

LIBERTÀ E DIRITTI? TOCCA SUDARLI. ANCHE IN RETE

Infoaut intervista Autistici/Inventati

«Non pensiamo la nostra struttura come una risposta al controllo statale, ma più in generale come l'unica cosa decente venutaci in mente per garantire libertà d'espressione ed evitare la profilazione selvaggia da parte di aziende e governi». Sono queste le prime parole digitate da uno dei ragazzi di Autistici/Inventati appena cominciamo la nostra chiacchierata in una delle chat room del loro network. Una precisazione necessaria, soprattutto dopo che gli scossoni del terremoto Snowden hanno cominciato a sentirsi anche in Italia. Sono i primi giorni di agosto quando Lavabit e Silent Mail, due provider statunitensi di posta orientati alla tutela della privacy, vengono costretti a chiudere i battenti a causa delle minacce dell'NSA. Centinaia di migliaia di utenti restano improvvisamente senza strumenti di comunicazione sicura e molti di loro si rivolgono ad AI in cerca di una soluzione alternativa. In poco tempo il collettivo viene sommerso da un'ondata di richieste d'iscrizione ai suoi servizi. Un fatto che ha segnato un momento di difficoltà per la crew di hacker nostrani, tanto da determinare la temporanea sospensione dell'apertura di nuovi account. Ma che ha anche alimentato un forte dibattito in seno ai partecipanti del progetto sulle prospettive da intraprendere. È difficile per adesso dire come il datagate cambierà le esperienze di comunicazione autogestita. Autistici sa solo che potrà affrontare le nuove sfide all'orizzonte con una certezza che l'accompagna da più di 10 anni: quella di non essere un semplice servizio di posta ma una comunità. Che oggi ha bisogno del supporto di tutti quelli che si sentono di farne parte.

IFF: *Dopo la chiusura di Lavabit la quantità d'iscrizione ai vostri servizi è stata tale da costringervi a sospendere temporaneamente l'apertura di nuovi account. Nella decennale storia di AI fatti di questo tipo si erano verificati solo di fronte ad eventi repressivi di estrema gravità (come il crackdown Aruba). Perché avete definito quest'ondata di richieste «preoccupante»?*

Joe: Partiamo da quest'ultimo punto. Preoccupante è il fatto che ci sia gente che per le sue necessità non ha alternative rispetto ad Autistici/Inventati. Se nel tuo modello di

comunicazione c'è un singolo *point of failure* siamo immediatamente di fronte ad un problema. Se cioè c'è un solo bersaglio da colpire, è più facile prenderlo di mira. In questo momento di fatto sono rimaste poche o nulle alternative “commerciali” che oltre ai loro servizi offrano anche la possibilità di usufruire del diritto alla privacy. Detta in altro modo sono rimaste poche alternative commerciali che non collaborino fattivamente con i servizi segreti americani.

Ginox: Oltre a questo è preoccupante che le persone che ci richiedevano un servizio si fidassero di noi solo perché avevano trovato il nostro link da qualche parte in rete. Questa dinamica riproduce un meccanismo di delega che in buona sostanza sposta solo il problema della privacy sul lato tecnico o sulla necessità immediata di trovare un'altra mail. Ma il punto da affrontare è politico: riguarda sia il rapporto tra gli americani ed il proprio governo, sia tra il resto del mondo e gli Stati Uniti.

Pepsy: A quanto detto da Joe aggiungerei anche che l'ondata era “potenzialmente” preoccupante perché Lavabit al momento della chiusura dichiarava 410.097 utenti.

IFF: *Ma quante sono state le richieste di iscrizioni che avete ricevuto in quel periodo? Di quali numeri stiamo parlando?*

Ginox: La curva oscilla a seconda dei lanci giornalistici sull'argomento in cui in qualche modo venivamo citati. Nello specifico, subito dopo la chiusura di Lavabit ci sono arrivate, diciamo, 10 volte il tasso di richieste che riceviamo di solito. Abbiamo registrato picchi di 200 richieste in coda giunte in poche ore, principalmente di mail. Eravamo ad un bivio: potevamo scegliere se accogliere tutti a caso oppure soffermarci a riflettere sul senso di quanto stava accadendo. Abbiamo scelto la seconda strada.

Joe: Vorrei aggiungere che tecnicamente non avremmo avuto particolari problemi a gestirci questo flusso improvviso di richieste.

Ginox: Sì, sarebbe bastato prendere altri server, ma avremmo avuto sicuramente qualche difficoltà a gestire l'*helpdesk*. Questo tipo di scelta però non avrebbe rappresentato una soluzione.

Pepsy: E poi siamo abituati a confrontarci sempre quando c'è qualche problema, fa parte del DNA di A/I. Lo facciamo sia internamente sia attraverso i comunicati sia su cavallette.noblogs.org, dove cerchiamo un feedback dalla comunità.

Ginox: Noi vorremo che emergesse bene la contraddizione generata dalla chiusura di questi servizi commerciali. Dato che la natura del nostro progetto è differente, abbiamo pensato di prenderci del tempo: i nuovi utenti si relazionavano con noi come se fossero

dei clienti e quindi ci è parso il caso di mettere in campo un momento di chiarimento. La nostra comunità resiste ai problemi repressivi o di censura perché ha delle affinità e sa unirsi nelle difficoltà. Qui invece ci sembrava che molte delle persone che richiedevano di poter utilizzare i servizi si fossero spostate da Lavabit senza battere ciglio, esattamente come avrebbero fatto con noi se ci fossimo trovati nella medesima situazione.

Joe: Infatti tra i commenti al post sul blog in cui spiegavamo che le attivazioni erano temporaneamente sospese, puoi trovare anche quelli che dicono: «*Ma io vi pago!*». No, non funziona così, ovviamente. Ed abbiamo cercato di ribadirlo.

IFF: *Quest'impennata di richieste è arrivata solo dopo la chiusura di Lavabit (e quindi anche dopo la sovraesposizione mediatica che avete avuto sul Washington Post e sul New York Times) o anche già con l'esplosione del "datagate"?*

Pepsy: Qualcosa si era cominciato a vedere già nella fase immediatamente successiva alla rivelazione di PRISM al grande pubblico.

Joe: Sì, ma c'è stato un trend costante di crescita delle richieste anche prima del datagate. Poi senza dubbio con le dichiarazioni di Snowden le richieste sono aumentate. In particolar modo dopo che il sito [prism-break](#) ci ha indicato come una delle possibili alternative gratuite.

Ginox: Nella quasi totalità dei casi si è trattati comunque di richieste provenienti da utenti statunitensi.

IFF: *AI è probabilmente il network autogestito più importante d'Europa. È risaputo che le Forze dell'ordine avanzino spesso richieste di log o di informazioni relative agli utenti della vostra piattaforma. Dopo il datagate avete ricevuto più pressioni rispetto al passato? È cambiato qualcosa nell'atteggiamento delle FdO?*

Ginox: Non sappiamo dirlo ancora. Senza dubbio l'esposizione mediatica a cui siamo stati sottoposti negli ultimi tempi avrà modificato la percezione che hanno di noi i "servizi". Vedremo in futuro se questa cosa avrà delle conseguenze o meno. Ora come ora non è successo nulla di nuovo, né abbiamo registrato pressioni più esplicite del solito. Di tanto in tanto i nostri server sono oggetto di sequestri clamorosi. Solitamente però quelle che riceviamo dalle FdO sono richieste di routine: riguardano acquisizioni di dati che non abbiamo. Normalmente il tutto finisce con un fax dove comunichiamo che non siamo in possesso delle informazioni che ci vengono richieste.

Joe: La nostra strategia di fondo è quella di non tenere in memoria alcuna informazione utile alla profilazione degli utenti, secondo quello che per noi è semplice rispetto



delle libertà individuali e buon senso. Va anche sottolineato però che in Italia le indagini tendono ormai a concentrarsi direttamente sull'utente piuttosto che sul servizio, ricorrendo anche a *malware* per compromettere il computer dell'indagato e tenerlo sotto controllo a sua insaputa (la nostra legislazione li chiama “*captatori informatici*”). L'utente finale di solito è l'anello debole della catena e le FdO nel 99% dei casi preferiscono prendere direttamente da lì le informazioni che gli servono. L'intento è duplice: da una parte raccogliere elementi probatori dall'altra portare avanti attività d'intelligence attraverso cui ricostruire gli insiemi relazionali del soggetto interessato. È anche per questo motivo che periodicamente insistiamo sul fatto che la tutela della propria privacy non può essere delegata a nessuno. Neanche a noi.

Ginox: Tutte le polizie europee mostrano un'attenzione crescente per i “captatori informatici”. La prassi è simile alle intercettazioni ambientali, ma con molte più implicazioni, poiché si va a mettere mano su quello che in seguito potrebbe essere utilizzato come prova in caso di processo. Il che è una pratica piuttosto discutibile. Per ora questi oggetti sono equiparati ad un'intercettazione, ma in maniera sufficientemente ambigua per farne uno strumento agile per le FdO, e con pochissime garanzie per gli indagati.

Pepsy: Ci sono numerose aziende anche italiane specializzate in questo genere di lavori.

Joe: Già. C'è un mare di consulenti che fanno il lavoro sporco per le procure (salvo poi mettersi le magliette hacker quando vanno ai meeting della comunità).

Ginox: In Italia il mercato della sicurezza informatica decolla intorno al 2000. Andrea Pompili, autore del libro *Le Tigri di Telecom*, security manager dell'azienda arrestato all'interno dell'inchiesta Telecom-Sismi, spiega bene l'atmosfera che si respirava all'epoca. Dalle sue ricostruzioni appare chiaro come quello della sicurezza sia un mercato pompato dove qualsiasi minchiata può fruttare un sacco di soldi. Cerchiamo di capirci: i "captatori informatici" non sono nulla di nuovo se non rimaneggiamenti di idee partorite in passato dal giro hacker: non fanno nulla di diverso da, che so Dark Comet o lo storico Back Orifice o altri *rat* (categoria di software per controllare da remoto un computer). La differenza è che oggi il commercio di questi gingilli per le intercettazioni viene infiorato con un "marketing dell'emergenza". Pensiamo per esempio al tormentone della *cyberwar*. La richiesta di questi strumenti va di pari passo con la scoperta di Stuxnet o di Flame, due *malware* utilizzati in operazioni di intelligence in medio oriente. Da allora tutti i governi stanno cercando di attrezzarsi. Una storia interessante in termini di malware e polizia è il caso tedesco, smascherato dal Chaos Computer Club.

Joe: Già. La *cyberwar* è un concetto indefinito, rarefatto, aleatorio. Una *buzzword* che non si capisce bene cosa indichi e che come tale di norma viene utilizzata da gente che non ne conosce il senso, non sa di cosa sta parlando e quindi usa il latinorum.

IFF: *Dopo la chiusura di Lavabit e di Silent mail anche Riseup ha preso parola pubblicamente. In un suo recente comunicato ha affermato che sta ridisegnando l'architettura del suo network in modo da renderla ancora più sicura. L'obiettivo è quello di non trovarsi in una situazione simile a quella di Lavabit, ovvero essere obbligati a scegliere tra due mali minori: collaborare con l'NSA o dover spegnere l'infrastruttura. Anche voi avete in programma qualcosa di simile o pensate che sia sufficiente il piano R* da voi implementato ormai diversi anni fa?*

Joe: Riseup in questo momento sta lavorando ad un progetto che includa la crittografia *end-to-end* e che renda impossibile, anche allo stesso gestore del servizio, sapere cosa transita sui suoi server. Per fare questo però è necessario proporre nuovi strumenti agli utenti. Senza dubbio noi ora non forniamo crittografia *end-to-end* trasparente. Se vuoi cifrare la posta devi essere tu a farlo. Mi spiego meglio: ad oggi se un utente riceve in chiaro una mail su un server di AI, io in quanto amministratore sono in grado di accedere al contenuto di quella mailbox. Se tu invece attivamente scambi email solo in forma cifrata con GPG, allora neanche io ho la possibilità di leggerla. Questo non toglie che sui nostri server le caselle di posta si trovino su dischi cifrati: anche in caso di sequestro risulta molto difficile accedere a quei dati. È il motivo per cui consigliamo di scaricare la posta e non lasciarla sui server. Ed è un consiglio valido in generale, non solo per i nostri utenti.

Ginox: Stiamo osservando e studiando le soluzioni disponibili per capire come affrontare questi problemi, consapevoli del fatto che non avremo una soluzione pronta tra due mesi. Quello illustrato da Joe però è il punto della questione che Riseup sta affrontando: se anche gli amministratori di un network non hanno alcun accesso ai dati degli utenti allora non c'è profilazione possibile, né nulla di utile che possa essere richiesto in tal senso.

Joe: E così facendo viene resa ancora più complicata l'intercettazione dei dati in transito su Internet, cosa che sappiamo bene – e PRISM l'ha confermato – essere un bel problema.

Ginox: Si tratta di un progetto sicuramente più avanzato del Piano R* che abbiamo attualmente implementato e che nasceva da un contesto diverso. Noi, per la nostra “esperienza repressiva” negli anni passati ci siamo posti il problema di distribuire i server, cioè decentralizzare la struttura, e di oscurare un po' le cose per rendere bassa la probabilità che un sequestro porti al server giusto. Loro adesso stanno affrontando un altro pezzo del problema.

IFF: *Autistici vive da anni di donazioni e contributi economici volontari. Prima mi raccontate però che dopo quanto accaduto ad agosto alcuni utenti si sono detti disponibili a versare una quota annuale obbligatoria per mettervi nella condizione di continuare ad erogare i servizi e mantenere la vostra policy in fatto di privacy. Non pensate che questa opzione renderebbe più semplice affrontare la situazione d'emergenza che state attualmente attraversando?*

Ginox: No, non vogliamo che le persone pensino di poter comprare libertà e diritti. Quelli tocca sudarli. È il motivo per cui eravamo in imbarazzo in questi giorni a rispondere alle richieste di attivazione: capivamo che ci trovavamo di fronte a questo ragionamento, magari fatto in buona fede ma che non va nella direzione in cui ci muoviamo noi. Non ci interessa mettere quote fisse o far diventare Autistici il nostro lavoro: non saremmo più in grado di essere credibili. Se agli utenti di Lavabit da noia aver perso un servizio utile, se si sentono privati di un loro diritto... beh, andassero nel Maryland a prendere a pietrate la sede dell'NSA e non si limitassero a cercare di comprare una mail da un'altra parte.

Joe: Tocca essere pronti ad agire in prima persona, senza deleghe. In un mondo di spettatori e votanti questo spesso è spiazzante. Il problema che sta a monte è proprio il concetto malato di democrazia che è filtrato alla gente: passa tutto per la delega, mentre perfino i teorici della democrazia borghese ti direbbero che questa è una baggianata. Poi c'è anche l'atteggiamento capitalista del *mi-serve-qualcosa-e-quindi-lo-compro*. Che in effetti, vedendo il mondo intorno è un meccanismo universale. Noi ovviamente ci

opponiamo a questa visione. Inoltre credo sia più interessante fornire servizi ad un attivista ucraino per cui 15 euro sono una cifra significativa, piuttosto che alla middle class statunitense per cui 15 euro sono facili da spendere. Ci sono quindi ragioni pratiche e politiche per non accettare questo ragionamento.

Pepsy: Diciamo che non abbiamo simpatia per la mercificazione in genere.

IFF: *Com'era ipotizzabile qualcuno ha colto al balzo la palla del "datagate". La settimana scorsa Kim Dotcom ha lanciato una campagna di marketing per pubblicizzare un nuovo servizio di mail sicura. Così facendo ha scelto di continuare a battere quella strada che a gennaio aveva portato all'apertura di Mega, alla cui base sta un'idea semplice: gli utenti in internet non hanno alcuno status giuridico. La loro privacy non è protetta da alcun tipo di tutela legale. Chi desidera ottenere riservatezza in rete deve quindi acquistarla. Mi pare che questa dinamica presenti delle ambivalenze. Da una parte è innegabile che l'affermazione di questo modello d'impresa sancisca definitivamente la privatizzazione della privacy: questa smette di essere un diritto e viene garantita solo in quanto bene scarso, in quanto servizio erogato dietro compenso da attori privati. Con una metafora potremmo dire che anche in rete l'accesso alla cittadinanza è ancorato al reddito. Allo stesso tempo però il fiorire dell'industria della privacy rende accessibile la crittografia per le masse e più complicato il lavoro delle agenzie di law enforcement. Lo stesso caso di Lavabit è paradigmatico: fa riflettere come,*



nonostante la supremazia tecnologica, la più grande super potenza del mondo abbia avuto bisogno di ricorrere a pesanti intimidazioni di fronte ad uno strato di cifratura. Per altro senza nemmeno riuscire a conseguire il suo obiettivo. Che ne pensate? Non credete che questo fenomeno possa avere anche ricadute positive?

Joe: Mi pare chiaro da quanto detto prima che crediamo che il problema della privacy sia più politico che tecnico. Quindi non penso che l'industria della privacy risolva alcunché, dato che abbiamo a che fare con un antagonista con risorse sostanzialmente illimitate e con cui ogni "corsa agli armamenti" promette poche speranze di vittoria. La soluzione tecnica non può che essere parte della soluzione. E sospetto fortemente che sia una parte abbastanza secondaria. Poi mi aspetto che un po' di gente crei servizi per riempire questo vuoto del mercato. Ci saranno quelli con buone intenzioni (come Lavabit) e quelli che sono interessati solo ai soldi, in stile Kim Dotcom. Nello specifico le iniziative di "mister Mega" hanno uno scopo fondamentale: parargli il culo mentre conta i nostri soldi. Di fronte ad un'entità come l'NSA della privacy degli utenti a lui non frega nulla: basta guardare com'è fatto mega.co.nz per capirlo. E comunque dal punto di vista dell'utente significa mettere la tua privacy nelle mani di un ente privato che ha interessi diversi dai tuoi. Io personalmente non mi fiderei mai :-)

Ginox: L'uso della crittografia di massa è sempre stato legato allo sviluppo del commercio elettronico. Negli anni '90 la crittografia viene strappata all'NSA ed ai militari perché il mercato aveva bisogno di soluzioni per garantire la sicurezza delle transazioni, altrimenti non sarebbe mai potuto decollare. Credo che questa sia un'ambiguità irrisolvibile che però lascia aperto il nodo politico della questione, come diceva anche Joe. Così va il capitalismo: distrugge valore per creare profitto, dalle macerie di una cosa ne crea un'altra e apre degli spazi di mercato.

Joe: Posso fare una postilla che mi viene spontanea? È veramente divertente vedere come funziona bene il "libero" mercato. Tanta gente nel mondo vuole ottenere un servizio di posta sicura... e la loro migliore opzione è un gruppo di attivisti anticapitalisti italiani? Beh, non mi pare esattamente un prototipo di efficienza.

Pepsy: Sulla deficienza del mercato sono d'accordo. Un po' meno sull'esempio fatto da Joe perché tutto sommato lo tsunami di richieste non è ancora arrivato: evidentemente non siamo la sola alternativa. La necessità di mail sicure d'altra parte viene gestita direttamente anche da enti e società private.

Ginox: La Germania per esempio sta tentando a sua volta un approccio diverso. Non so se definirla una barzelletta, un moto d'orgoglio o qualcosa da buttare sul piatto della diplomazia. La proposta del governo tedesco di offrire ai suoi cittadini servizi "made in Germany" è un po' l'equivalente del dire: «Non fatevi spiare dall'NSA! Fatevi spiare solo

dai nostri servizi segreti!» Si tratta quindi di una soluzione che tecnicamente non risolve nulla, però sposta il soggetto in campo e delinea un'inversione di tendenza: si passa da un attore privato ad un ritorno dello stato nella gestione delle comunicazioni.

IFF: *In un certo senso potremmo dire che anche la Germania sta perseguendo una balcanizzazione di Internet seguendo l'esempio russo e cinese (fatte le debite differenze ovviamente)?*

Ginox: Sì, qualcosa del genere, pur elaborando risposte diverse rispetto a Mosca e Pechino.

Joe: Anche perché una balcanizzazione in stile cinese in Europa non potrà mai funzionare a meno che non si voglia creare uno spaventoso effetto recessivo in uno dei pochi settori floridi dell'economia occidentale. In realtà io credo che quella del governo tedesco sia stata una mossa per dare un contentino ad un'opinione pubblica inferocita ed allo stesso tempo uno stratagemma per avere un argomento di trattativa con gli Stati Uniti.

Pepsy: Da parte mia credo che la rete sia sempre stata balcanizzata. Rispetto ad Internet c'è ancora troppa mitologia: quella di una rete "anarchica" che porta libertà. Una mitologia che cela le internet iraniane, nord coreane e cinesi e che allo stesso tempo ci fa però dimenticare che fino all'altro ieri anche in Italia bisognava dare i documenti per accedere ad un hotspot wifi pubblico. Una mitologia insomma che nasconde il fatto che la rete ha dei padroni, da sempre.

Ginox: Internet riflette rapporti di forza materiali: più si espande e più si lega al reale rispetto a quando era composta da qualche milione di utenti. Nel mondo reale i soldi contano e le aziende si mangiano a vicenda. È il capitalismo baby! Il mercato è una parte importante e aggressiva della rete: è stata una scelta precisa quella di smettere di sovvenzionare Internet con soldi pubblici e fare in modo che soggetti privati la lottizzassero. Finanza e politica vanno a braccetto, la rete tende a polarizzarsi verso grossi soggetti così come il capitale tende a concentrarsi in grossi monopoli e cartelli, o a essere terreno di bolle e speculazioni. La bolla delle *dotcom* ha anticipato quella immobiliare a dimostrare la fragilità di questa costruzione. La privacy è un mercato come un altro, dove c'è un bisogno il mercato accorre. I flussi di bit vanno a coincidere con i flussi finanziari. Segui quest'ultimi e capisci dove si concentra il potere. Sebbene il meccanismo sembri rodato e inarrestabile, in realtà va spesso in crisi e va avanti ad azioni di forza e calci in culo, con una certa tendenza al cannibalismo. E quando si crea una contraddizione c'è spazio per inserirsi. Questo sarebbe paradossalmente un buon momento per far nascere nuovi server autogestiti o progetti simili. Non saprei se ci sono soggetti interessati a farlo.

IFF: *Quindi secondo voi le rivelazioni di Snowden rappresentano un punto di forza per chi lotta per i diritti digitali?*

Ginox: Non solo per i diritti digitali. È un momento di forte imbarazzo per il governo americano. Se lo superano illesi allora ne usciranno fortificati. Altrimenti qualcuno se ne gioverà e credo che all'orizzonte si possono anche aprire spazi per le esperienze di comunicazione autogestita (a patto di saperle cogliere ovviamente). In generale poi è interessante che un impiegato metta in crisi una struttura da miliardi di dollari.

Pepsy: Ed è sempre un bene che ci sia il fattore umano che manda all'aria il sistema alla faccia degli incubi tecnologici. In questo caso è stato mosso un primo piccolo passo essenziale nella direzione giusta: certe tematiche stanno cominciando ad uscire dall'ambito underground.

IFF: *In che modo gli utenti possono aiutarvi in questo momento?*

Pepsy: Diciamo che ci piacerebbe che i nostri utenti imparassero a non delegare a noi la difesa della loro privacy.

Joe: Senza dubbio possono donare, mica ci fa schifo!

Ginox: Sì, ma quello possono farlo sempre. Nell'immediato i nostri problemi sono principalmente di relazione verso l'esterno. Chi utilizza i nostri servizi e vuole aiutarci può farlo diffondendo un semplice messaggio: ovvero che Autistici è in primis una comunità e non semplicemente un servizio mail. Poi certo, una crescita di consapevolezza tecnica sarebbe una cosa auspicabile e sempre utile. Soprattutto nel momento in cui ti rendi conto che dall'altra parte non si risparmiano.

[InfoFreeFlow \(@infofreeflow\)](#) per Infoaut

Questa intervista è stata pubblicata originariamente da [Infoaut](#)



Attribuzione – Non commerciale – Condividi allo stesso modo 2.5 Italia (CC BY-NC-SA 2.5 IT)