ESTILS

Les 'cryptoparties' arriben a Catalunya

Cornellà se suma a les 'cryptoparties', un moviment internacional per ensenyar els ciutadans a protegir la seva privacitat i les seves comunicacions a la xarxa

NEREIDA CARRILLO
CORNELLÀ DE LLOBREGAT

"Internet, utilitzat ingènuament, ens exposa". Amb aquest advertiment obria Jordi Delgado, doctor en informàtica i professor de la UPC, la *cryptoparty* que ara fa uns dies es va celebrar al Citilab. Equipats amb els seus portàtils, una quarantena de persones participen en una activitat que els ensenyarà a navegar amb més privacitat o a millorar la seguretat de les seves contrasenyes. La de Cornellà és només una de les moltes *cryptoparties* que es fan arreu del món i que beuen d'un moviment internacional que vol acostar a l'usuari mitjà de la xarxa eines per protegir-se davant de possibles atacs a la seva privacitat.

"La majoria de gent no és conscient dels perills d'internet", reflexiona el Pol rere la pantalla del seu ordinador. Unes files més endavant d'aquest jove, Fernando Badía expressa les seves pors: "Et pots intentar protegir, però si hi ha algú que et vol fer mal, podrà fer-ho". Absortes en les seves màquines, Rosa Garvi i Maria Torrente identifiquen quins dels seus comportaments són poc segurs. "He de posar contrasenyes més llargues", comenta la Maria.

Els dubtes i preguntes al taller són una mostra més de com la preocupació per la seguretat a la xarxa creix cada cop més. La filtració de fotografies de famoses, els atacs a webs i comptes de Twitter o l'espionatge dels governs revelat per Snowden són alguns dels esdeveniments que han encès la llum d'alarma. "La seguretat s'anirà incorporant, però no ve de sèrie", comenta Jordi Iparraguirre, membre del capítol català de la Internet Society i coorganitzador de la *cryptoparty*. Aquest enginyer informàtic recalca que la xarxa "ve d'un món idíl·lic en què les universitats es connectaven i tot era bon rotllo". Ara la situació és ben diferent.

Dret a amagar

De qui ens hem de protegir? "Si faig *cryptoparties* és perquè em preocupen molt més els governs que els lladres, infinitament més", comenta Delgado. Al taller expliquen que cal saber protegir les dades personals per si algú ens roba el mòbil o l'ordinador, però també poder decidir què és públic sobre nosaltres a internet. "Tenim tot el dret a amagar", afirma Delgado, taxatiu. I per amagar, una fórmula antiga però que cada vegada es revela més útil i més popular és el xifratge. No només és la manera de funcionar que té el TOR (The Onion Router), un servei de navegació anònima que s'està estenent. També fan servir l'encriptació moltes altres eines i serveis.

Orígens
La xarxa ve d'un món idíl·lic en què tot era "bon rotllo" i bones intencions

Pioner
El 1991 un alemany ja va crear un sistema de xifratge molt modern

Iparraguirre i Delgado recorden que les operacions de banca electrònica o les transaccions comercials a internet acostumen a ser xifrades. Malgrat que aporta seguretat, l'encriptació també provoca les suspicàcies dels governs. Fa poques setmanes, després de l'atac al setmanari *Charlie Hebdo*, el primer ministre britànic, David Cameron, va anunciar la intenció de prohibir en la pròxima legislatura eines xifrades com el WhatsApp o l'Snapchat. Iparraguirre ho veu una mesura absurda per lluitar contra el jihadisme i ho interpreta com una excusa dels governs per controlar internet.

Por de les elits polítiques

Els dos enginyers informàtics rebutgen l'anunci de David Cameron, però també altres iniciatives similars que interpreten com intents de controlar la xarxa, com ara que la policia o les autoritats demanin sistemes d'encriptació als quals puguin accedir. "Si té una clau per a la policia, té una clau per a tothom", explica Iparraguirre. També critiquen que el fet d'utilitzar algunes eines –com ara instruments comuns per fer auditories de seguretat informàtica– et situï com a possible "sospitós" davant les autoritats.

Delgado recorda que aquesta por de les elits polítiques cap a la llibertat de la xarxa no és nova i rescata el cas de Phil Zimmermann, un dels pioners del xifratge que ja l'any 1991 va crear el PGP (Pretty Good Privacy), un programari que encara es fa servir avui i en el qual la NSA, l'agència de seguretat dels Estats Units, no ha aconseguit penetrar. Almenys així ho apunten les últimes revelacions de Snowden fetes públiques a finals de l'any passat pel setmanari alemany *Der Spiegel*. El cas és que Zimmermann va ser investigat per una possible violació de la llei d'exportació de *software* de xifratge dels Estats Units, però finalment l'acusació es va retirar. Washington veia amb recel que el xifratge estigués a l'abast de tothom.

Postal electrònica

Malgrat que l'encriptació és un mètode antic, encara avui moltes comunicacions no l'utilitzen, com ara la majoria de serveis de correu electrònic. "Se li hauria de dir postal electrònica, més aviat", reflexiona Iparraguirre. Els serveis d'emmagatzematge d'arxius al núvol, com Dropbox, també són poc segurs. Malgrat que per accedir a aquests serveis cal un nom d'usu-

MANOLO GARCÍA

ari i una paraula de pas, aquestes dades viatgen amb poca protecció per la xarxa i es podrien produir accessos no desitjats a la informació que es guarda al núvol. De fet, l'any passat, en resposta a una consulta feta pel Col·legi d'Advocats, l'Autoritat Catalana de Protecció de Dades reconeixia els "riscos" de guardar informació a Dropbox, Google Drive i Microsoft Onedrive. Serveis com SpiderOak o Wuala prometen xifratge i més seguretat. Iparraguirre, a més, té dubtes sobre els wifis públics o compartits amb altres usuaris, en què algunes persones amb coneixements informàtics avançats poden aconseguir interceptar els arxius o les informacions que hi viatgin.

"Estic en contra de qualsevol control d'internet", es posiciona Delgado. Els dos enginyers es mostren convençuts que iniciatives com les de Cameron o d'altres d'autoritats que volen tenir una clau per accedir a informació encriptada no fructificaran. Confien que cada intent de control serà respost amb una drecera: "La xarxa interpreta la censura com una errada i li fa un *bypass*. És el disseny tecnològic", remarca a l'ARA Iparraguirre. Després de la sessió a Cornellà, els dos professionals ja preparen la pròxima *cryptoparty*.

La de Cornellà és només una de les *cryptoparties* que es fan arreu del món i que volen ajudar els usuaris a xifrar els seus moviments a la xarxa. M. GARCÍA