

Contro il cyberfascismo: autodifesa dei diritti digitali e indipendenza tecnologica

*«Quando hanno rediretto i DNS catalani
non ho aperto bocca
perche non ero catalana
Quando hanno sequestrato i server agli hacker
non ho aperto bocca
perche non ero un hacker
Quando hanno bloccato gli indirizzi IP ai sindacalisti
non ho alzato le mani in protesta
perche' non sono sindacalista
Quando hanno tagliato la connessione ai migranti
non ho detto una parola
perche' non sono un'immigrata
Quando infine sono venuti e mi hanno sequestrato il telefono
non c'era piu' nessun DNS, IP, servers o connessione che potessi usare
per denunciarli.»*

Martin Hackmüller

Le immagini della repressione contro le persone che hanno sostenuto il loro diritto a decidere per se stessi, il 1° ottobre in Catalonia, hanno fatto il giro del mondo. Più di 800 cittadini feriti e milioni di persone che ha partecipato al referendum, attestano la durezza repressiva di quel giorno: botte, calci e colpi contro persone che difendevano le urne, più la paura e l'incertezza di non sapere quando arrivano a prenderti.

Quello che NON ha avuto abbastanza attenzione sociale o mediatica è stata la repressione informatica che durante quel giorno e durante le due settimane precedenti ha colpito innumerevoli persone, infrastrutture, scuole, server, connessioni e dispositivi. Un attacco senza precedenti (né nello stato spagnolo né in Europa) e che crea un pericoloso precedente per brutalità e violenza tecnologica, soprattutto quando è occultato o presentato dai media come irrilevante, o perfettamente legittimo in una società democratica. Una violenza coperta dallo stesso sistema giudiziario [cut] che non ha esitato a dettare frasi bestiali e assurde come quelle di "cancellare l'identità digitale" di una persona il cui "crimine" è stato quello di insegnare a clonare un sito web. Una violenza praticata in tutti i livelli di Internet: fornitori, gestori di domini, contenuti, IP, DNS, connessioni e dispositivi.

Ecco una sintesi degli eventi repressivi che sono avvenuti in quei giorni:

- * Cambio dei DNS dagli operatori dei domini
- * Reindirizzamento del traffico HTTP
- * Blocco del traffico SSL-to-IP
- * Taglio fisico delle connessioni Internet della Rete Educativa della Regione
- * Chiusura di web hosting delle società di hosting catalane
- * Attacco DDoS all'IP per la registrazione nelle liste del referendum
- * Detenzione e minacce, alle persone che hanno inviato risposte via web, di requisizione dei dispositivi telefonici, computer e cambio della password dell'account github
- * Monitoraggio degli IP delle istituzioni educative pubbliche
- * Rimozione di un'applicazione informativa dal Play Store (Android - Google)
- * Hanno obbligato i sysadmin a rivelare le password delle applicazioni delle istituzioni pubbliche

Alcune voci hanno descritto questi fatti come "la prima cyberguerra" contro la democrazia. Una guerra asimmetrica, dove un governo e le sue forze armate hanno attaccato con tutti mezzi possibili, mentre altri esseri umani difendevano in forma non violenta le loro infrastrutture e diritti digitali. In larga misura le istituzioni catalane e la società civile sono riuscite ad impedire alla repressione di arrivare al suo scopo. Ma questo tentativo è molto grave e le forze repressive hanno un obiettivo a cui noi abbiamo il dovere di opporci: vogliono attivare e normalizzare il fascismo cibernetico.

Come in tutte le guerre e le forme del fascismo, le prime vittime sono i diritti fondamentali: in questo caso il diritto all'accesso alle informazioni, il diritto di connettersi e il diritto all'espressione libera.

Purtroppo, se non facciamo niente, il cyber fascismo "da solo" non si fermerà qui. Dalla Ingoberhack, l'Hackmeeting 2017 che è stato a Madrid, vogliamo denunciare i fatti e ricordare che:

1. Soprattutto e al di là di tutte le misure di protezione e di resistenza tecnologica, vogliamo e pratichiamo: il rispetto al diritto di accesso alle informazioni, la connessione e la libertà di espressione, il diritto a infrastrutture che permettono alla gente di collegarsi, di dialogare e di esprimere i loro desideri, opinioni e affetti.

2. Quando la repressione viene esercitata su infrastrutture di internet, colpisce tutte le persone. È responsabilità di tutta la società denunciare e difendersi da questa repressione.

3. che la garanzia dell'esercizio effettivo di questi diritti, in ultima analisi, risiede in una sovranità tecnologia che ci riguarda in modo identico: nello sviluppo di infrastrutture di connettività libere, come Guifi.net, nello sviluppo e diffusione di sistemi di traffico distribuiti come Tor, nella costruzione e nell'uso di informazioni P2P come IPFS, nella promozione e nella formazione popolare di strumenti di crittografia (come GPG), nella promozione e la difesa del Software Libero.

4. che questa sovranità tecnologica e la libertà di informazione siano la condizione della possibilità di una società libera. Al di là di qualunque altra questione politica, dobbiamo difendere l'uso di questi strumenti che ci permettono di esprimerci e di organizzarci come esseri umani liberi.

Per questo motivo, al di là di specifiche opinioni politiche, lanciamo una chiamata per difendere i luoghi digitali che garantiscono la libertà di espressione tra pari.

Per approfondire:

<http://censura10.musaik.net/>

<https://es.hackmeeting.org/>

HACKMEETING 2017



INGOBERHACK