El navegador Tor garanteix l'anonimat i permet arribar a les profunditats d'internet, a la zona més obscura de la xarxa.

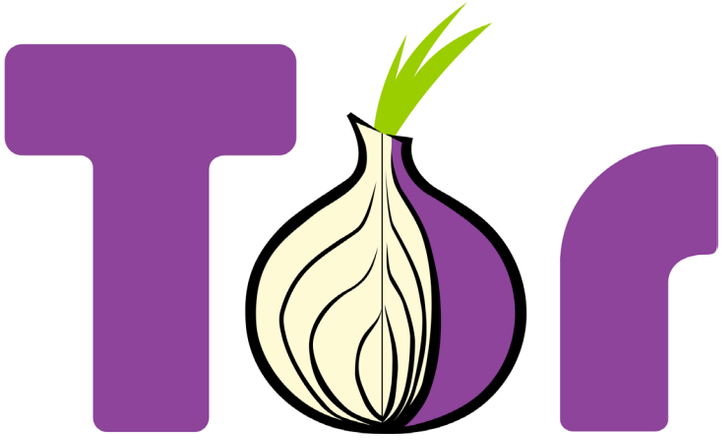
El desconegut internet

La majoria de la gent suposa que internet és allò que es coneix habitualment: Google, Yahoo, adreces .com –o amb qualsevol altre sufix dels més comuns... Però no és així. Tot això és només una ínfima part del total. Moltíssima més informació es troba en un internet desconegut, anomenat profund, al qual no es pot accedir amb els navegadors i buscadors habituals. És on estan allotjades per seguretat les pàgines d'organitzacions de drets humans que lluiten sota règims dictatorials, és la forma ideal per assegurar la comunicació entre el periodista d'investigació amb la font més sensible... però també és on apareixen les webs més sòrdides i il·legals. Per accedir tant a unes com a les altres Tor és l'eina perfecta. Perquè no deixa rastres.

Les pàgines d'informació sobre internet i programari que parlen de Tor solen advertir que el simple fet d'emprar el navegador pot posar l'usuari a la diana de l'interès dels principals serveis de policia i d'intel·ligència del món, especialment de la famosa i poderosa National Security Agency (NSA) nord-americana. L'advertència dóna una clara idea que no és un navegador qualsevol. Per a molts és una de les armes més importants que tenen els que lluiten per la llibertat arreu del món. Per a d'altres, és l'instrument d'accés a la zona obscura d'internet que és el refugi de pederastes, terroristes, traficants de persones, d'armes...

Àngel i dimoni. Així és Tor. El nom del qual no honora, com per ventura es podria suposar, el déu del tro de la mitologia nòrdica. Fa referència a quelcom més prosaic, quotidià i banal: una ceba.

Què és i com funciona Tor? Tor és l'acrònim de The Onion Router o l'encaminador ceba. El nom fa referència a com encripta la informació, amb diverses capes que s'acumulen una sobre l'altra, com les de la ceba, que protegeixen la connexió, les dades. Com tantes altres coses relacionades amb l'alta tecnologia, aquest sistema d'encriptació fou inventat pels investigadors militars dels Estats Units. En concret, va ser una divisió tecnològica de la US Navy la que l'any 2003 el creà com a sistema de protecció de les comunicacions per internet de tota la flota dels Estats Units. Al cap d'uns pocs anys passà a ser emprat, amb el nom de Tor, per moltes organitzacions, empreses i particulars que volen usar internet amb seguretat i anònimament.



The Onion Router és el navegador que atorga l'anonimat a qui l'usa correctament.

La relativa popularització del sistema fou ulterior i es relaciona amb el famós cas d'Edward Snowden i les seves revelacions –vegeu requadre– d'informació secreta del Govern dels Estats Units a través de diaris com *The Guardian* el 2013.

Quan un ordinador es connecta a un lloc web, ho fa per la ruta més directa. És qüestió d'eficiència, de velocitat. L'origen de la comunicació digital és sempre el mateix: la màquina emissora, la qual està identificada mitjançat una numeració única. És a dir, cada ordinador té la seva designació respectiva, la que s'anomena direcció IP –sigles d'Internet Protocol–. Per tant, tot el flux de dades que estableixi cada màquina pot ser identificat inequívocament. El que fa el navegador Tor és, en síntesi, alterar aquesta estructura del fet comunicatiu virtual. De ser establert entre un emissor i un receptor passa a ser en xarxa. Fa que la connexió no s'estableixi directament entre dos punts sinó que la fa voltar a través de diversos nodes situats arreu del món –n'hi ha uns 4.000–, cadascun dels quals xifra les dades que rep i les reenvia, de manera que la informació queda protegida sota capes i més capes de seguretat –d'aquí el nom de ceba– acumulades pels múltiples nodes. Quan la informació, després de rebotar i rebotar, arriba a l'últim node –que pot ser un o un altre, mai el mateix–, aquest l'aboca al destinatari. D'aquesta manera ningú pot saber quin és l'origen. L'anonimat està garantit. Ara bé, tal com recorda una de les més conegudes pàgines especialitzades en internet, Genbeta, la seguretat té un preu: és un navegador més lent que els altres. A hores d'ara aquest és el principal escull. La raó és bona de comprendre. Els múltiples salts de node en node fan que el flux d'informació redueixi la velocitat.

Les pàgines web especialitzades en informació sobre internet consultades calculen que Tor ha estat baixat per uns 30 milions d'usuaris, dels quals una mica menys d'un milió l'usen habitualment. Qualsevol persona el pot instal·lar en el seu ordinador, però abans d'usar-lo és recomanable llegir els consells de seguretat que s'ofereixen en gairebé totes les pàgines especialitzades.

Tor i la llibertat. A la segona meitat de la primera dècada d'aquest segle els moviments de drets humans que actuen en països on són conculcats, els de reivindicació democràtica en Estats dictatorials, defensors de la llibertat d'expressió on no es garanteix totalment i d'altres per l'estil començaren a usar Tor com a navegador preferit ja que permet no ser identificats. Igualment, els moviments antisistema el tenen com l'instrument més segur de comunicació, com és el cas dels grups antiglobalització. També és essencial per a la famosa xarxa Anonymus, que ha convertir la careta que l'identifica en una icona de la llibertat d'expressió en les accions que protagonitza tant a la xarxa com a fora.

L'ús de Tor per tots aquests moviments posa nerviosos molts Governs. Sobretot els dictatorials, i també els que són escassament democràtics. Per exemple, el líder de Rússia, Vladimir Putin, ha ofert 100.000 dòlars a qui pugui rompre la seguretat de Tor. A Xina, els serveis d'intel·ligència i policíacs consideren el navegador una eina "contrarevolucionària" la qual espien per intentar identificar i detenir-ne els usuaris. A Veneçuela el Govern de Maduro vol destruir Tor perquè, a parer seu, l'empren els "imperialistes" per atacar "la revolució bolivariana". A Cuba la dictadura familiar comunista dels Castro igualment el vol acotar perquè el considera un perill... S'ha convertit en un dels principals instruments per a la llibertat. En aquest sentit, la Fundació Fronteres Electròniques, organització més coneguda per les seves sigles en anglès, EFF –Electronic Frontier Foundation–, l'ha assenyalat formalment i públicament com l'eina que més garanties atorga per a l'ús segur i lliure d'internet. Val a dir que EFF fou creada el 1990 per preservar el dret a la llibertat d'expressió en l'era digital, té la seu principal a San Francisco i compta amb oficines a Toronto i Washington, s'alimenta econòmicament d'aportacions particulars i el seu objecte fonamental és ampliar les llibertats civils –especialment la d'expressió– en el món digital en què vivim. Que l'EFF reconegui el valor de Tor és un bon indicatiu del gran instrument que és. Per si no quedava prou clar, Christopher Soghoian, especialista en alta tecnologia de l'*American Civil Liberties Union* –ACLU– escrivia un article a *The Guardian*, l'octubre de 2013, en el qual assegurava que la codificació de la informació que fa Tor "és allò que li dóna i atorga el poder" per eixamplar la llibertat, "i per a aquells que ho dubtin que pensin en això: el Govern dels Estats Units encara no sap quins documents s'emportà Ed [Snowden] perquè ho codificà tot".

Les agències d'intel·ligència de tot el món, com és ara l'NSA dels Estats Units, intenten trencar l'anonimat de Tor

No hi pot haver dubte que Tor és un instrument perfecte per a la llibertat. No obstant, també és ver que els serveis de policia i d'intel·ligència especialitzats en internet de Governs democràtics de tot el món desconfien profundament de Tor i l'intenten controlar. Perquè també és la porta cap a la zona més obscura d'internet.

Tor i 'darknet'. Internet es divideix en dues parts. Una, la superficial. L'altra, l'oculta, la coneguda en anglès, entre d'altres denominacions, com *deepweb*, *invisible web*, *darknet* o *hidden web*, si bé les que pareixen consolidar-se en l'ús habitual són *deepweb* i *darknet*, profund i obscur, respectivament. A aquest internet profund, no hi accedeixen els motors de recerca digital que habitualment tots fem servir. Per què? Els motius són diversos però essencialment perquè no són capaços o no tenen interès –les empreses que els creen, òbviament– a indexar tota la informació que allà es troba. Els navegadors més habituals són poc recomanables, per baixar tan avall del món digital, perquè deixen rastre.

Per què algú hauria de voler accedir a *deepweb*? Senzillament perquè és allà on més informació hi ha. Se sol comparar internet amb un iceberg. La part visible ocuparia entre un 10% i un 5% del total. Mentre, la submergida, *darknet*, representa entre el 90% i 95% del conjunt. És a dir que allò que coneixem la majoria dels ciutadans d'internet és, en realitat, una part ínfima. El gruix de la informació digital es troba a les profunditats. Amagada. Accedir-hi no és fàcil. L'usuari de *deepweb* ha de ser un iniciat. Ha de saber on va i què està cercant. Allà, no hi val Google ni hi ha adreces com les que tots coneixem. No hi ha res de *.org* o *.com*. El sufix més comú és *.onion*. En efecte, 'ceba': no és per casualitat.

Com el lector ja deu haver imaginat, Tor és una de les claus que obre la porta cap a les profunditats més obscures d'internet. Allà on figuren infinitat de documents escrits, fotogràfics, vídeos de particulars, d'empreses, de Governs –fou l'àmbit a través del qual es conegueren les dades de WikiLeaks, per exemple–

Snowden i Tor

Edward Joseph Snowden (Estats Units, 1983) és un antic consultor tecnològic de la CIA i de l'NSA, les dues famoses agències d'intel·ligència del Govern nord-americà. Va saltar a la fama el juny de 2013 quan va fer públic, a través dels diaris *The Guardian* i *The Washington Post*, documents oficials considerats secrets que provaven que l'administració nord-americana espiava arreu del món, ciutadans i empreses del seu propi país inclosos, a través de programes de vigilància massiva. Des d'aquell moment va ser titllat de "traïdor", "espia" i d'altres epítets per l'estil pel Govern de Barack Obama. Es va salvar de ser detingut i amb tota probabilitat de ser empresonat per molts d'anys, fins i tot amb possible cadena perpètua, fugint cap a Hong Kong. El Departament de Justícia dels Estats Units el considera "responsable d'activitats criminals" contra "la seguretat nacional" i per això ha posat preu a la seva detenció. Des de l'antiga colònia britànica del sud-est asiàtic, i després d'una rocambolesca combinació de viatges amb avió –inclús comprant bitllets que no usà, per evitar ser segrestat–, va aconseguir arribar a Rússia. Un mes més tard, Vladimir Putin li atorgà, l'1 d'agost de 2013, asil especial durant tres anys amb "absoluta llibertat de moviments i d'activitats sempre que no actuï contra els interessos americans". Altres països com Equador i Veneçuela han assegurat que estan disposats a atorgar-li refugi polític si Rússia no li renova la protecció l'estiu de 2016.

Snowden s'ha convertit en una mena de guru internacional de la seguretat a internet. De fet, sempre ha justificat la difusió que va fer de la informació classificada per motius "ètics" ja que considera que els ciutadans han de tenir dret a la "seguretat de les seves comunicacions" i, consegüentment, també, a conèixer "que el Govern (dels Estats Units) els estava espiant". Aquest zel en la defensa del dret a la seguretat a internet l'ha portat a ser un dels principals propagandistes de Tor. L'estiu de 2014 participà, via teleconferència, en el festival multidisciplinari anomenat South by Southest, a Austin (Texas, Estats Units), durant el qual se sotmeté a preguntes dels presents. "Què pot fer una persona normal i corrent per assolir la major seguretat digital possible?", li demanà un dels participants. La resposta no va deixar cap escletxa per al dubte: "Tor és la millor opció, una xarxa que resulta molt difícil d'atacar". Opinions com aquesta han convertit el navegador en una referència de culte en el món dels internautes.

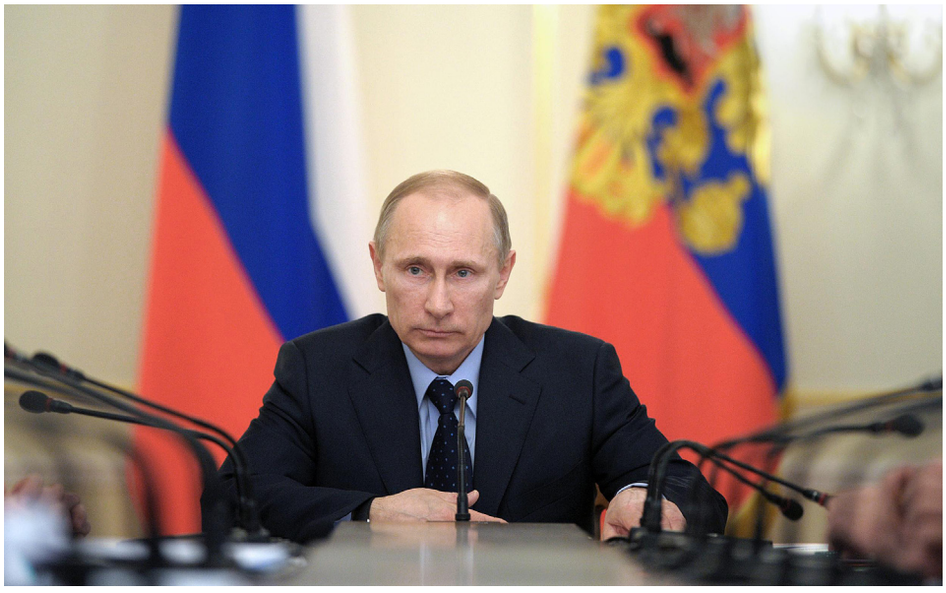
L'internet que coneixem la majoria només ocupa entre un 5% i un 10% del total; la resta és el profund, 'darknet', i per accedir-hi res millor que Tor

que fan referència a qualsevol tema que hom pugui imaginar. És el paradís per intercanviar informació de tota casta amb la màxima seguretat. Un lloc de relació ideal, com s'ha dit, per a tots els que lluiten a favor de la llibertat arreu del món; per als periodistes que tenen fonts que es juguen la vida... Però també per a d'altres persones i grups més sinistres.

Les webs de la profunditat ofereixen, entre moltes altres coses, tècniques detallades per a ús de tot tipus de pirates informàtics, siguin *hackers* o *crackers* –la diferència, essencialment, és que els primers no ho fan per diners i els segons sí– per atacar pertot arreu; hi venen qualsevol classe de medicament prohibit i, naturalment, si se cerca una droga, per forta o rara que sigui, no hi ha cap problema per aconseguir-la... si es paga el preu que es demana. Aquests exemples són els que es troben rere de les primeres capes de la ceba profunda d'internet. Aviat n'apareixen d'altres, més inquietants. *Deepweb* ha esdevingut el paradís comercial per a la indústria dels objectes robats –sobretot targetes de crèdit, un dels productes estrella–, per trobar manuals per fabricar tota mena d'explosius, per comprar armes de foc de qualsevol tipus, per contractar grups de delinqüents, per trobar on netejar diners negres, per saber com comprar doblers falsificats de totes les divises... A la profunditat més negra apareixen les webs brutals, les que ofereixen les imatges d'abusos sexuals a menors, vídeos *snuff* –que enregistren tortures, violacions i assassinats–, webs especialitzades en compra-venda d'esclaus, d'òrgans humans, ofertes de feina d'assassins professionals, de mercenaris, pàgines de grups terroristes, d'intercanvi entre pedòfils... La naturalesa humana més sinistra i perversa, en fi.

Per accedir a tot aquest *darknet* Tor és l'instrument perfecte. Perquè no deixa rastres. Es més, hi ha un seguit de pàgines del profund internet que únicament es poden consultar a través d'aquest navegador. És, igualment, el que se sol usar per anar als mercats de diners digitals, els cada cop més emprats *bitcoins*, que tenen un desenvolupament enorme des de 2013. Amb el nom de *bitcoin* es coneix la moneda virtual que s'usa a l'internet. Va ser concebuda el 2009 per Satoshi Nakamoto. Es tracta d'una unitat per quantificar transaccions a la xarxa sense que estigui validada per cap autoritat financera o política, Govern, banc o grup. Es basa en la confiança i el consens entre els que l'usen. Va nàixer com una possibilitat d'alliberar-se del bancs i emissors de moneda –Estats– tradicionals. Però a *darknet* s'ha convertit en la manera de pagar els serveis i transaccions més obscurs, relacionats amb tot tipus d'il·legalitats i pràctiques criminals.

No pot estranyar que Tor i el profund internet tinguin una imatge tèrbola. Però, com s'ha dit, no es pot oblidar que també a *deepweb* s'allotgen les pàgines que ajuden a promocionar la llibertat a països sota règims dictatorials, les que experimenten amb relacions humanes i socials fora dels circuits controlats per les estructures governamentals i pels grans interessos econòmics internacionals, les que per-



Dalt, els Governs dictatorials o els menys democràtics lluiten aferrissadament contra Tor: Vladimir Putin oferí 100.000 dòlars a qui trenqués la seguretat del navegador. Baix, els moviments per la llibertad d'expressió, com Anonymus, i tots els que lluiten sota les dictadures, usen Tor; però també és ver que el fan servir els criminals.

meten a mitjans de comunicació informar d'abusos il·legítims de Governs, és on hi ha nombrosos llocs –que es coneixen com The Academic Invisible Web– que difonen els avenços tecnològics, publicacions científiques i material que ajuden a prosperar la humanitat...

Naturalment, *darknet* també està farcit dels serveis d'intel·ligència i policíacs d'arreu del món que el rastregen contínuament intentant identificar i controlar els usuaris, a banda de mirar de rebentar la seguretat de Tor, el navegador que s'ha convertit en l'enemic d'aquests tipus d'agències. *The Guardian* informava a finals de 2013 que l'NSA usava –i tothom suposa que la resta de serveis d'espionatge també– tot tipus de trampes, com és ara crear una web falsa que, quan se li obri automàticament la identitat de qui la consulta passa a ser detectada, per així tenir controlats els usuaris. Per això les pàgines especialitzades en l'ús d'internet solen advertir que el simple maneig de Tor implica –tot i que és legal– la possibilitat de ser considerat objecte d'interès per aquests serveis o altres grups que operen en el profund internet, i per això donen instruccions sobre com usar-lo amb el màxim de seguretat possible. Corren moltes històries sobre usuaris que no han estat prudents i han acabat amb els seus equips informàtics infectats amb coses molt més greus que el pitjor dels virus que hom pugui imaginar. Algunes veus ho dubten i asseguren que tot és una mena de llegenda urbana sense cap ni peus. Qui sap. Però no costa res tenir present que si algú es vol baixar Tor per descendir a *darknet*, convé que ho faci essent conscient dels perills potencials que assumeix.

Miquel Payeras

El fals cop a Tor

El passat mes de novembre Europol anunciava un "important cop" contra "els llocs obscurs" d'internet. Segons la nota policial feta pública, 16 països europeus i Estats Units havien unit esforços per atacar l'anomenat internet ocult, en el qual clausuraren, segons digueren, 410 llocs web il·legals, i, a més, aconseguiren detenir 17 persones a diverses ciutats. La nota va tenir força impacte entre els grups d'iniciats en l'ús de Tor, perquè deixava entendre que la seguretat del navegador havia estat trencada i que els detinguts n'eren usuaris. Tot d'una va contestar Andrew Lewman, director executiu del Projecte Tor, el qual assegurà que tot era una exageració i que "en absolut" la xarxa que garanteix l'anonimat "no ha estat en cap moment compromesa de cap manera" per les policies. És més, dubtava que les forces de l'ordre haguessin aconseguit les detencions mitjançant l'espionatge a Tor sinó més aviat, aventurava, per "la persecució" de diners il·legals a la xarxa. En un comunicat posterior, Europol confessava que només havia tancat 27 llocs web. Informacions ulteriors corroboraren el mateix que havia dit Lewman, que havia estat una operació policial contra els diners opacs que s'usen a la xarxa i que el navegador continuava funcionant normalment.