lluitar contra censura i la vigilància a Internet. I és que persones com Vasile alerten que l'ús de navegadors com Google o de xarxes socials com Facebook pot ser contraproduent pels nostres interessos.

Big Data, adéu a la privacitat

L'any 2012, els grans magatzems estadounidencs Target, mitjançant l'extrapolació de dades massives, van protagonitzar una anècdota significativa. El pare d'una jove va cridar a la seu d'aquesta empresa queixant-se que la seua filla adolescent no parava de rebre publicitat de productes premamà. I la seua filla, efectivament, estava embarassada. Target, la sisena empresa de venda al detall dels EUA, havia identificat 25 patrons de conducta que es repetien en dones que anaven a ser mares. Creuant totes aquestes dades, els correus electrònics s'encarregaven de la resta: enviaven propaganda als potencials compradors de manera automàtica.

A la pràctica, parlem d'enormes bases de dades que, traslladades a internet, reben el nom de Big Data, un dels negocis més sucosos al món digital. Grans companyies nord-americanes estan creant aliances en aquesta direcció, i unes altres, com ara Mongo DB, ja han assolit un valor de 1.600 milions de dòlars. En plena era de la informació i del capitalisme informacional, aquestes dades són el nou or. "Quan seus davant de l'ordinador, et penses que estàs sol davant a la pantalla, però no es així: diferents empreses miren tot el que fas, pas a pas", afirma Sandy Ordonez, un alttre dels organitzadors del Circumvention. Les nostres petjades digitals alimenten el malanomenat "màrqueting predictiu".

De la mateixa manera que Big Data anota totes les nostres petjades, les metadades actuen d'una manera similar. El 2013, el món sencer va assabentar-se que les companyies de telecomunicacions dels Estats Units havien sotmès les seues trucades i els seus correus electrònics als serveis d'intel·ligència NSA. Aquesta informació descriptiva naix tot just quan es produeix una cridada telefònica o quan s'envia un correu electrònic. Amb ella, es pot conèixer la nostra ubicació exacta i, fins i tot, la durada de cada trucada i els asssumptes tractats.

Els estats són els grans aliats d'aquestes empreses. Més enllà de crear un marc legislatiu a la carta per a totes elles, poden fer ús de la informació obtinguda. L'excusa és ben senzilla: la violació de la

privacitat individual és necessària per a mantenir la seguretat de la resta de la població. A l'Estat espanyol, una modificació de la llei d'enjudiciament criminal hi ha aplanat el camí.

Els afers polítics i la pugna pels interessos de cada institució són habituals a la xarxa. El 9 de novembre del 2014, la consulta sobiranista catalana va erigir-se com a exemple de la manera com els governs estan disposats a intervenir per tal d'imposar els seus criteris. Els dies precedents, el Centre de Seguretat de la Informació de Catalunya (Cesicat), encarregat de vetlar pel bon funcionament de les telecomunicacions, ja va detectar problemes de funcionament a diverses pàgines i serveis digitals, incloent-hi la web i el correu electrònic de la Generalitat i la pàgina oficial del 9N, www.participa2014.cat. Aquest ciberatac encara és visible al mapa interactiu Digital Attack Map, elaborat per l'empresa de seguretat Arbour Networks en col·laboració amb Google.

A Catalunya, de fet, aquesta mena d'actuacions no són casos aïllats. L'any 2013, a partir d'unes filtracions del mateix Cesicat, es va saber que el centre havia efectuat un seguiment exhaustiu de diversos activistes de Twitter relacionats amb el moviment 15M, amb la vaga de Transports Municipals de Barcelona (TMB) o contraris el congrés anual de telefonia mòbil que cada any acull la capital catalana, Fins i tot va eixir a la llum una carta signada per l'aleshores cap dels Mossos d'Esquadra, Manel Prat, en què li comunicava al màxim responsable del Cesicat, Carles Flamerich, els noms concrets dels perfils que calia seguir de prop.

Vida privada i encriptada

Aleshores, en quin punt ens deixa la intimitat dels usuaris aquestes pràctiques?. Malgrat no estar divulgades, hackers i activistes faciliten eines de la xarxa per tal de burlar l'ull gegant d'internet, el Gran Germà que ens vigila. Els navegadors alternatius, operar de manera segura a través de la plataforma anomenada núvol, les connexions privades virtuals, l'encriptació de missatges als correus electrònics o el mateix xifrat de videoconferències, en són algunes. Però no totes. Encara n'hi ha un bon grapat més.

Unes ferramentes que, al capdavall, es presenten com a alternativa a les existents. El cas més significatiu és el del navegador Tor [vegeu EL TEMPS núm. 1.602]. Conegut també com The Onion Router, permet navegar anònimament a la xarxa sense deixar-hi rastre. Amb tot, n'és una arma de doble fil. El seu ús pot situar els usuaris en el punt de mira dels serveis d'intel·ligència de diversos països, atès que permet endinsar-se en les zones més fosques d'Internet, les conegudes com a Deep Web o Dark Net, que aixopluguen des d'organitzacions defensores dels drets humans fins a règims dictatorials.

Una altra de les opcions és Tresorit, un servei d'emmagatzematge encriptat en línia, el qual permet l'intercanvi segur d'informació. Els seus creadors estan tan convençuts de la seua fiabilitat que ofereixen 50.000 dòlars a qui siga capaç de crackejar el seu sistema. Hi ha hagut més d'un miler d'intents durant els darrers dos anys, tots ells sense èxit.

Per a una praxi correcta d'aquests instruments, però, cal tenir un bagatge considerable. També cal molta preparació per tal de posar en pràctica mètodes i protocols d'actuació, el primer dels quals, i un dels més importants, l'avaluació de riscos. Es tracta de rebaixar a la mínima expressió tots els perills a què ens enfrontem cada vegada que connectem un ordinador. Actes tan senzills com per exemple no connectar-se a xarxes públiques wireless (com la dels aeroports) ens poden estalviar més d'un ensurt. Projectes com el Tactical Technology Collective o el Me And My Shadow caminen en aquesta direcció.

Sergio Araiza, capacitador certificat pel Front Line Defenders, un organisme de defensa dels drets humans en base a la seguretat i privadesa a internet, fa la seua divisió particular del públic internauta: "A internet trobem diferents tipus d'usuaris dividits segons el grau d'anonimat que fan servir a la xarxa", afirma. El resultat és una mena de piràmide invertida on la quantitat de gent que es preocupa per garantir la seua privacitat se situa a l'extrem inferior. Els qui no hi dediquen gaire atenció són la pràctica totalitat dels internautes. •

James Vasile, director de l'Open Internet Project Tools, opina que la sensació de seguretat que tenim a Facebook és errònia.