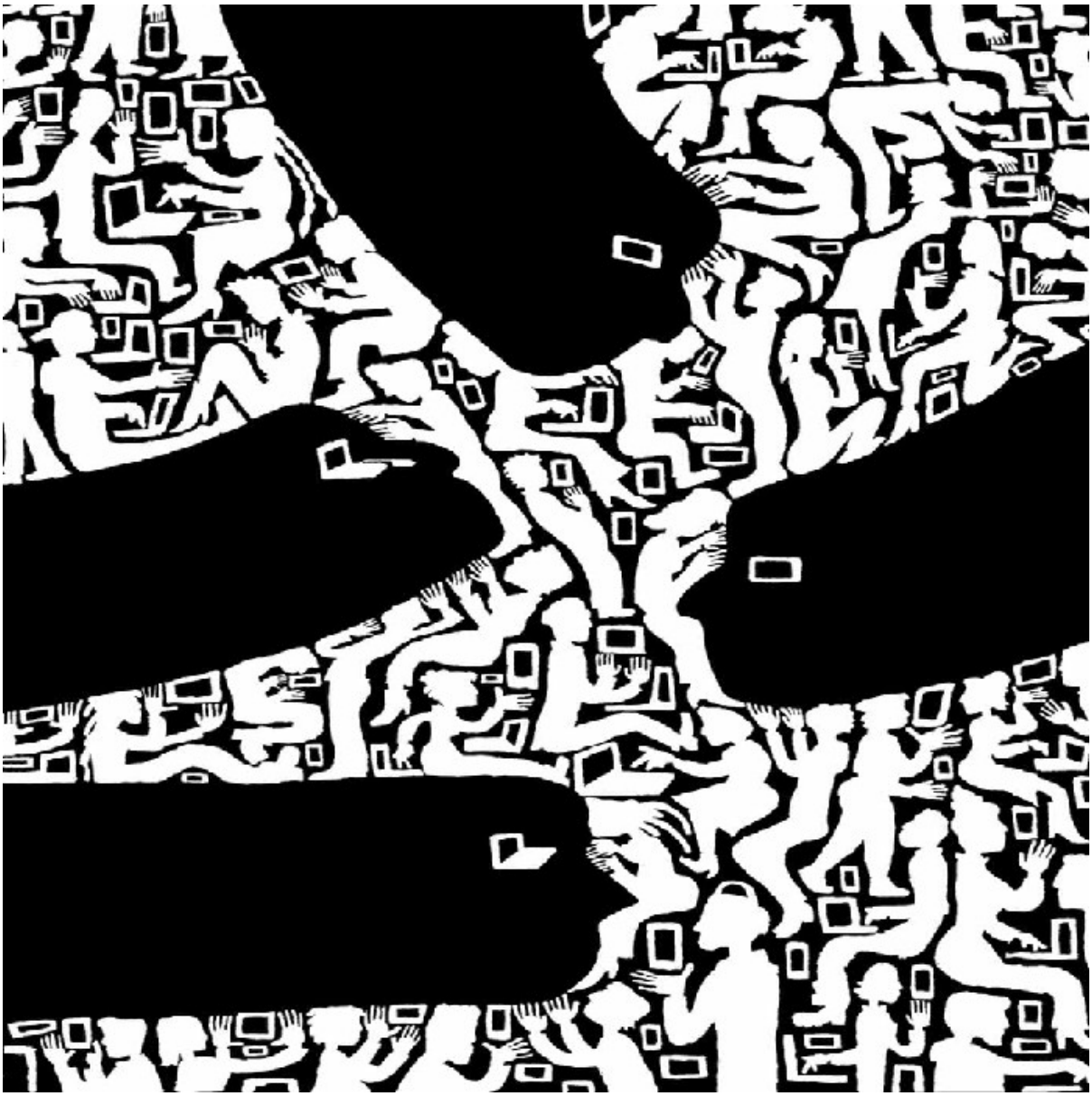
# I CUSTODI DELLE CRIPTO VALUTE



**SI PARLA DI TELEGRAM E DELLA SUA INTEGRITÀ**

Intervista a Pavel Durov di Yasha Levine - Settembre 2017

Sono le 19:30 un lunedì di giugno in una località segreta da qualche parte nel nord Europa. Sono seduta in una sala da pranzo privata in un hotel di lusso e parlo con Pavel Durov, il "Mark Zuckerberg della Russia", un giovane magnate di Internet che aveva costruito il social network più popolare del paese e lo aveva perso per il Cremlino prima di compiere trent'anni. Non molto tempo dopo che il famoso informatore americano Edward Snowden era fuggito in Russia per evitare il processo federale, Durov aveva offerto a Snowden un lavoro, ma poi lui stesso ha dovuto fuggire dalla Russia a causa di un conflitto in espansione con il governo

russo. Inizialmente acclamato come cyber-dissidente a causa dei suoi battibecchi con il Cremlino, Durov da allora ha attirato l'interesse ripetuto e aggressivo anche dei funzionari dell'intelligence americana.

Un gruppo di turisti facoltosi si aggirava nella hall, chiacchierando entusiasti della loro giornata di visite turistiche e visite ai musei. La nostra conversazione era di natura più oscura. Durov e io stavamo parlando del mondo torbido e iperparanoico del movimento per la privacy ossessionato dalle criptovalute, un luogo in cui le spie governavano, niente era come sembrava e nessuno poteva fidarsi.

Per me, la paranoia aveva un senso. Negli ultimi tre anni ho indagato sugli accessori tecnologici crittografici di base al centro del potente movimento per la privacy di oggi: anonimizzatori Internet, app di chat crittografate, caselle non rintracciabili per gli informatori e sistemi operativi super sicuri che persino la NSA presumibilmente non poteva decifrare. Questi strumenti sono stati promossi da giornalisti vincitori del Premio Pulitzer, hacker, informatori e dai nomi più grandi e credibili nel settore della privacy, da Edward Snowden alla Electronic Frontier Foundation e all'American Civil Liberties Union. App come Tor e Signal promettevano di proteggere gli utenti dall'apparato di sorveglianza onnicomprensivo americano. E i crittografi e i programmatori che hanno costruito le armi crittografiche di queste persone? Ebbene, molti di loro hanno affermato di vivere al limite: criptoanarchici sovversivi che combattono l'uomo, inseguiti e assaliti dalle oscure forze del governo degli Stati Uniti. Citando molestie, alcuni di loro erano del tutto fuggiti dagli Stati Uniti, costretti a vivere in esilio autoimposto a Berlino.

Almeno è così che si vedevano. La mia segnalazione ha rivelato una realtà diversa. Come ho scoperto scavando tra i documenti finanziari e le richieste FOIA, molti di questi sedicenti radicali online erano in realtà appaltatori militari, che ricevevano stipendi con benefici dallo stesso stato di sicurezza nazionale degli Stati Uniti che sostenevano di combattere. La loro audace tecnologia crittografica si è anche rivelata, a un esame più attento, una versione truccata e porosa di comunicazioni digitali sicure del Potemkin Village. Inoltre, il software in questione qui è stato esso stesso finanziato dal governo degli Stati Uniti: milioni di dollari all'anno fluiscono ai radicali criptati dal Pentagono, dal Dipartimento di Stato e dalle organizzazioni scorporate dalla CIA.

La mia indagine su questa comunità mi aveva portato molti abusi: calunnie e minacce di morte lanciate da appaltatori militari contro di me e contro i miei colleghi; false storie diffamatorie diffuse dalla stampa sul fatto che io sia una bulla sessista e un agente della CIA pagato per minare la fiducia nella crittografia. Così ho imparato molto tempo fa ad avvicinarmi alle mie fonti con scetticismo e diffidenza, specialmente qualcuno famigerato come Durov, che di recente era entrato nel business delle criptovalute con Telegram, che ora gode del primato di essere l'app di chat preferita dell'ISIS.

**Mogul in Movimento**

Anche Durov, che mi ha chiesto di nascondere il luogo del nostro incontro a causa del suo conflitto in corso con il governo russo, era diffidente. Aveva il diritto di esserlo.

Ora a trentadue anni, è un miliardario e, se si vuole credere ai giornali, è il magnate di Internet più radicale della Russia. Nel 2006, quando aveva solo ventidue anni, aveva co-fondato VKontakte ("In Contact"), un clone di social network di Facebook che divenne più popolare in Russia e nell'ex Unione Sovietica rispetto a Facebook stesso. L'azienda non è rimasta a lungo sotto il suo controllo. Nel 2011, in seguito alle proteste di massa dell'opposizione contro il partito al governo di Vladimir Putin organizzate in gran parte tramite i social media, il governo voleva una presa più salda su VKontakte. Durov ha resistito e ha compiuto ogni sorta di atto di sfida: ha scattato foto di documenti che ordinavano alla compagnia di bloccare determinati gruppi politici e li ha pubblicati online, e ha deriso pubblicamente i funzionari delle forze di sicurezza statali dell'FSB della Russia.

Ma il Cremlino ha insistito e finalmente ha ottenuto la sua strada. Durov si era stancato della costante raffica di tattiche di pressione da parte dello stato russo, inclusi i tentativi della polizia di fare irruzione nell'appartamento di Durov, un bizzarro incidente di ricatto che coinvolgeva quello che Durov dice essere un video falso che pretende di mostrarlo in una Mercedes nera che investe un vigile urbano, e accuse penali inventate che lo hanno costretto a lasciare il paese. Così, nel 2014, il giovane magnate dei social media è stato costretto a vendere la sua quota del 20% di VKontakte a un'azienda gestita dall'Uzbekistan Alisher Usmanov, uno spaventoso miliardario fedele al presidente Putin. Privato del suo impero, Durov non poteva più affermare di essere lo Zuckerberg della polizia russa.

Durov è fuggito dalla Russia e, dopo aver effettuato un investimento strategico sulle due isole di St. Kitts e Nevis, è diventato cittadino dei Caraibi. Negli ultimi tre anni ha vissuto la vita di un multimilionario autonomo e autosufficiente, vagando per il mondo vivendo in hotel di lusso, abbandonando beni materiali come terreni e proprietà immobiliari. Durov avrebbe potuto fare tutto ciò che voleva, e così mentre era in esilio, ha lavorato con suo fratello maggiore Nikolai alla prossima grande novità: incanalare il suo tempo e la sua ricchezza, stimata in circa 300 milioni di dollari, nello sviluppo di una nuova app di messaggistica, Telegram.

**Ottenere il Messaggio**

Non sorprende che il governo russo abbia di nuovo messo Durov nel mirino. I funzionari della sicurezza russi gli hanno fatto pressioni affinché condividesse i dati con loro o rischiasse di bloccare il suo servizio. Ma i russi non sono gli unici a provare a mettere le mani su Durov. A quanto pare, anche gli americani vogliono una parte dell'azione.

Mentre una cameriera portava un piatto di pane e alcuni antipasti - calamari affettati e tartare di tonno - Durov ha spiegato che negli ultimi anni, l'FBI ha tentato di spingerlo a collaborare segretamente con l'agenzia, e che gli agenti si erano spinti fino in fondo come tentare di corrompere uno dei suoi sviluppatori a diventare una talpa. Non aveva mai discusso completamente i dettagli dei suoi scontri con l'FBI in pubblico, fino ad ora.

Durov afferma che la pressione è iniziata nel 2014, poco dopo aver venduto la sua partecipazione in VKontakte. Fu allora che iniziò per la prima volta a essere regolarmente intervistato e interrogato dagli agenti dell'FBI al confine americano.

A volte lo detenevano per ulteriori interrogatori all'ingresso; altre volte lo raggiungevano per “chiacchierare” mentre era al gate che si preparava a salire su un aereo. All'inizio, l'FBI era curioso del suo portafoglio di lavoro presso VKontakte e del rapporto dell'azienda con le forze dell'ordine russe, comprese le procedure seguite per ottemperare alle richieste di dati del governo. "Non ero a mio agio con queste domande", ha detto. "Non avevo intenzione di diventare una talpa americana, quindi ho fornito loro solo le informazioni minime che erano già disponibili nei media".

Durov e io stavamo parlando del mondo oscuro e iperparanoico del movimento per la privacy ossessionato dalle criptovalute.

Nei viaggi successivi, tuttavia, i funzionari dell'FBI hanno iniziato a chiedere informazioni su Telegram. Dov'era basato? Come ha funzionato? Come potrebbe l'FBI mettersi in contatto con Durov in futuro? Gli agenti hanno risposto con note amichevoli via e-mail, dicendo a Durov di contattarli se avesse avuto problemi o avesse bisogno di aiuto per qualcosa. Durov dice che ha continuato a ignorare le aperture, ma l'FBI voleva chiaramente qualcosa; la domanda era cosa. Nel 2016, Durov ha ottenuto la sua risposta. A maggio è volato dall'Europa a San Francisco per partecipare alla conferenza annuale di Google. La prima mattina della sua visita, due agenti dell'FBI si sono presentati senza preavviso alle otto del mattino in una casa di Mountain View che stava affittando tramite Airbnb. "Come hanno ottenuto l'indirizzo?" Chiede Durov. “Forse hanno rintracciato la mia scheda SIM? Mi hanno seguito dall'aeroporto? Forse hanno ricevuto le informazioni da Uber? Non lo so."

In ogni caso, i due agenti erano chiaramente in missione. "Immediatamente hanno iniziato a chiedere informazioni su Telegram, il che mi ha fatto preoccupare", dice Durov, spiegando che non ci è voluto molto perché i suoi visitatori mattinieri arrivassero al punto: l'FBI voleva impostare una sorta di processo informale di backchannel (canale posteriore) ciò consentirebbe a Telegram di trasferire dati su determinati utenti in caso di minaccia terroristica; venivano persino preparati con in mano documenti dall'aspetto ufficiale. "Mi hanno mostrato un'ordinanza del tribunale e mi hanno detto: 'Rispettiamo molto i tuoi valori in materia di privacy e crittografia e rispettiamo ciò che stai cercando di fare. Ma c'è il terrorismo, è un problema serio e abbiamo il dovere di proteggere la società. Ci auguriamo che tu capisca e condividi le nostre opinioni. Vogliamo creare un processo di scambio di dati in modo che tu possa aiutarci in caso di minaccia terroristica", ha raccontato Durov. Durante i venti minuti di intervista, gli agenti hanno chiarito che speravano che questo fosse solo l'inizio di una relazione lunga e fruttuosa.

Telegram è registrata nel Regno Unito come Telegram Messenger LLP, una società di proprietà di altre due società, una nelle Isole Vergini britanniche; l'altro in Belize. I suoi dati vengono anche tagliati e distribuiti in più giurisdizioni, parte del piano generale di Durov che in teoria rendeva l'accesso legale ai dati degli utenti il più difficile possibile. L'azienda non aveva una presenza legale negli Stati Uniti, quindi l'FBI non aveva l'autorità reale per chiedere qualcosa a Durov o alla sua azienda. Durov ha detto di aver capito che l'ordinanza del tribunale era uno stratagemma - un tentativo di convincerlo a collaborare - ma ha continuato e ha promesso che sarebbe tornato dagli agenti dopo che il team legale di Telegram avrebbe esaminato il documento.

Tuttavia, Durov dice di essere rimasto un po' scosso dall'esperienza. "In Russia, i ragazzi dell'FSB con cui ho interagito non erano impressionanti. Erano di abilità media; non proprio qualificata. Negli Stati Uniti, l'FBI è diverso. Quelli che mi hanno interrogato erano competenti. Parlavano più lingue. Avevano fatto le loro ricerche e sapevano esattamente quali domande porre. Erano di grosso calibro. E ho capito che l'America ha così tante risorse dedicate alla sicurezza che è assolutamente spaventoso. L'applicazione della legge in America è molto più efficiente".

**Colpisci una Talpa**

Gli agenti dell'FBI se ne andarono, ma non avevano finito. Come racconta Durov, avevano anche messo gli occhi su uno sviluppatore di Telegram che era arrivato in aereo per la conferenza di Google e stava anche lui nello stesso Airbnb di Mountain View con Durov. (Un portavoce dell'FBI ha rifiutato di discutere qualsiasi dettaglio del racconto di Durov con The Baffler.)

Questo sviluppatore era già stato fermato e interrogato all'aeroporto da agenti della divisione informatica dell'FBI, ma l'FBI ha programmato un incontro di follow-up (azione supplementare) in un bar di San Francisco. Gli agenti che hanno incontrato lo sviluppatore lì hanno iniziato tempestandolo di domande generali sull'architettura di Telegram e su come funzionava il suo algoritmo di crittografia, il tutto elogiandolo per la sua conoscenza esperta. Non ci volle molto per ottenere ciò che volevano veramente: l'accesso, per il quale erano disposti a pagare. Durov non ha rivelato il nome di questo sviluppatore, ma ha raccontato la storia che alla fine gli ha raccontato il suo dipendente. L'FBI voleva elaborare un accordo in cui lo sviluppatore avrebbe fornito segretamente ai suoi agenti informazioni sul funzionamento interno di Telegram, cose come nuove funzionalità e altri componenti dell'architettura del servizio di cui avrebbero potuto desiderare di conoscere. L'accordo sarebbe stato strettamente confidenziale ed erano disposti a pagare. "Faremo in modo che ne valga la pena", hanno detto. Dissero che avrebbe "consultato" l'FBI, un eufemismo appena velato per quello che era chiaramente un compenso. "Gli agenti dell'FBI gli hanno dato una gamma", ha detto Durov, sgranocchiando un pezzo di pane. "Era nell'ordine di decine di migliaia di dollari."

Dopo che lo sviluppatore ha rifiutato l'offerta, l'FBI lo ha incontrato ancora una volta. Questa volta, gli intervistatori dell'FBI gli hanno chiesto di non dire una parola a nessuno sulla loro conversazione, e soprattutto di non dirlo al suo capo. "Erano specifici", ha detto Durov. "Non dirlo a Pavel, questo è il nostro segreto."

Si strinse nelle spalle e sorrise. Sembrava che l'FBI non fosse in grado di concludere l'affare. "Paghiamo molto bene i nostri sviluppatori", ha detto in un piccolo gesto di autocompiacimento manageriale. “I nostri sviluppatori sono tutti milionari. Naturalmente non possono essere corrotti con questo tipo di offerta. "

L'FBI che cerca di trasformare il suo stesso dipendente in una talpa contro di lui? Mi aspettavo che Durov traesse un grosso vantaggio da questa rivelazione. Le società della Silicon Valley e i tipi di privacy criptata colgono ogni opportunità per dipingersi come vittime dell'oppressione del governo e spesso fanno esplodere piccoli incidenti che

potrebbero tornare a vantaggio del loro marchio nelle guerre di segretezza. Pensa, ad esempio, a come Apple ha trasformato la richiesta dell'FBI di sbloccare un singolo telefono utilizzato in un attacco terroristico del 2015 a San Bernardino che ha lasciato quattordici persone morte in una posizione contro l'oppressione del governo, anche se la società si stava sottomettendo alle richieste di dati della Cina. (Alla fine, ovviamente, l'FBI ha ottenuto i dati che stava cercando nel caso San Bernardino utilizzando un hack di dati di terze parti.) Oppure c'era il caso recente di uno sviluppatore che aveva lavorato per Tor, uno strumento di anonimato di Internet finanziato dal Pentagono, ed è fuggito in Germania dopo che un agente dell'FBI ha lasciato il suo biglietto da visita a casa dei suoi genitori.

Date le tendenze libertarie di Durov e la sua vicinanza a quel mondo, pensavo che avrebbe iniziato a delirare contro la tirannia del governo, ma Durov era sorprendentemente, quasi snervante, equilibrato e ragionevole riguardo all'intera faccenda. Era turbato e sconvolto dalle tattiche di pressione dell'FBI e si è impegnato a resistere a tutti i tentativi dell'agenzia di ottenere i dati di Telegram. Ma non era nemmeno sorpreso che fosse successo. Dopotutto, è quello che doveva fare l'FBI. “Fondamentalmente, gli americani stanno facendo il loro lavoro. Guardalo dalla loro prospettiva. Ecco un ragazzo giovane, la sua app è usata dai terroristi. Dobbiamo scoprire chi è. Che tipo di squadra ha. Questo è logico. Non vedo niente di straordinario in questo ", ha detto. "Avrei potuto renderlo pubblico con questo quando è successo e ha fatto una grande puzza. 'Guardami, guarda come gli americani stanno mettendo le viti su di me.' Ma ho pensato che sarebbe stato un po' pretenzioso e melodrammatico. "

Allora perché rendere pubblica la storia adesso? Durov dice che si sta facendo avanti per sottolineare un punto più grande che di solito si perde nella sceneggiatura auto-drammatizzante degli scontri della Silicon Valley con i federali: quello che è successo a Telegram è abbastanza rappresentativo di come il governo cerca di guadagnare influenza sui servizi di Big Data. "Sto sollevando la questione solo per sottolineare che le agenzie di sicurezza americane sono persistenti e invadenti e che stanno solo svolgendo il loro lavoro. Ti raggiungeranno all'aeroporto. Si presentano senza preavviso al tuo Airbnb, l'indirizzo di cui nessuno dovrebbe sapere tranne te. Cercano di ripagare gli sviluppatori. In un modo o nell'altro, l'FBI sta facendo molto attentamente il suo lavoro e lo fa nell'arco di un paio di giorni che io e il mio team trascorriamo in America", dice.

Se l'FBI è stato così tenace e invadente con Telegram, arrivando addirittura a tentare di corrompere i suoi dipendenti durante un breve viaggio di lavoro, allora cosa fa il governo degli Stati Uniti alle aziende con sede permanente in America? "Non riesco a immaginare me stesso o chiunque altro che gestisca un'app orientata alla privacy in quell'ambiente. Possono iniziare le loro richieste di informazioni con dati relativi al terrorismo e poi estenderle gradualmente a chissà cosa ".

**Crittografa o muori!**

Nel giugno 2013, Edward Snowden ha progettato una fuga di dati ascoltata in tutto il mondo. Un appaltatore della NSA che lavora per il colosso dei dati e della legge di Beltway Booz Allen Hamilton, Snowden ha denunciato l'apparato di sorveglianza Internet americano e ha

contribuito a far luce sulla relazione simbiotica tra la Silicon Valley e il governo degli Stati Uniti.

I documenti che ha rubato da una struttura della NSA alle Hawaii hanno fornito la prima vera prova che le nostre aziende tecnologiche più rispettate, tra cui Google, Facebook e Apple, lavoravano a stretto contatto con le spie americane, intercettando segretamente le loro server farm per la NSA e l'FBI. La drammatica fuga di notizie di Snowden ha messo il problema della privacy su Internet sulla mappa in un modo che non era mai stato prima.

All'improvviso, la privacy su Internet stava guadagnando la copertura quotidiana delle notizie via cavo, le indagini in prima linea e i premi Pulitzer. Ci sono state proteste anti-sorveglianza, campagne online e una raffica di rapporti da parte di cani da guardia del governo e organizzazioni non profit per i diritti dei consumatori. Nel 2013, sembrava che potessimo essere sull'orlo di un movimento globale che avrebbe galvanizzato le persone a spingere per leggi significative sulla privacy che non solo frenassero la sorveglianza del governo, ma mettessero anche limiti alle pratiche di raccolta dati illimitate della Silicon Valley. Ma le cose sono andate diversamente.

Ora, quattro anni dopo la fuga di notizie di Snowden, possiamo vedere che tutta quell'energia, l'indignazione e il potenziale di azione civica sono stati reindirizzati in una banda ristretta di politica di massa per app. Il nuovo consenso, espresso a gran voce nella Silicon Valley e nei dintorni, sostiene che tutto ciò che dobbiamo fare per proteggerci dalla sorveglianza è scaricare qualsiasi app di chat crittografica in voga al momento ed eseguirla sui nostri iPhone. Invece di trovare soluzioni politiche e democratiche alla crisi del governo e della sorveglianza aziendale che affligge la nostra società, il movimento per la privacy in qualche modo è finito in un solco libertario. In un ordine notevolmente breve, i sostenitori della privacy online avevano abbandonato l'idea che le persone e la politica potessero cambiare il mondo in meglio, e invece hanno inseguito qualcosa di più vicino a una fantasia della NRA: l'idea che se tutti fossero dotati di un'arma crittografica abbastanza potente, avrebbero potuto affrontare da soli sia le corporazioni che potenti agenzie di spionaggio come la NSA. Potrebbero usare la tecnologia per garantire la propria privacy alle proprie condizioni.

Se il tuo nemico era il governo degli Stati Uniti, non importava quale app di crittografia avevi utilizzato.

Lo stesso Edward Snowden è stato il principale promotore di questa idea, non perdendo mai l'occasione di dire alla gente che la politica collettiva è inutile e che armarsi di tecnologia è il punto. Si scrollò di dosso la sorveglianza a scopo di lucro che alimentava le attività della Silicon Valley, dicendo seccamente al Washington Post che "Twitter non mette testate sulla fronte". Invece, vedeva aziende private come Apple e Facebook come alleati, forse gli unici posti che offrivano anche solo un minimo di sicurezza nella pericolosa landa selvaggia di Internet. Per lui, gli sviluppatori privati e gli ingegneri del software erano i veri protettori del popolo, e li invitò a sollevarsi contro l'oppressione del governo. "Se vuoi costruire un futuro migliore, dovrai farlo da solo. La politica ci porterà solo lontano e, se la storia è una guida, sono i mezzi meno affidabili per ottenere un cambiamento effettivo. . . in fin dei conti, la legge è semplicemente lettere su una pagina. Non salteranno in piedi e proteggeranno i tuoi

diritti ", ha detto al pubblico alla Fiera del futuro reale di Fusion 2016 a Oakland tramite collegamento video-robot da Mosca. A Snowden, ora un leaker, divenuto filosofo politico - i movimenti politici e l'azione collettiva erano volubili, sforzi puramente umani che non offrivano garanzie; la crittografia e la tecnologia informatica erano una cosa sicura, basata sulle leggi della matematica e della fisica. "La tecnologia funziona in modo diverso dalla legge", ha detto il fuggitivo alla folla alla Fiera del futuro reale. "La tecnologia non conosce giurisdizione."

Era una posizione assurda. Sostituisci "tecnologia" con "fucile d'assalto" e il discorso di Snowden si trasformerà in qualcosa che sentiresti a una conferenza del CPAC repubblicano. Tuttavia, Snowden ha ottenuto una standing ovation alla Fiera del futuro reale. E perchè no? Dal momento in cui Snowden è apparso sulla scena, la sua visione del mondo incentrata sulla tecnologia è stata sostenuta da un coro di giornalisti pluripremiati, attivisti per la privacy, think tanker di sinistra e potenti gruppi di difesa come la Electronic Freedom Foundation e l'ACLU. Anche la Silicon Valley ha sostenuto la chiamata alle armi di Snowden. Una nuova coraggiosa coorte di sviluppatori di app ha sostenuto soluzioni tecnologiche per la privacy molto ristrette che, secondo loro, avrebbero protetto i loro utenti dallo spionaggio del governo, il tutto mentre tracciavano senza vergogna questi stessi utenti per profitto e guadagno privato.

Come è successo, la chiamata di Snowden alle armi di crittografia ha contribuito a ispirare Pavel Durov a costruire Telegram. "Sono lontano dalla politica e non posso fare pressioni per un divieto di sorveglianza totale", scrisse nell'ottobre 2013, pochi mesi dopo che Snowden era fuggito a Mosca e subito prima che Durov a sua volta dovesse fuggire dalla Russia. “Ma c'è qualcosa che noi imprenditori e programmatori IT possiamo fare. Possiamo sviluppare e finanziare tecnologie volte a rendere tecnicamente impossibile la sorveglianza totale ".

In America, il movimento iniziale per portare la lotta anti-sorveglianza nella Silicon Valley è svanito e si è trasformato in qualcos'altro che era allo stesso tempo bizzarro e patetico: attivisti per la privacy che lavorano con Google e Facebook per combattere la NSA con la tecnologia della privacy. Ciò aveva esattamente tanto senso quanto schierarsi con Blackwater (o Xe o Acadami o come si definisce ora l'appaltatore del Pentagono) contro l'esercito degli Stati Uniti. Eppure questa tendenza della politica per app è andata in overdrive dopo che Donald Trump è stato eletto presidente. L'hai visto ovunque: libertari civili, difensori della privacy e liberali demoralizzati sono sorti per proclamare che la crittografia - anche le cose lanciate dai giganti della sorveglianza della Silicon Valley - era l'unica cosa che poteva proteggerci da un'amministrazione Trump totalitaria.

Trump è il presidente. Now Encrypt Your Email" (Ora crittografa la tua email), ha esortato Max Read, redattore di tecnologia della rivista di New York, in un articolo pubblicato sul New York Times a marzo. “Nelle settimane successive alla vittoria delle elezioni di Donald J. Trump, uno scisma minacciò di spezzare in due il mio gruppo di amici. Non un argomento politico portato dal presidente eletto, o una lotta filosofica sul futuro del paese, ma una domanda su quale app dovremmo usare per chattare. . . ." Buzzfeed concorda: "Ecco come proteggere la tua privacy nell'America di Trump: consigli facili per proteggerti

dall'espansione della sorveglianza del governo", ha scritto il punto vendita, offrendo ai suoi lettori millenari una guida all'elenco per "diventare oscuri" in rete.

Quali erano queste app? Chi le ha fatte? Funzionavano davvero? È qui che la storia è diventata ancora più strana.

**Segreti e bugie**

Gli incontri involontari di Durov con l'FBI portano a casa uno spiacevole fatto della vita nell'economia dei big data: l'odierno movimento per la privacy ossessionato dalle app si basa quasi interamente su strumenti crittografici che sono stati covati e finanziati dall'apparato di politica estera americana, un corpo di agenzie e organizzazioni che sono venute da un vecchio progetto di propaganda della Guerra Fredda gestito dalla CIA.

Nel 1948, la CIA ricevette un assegno in bianco per intraprendere un programma di "operazioni segrete" a tutto campo per contenere e ridurre la diffusione del comunismo, a cominciare dall'Unione Sovietica e dall'Europa orientale. La propaganda radiofonica è stata uno strumento centrale in questa guerra di idee segreta e la CIA ha utilizzato gruppi di facciata privati per gestire stazioni con nomi come "Radio Liberation from Bolshevism" e "Radio Free Europe". Negli anni '50 e '60, l'agenzia ha ampliato la sua rete radiofonica per includere operazioni contro forze comuniste, di sinistra e altrimenti sospettosamente riformiste che avrebbero potuto diffondere il terrore bacillo del bolscevismo attraverso l'Asia e l'America Latina.

L'idea era di impedire a questi Stati di esercitare il controllo sovrano sul loro spazio informativo, nonché di dominare e influenzare le idee delle persone in un modo che fosse in linea con gli interessi americani. Per quanto riguardava la CIA, questa operazione di propaganda sub rosa era una bellezza, e l'agenzia si vanta ancora con orgoglio che rimane uno dei progetti di guerra psicologica segreta di maggior successo mai gestiti dagli Stati Uniti.

Alla fine, l'operazione di propaganda multi-tentacolare della CIA ha perso il suo status segreto ed è stata trasformata dal Congresso nel Broadcasting Board of Governors, un'agenzia federale sorella del Dipartimento di Stato. Con un budget di quasi un miliardo di dollari, oggi la BBG gestisce il tentacolare nesso di propaganda straniera dell'America. Il pubblico americano è solo vagamente consapevole dell'esistenza della BBG, ma questo impero dei media non lascia quasi nessun angolo del mondo non toccato dalle trasmissioni satellitari, televisive e radiofoniche. E proprio come avveniva quasi settant'anni fa sotto la CIA, la missione della BBG è perpetrare sistematicamente la stessa cosa che lo stimato establishment politico americano sta attualmente accusando la Russia di fare: sponsorizzare notizie - alcune delle quali oggettive, altre selvaggiamente distorte. — Come parte di una più ampia campagna per proiettare il potere geopolitico.

Ma c'era di più. Quando Internet si è diffuso in tutto il mondo, è diventato un potente mezzo di influenza e il governo degli Stati Uniti si è mosso spietatamente per sfruttare il suo vantaggio competitivo contro i rivali sotto la bandiera di "Internet Freedom". La politica, messa in atto dal Segretario di Stato Hillary Clinton, riguardava più che la semplice

trasmissione di notizie. Il suo scopo era quello di armare questa tecnologia di comunicazione globale in tutti i modi creativi per indebolire i rivali, rovesciare governi ostili e sostenere i movimenti di opposizione dalla Cina alla Russia, Iran, Siria e Libia. "L'amministrazione Obama sta conducendo uno sforzo globale per distribuire Internet 'ombra' e sistemi di telefonia mobile che i dissidenti possono utilizzare per minare i governi repressivi che cercano di zittirli censurando o chiudendo le reti di telecomunicazioni", ha riferito il New York Times nel 2011, quando il programma per la libertà di Internet è iniziato in modo importante.

Lo sforzo include progetti segreti per creare reti di cellulari indipendenti all'interno di Paesi stranieri, nonché un'operazione da un romanzo di spionaggio in un negozio al quinto piano di L Street a Washington, dove un gruppo di giovani imprenditori che sembrano una banda di garage sta inserendo hardware apparentemente innocente in un prototipo di "Internet in una valigia". . . La valigia potrebbe essere nascosta attraverso un confine e configurata rapidamente per consentire la comunicazione wireless su una vasta area con un collegamento a Internet globale.

Questo era solo l'inizio. Negli anni successivi, la BBG, sostenuta dal Dipartimento di Stato, ha ampliato l'iniziativa Internet Freedom in un programma da 50 milioni di dollari all'anno che finanzia centinaia di progetti rivolti a paesi in tutto il mondo: Cina, Cuba, Vietnam e Russia. E qui le cose, ancora una volta, hanno preso una svolta per il surreale: l'apparato per la libertà di Internet è stato progettato per proiettare il potere all'estero, ma è emerso anche come il motore principale e l'agitatore nel movimento per la privacy interno americano. Ha finanziato attivisti e ricercatori sulla privacy, ha lavorato con EFF e ACLU e persino aziende come Google. Ovunque guardassi, gli strumenti per la privacy finanziati da questa agenzia hanno dominato la scena. Ciò includeva i prodotti per la privacy più ardentemente promossi ora in offerta: Tor, la piattaforma di navigazione Internet anonima che alimenta quello che è noto come il "dark web" e Signal, l'app di chat sostenuta da Edward Snowden. Entrambi hanno raccolto milioni di soldi dal governo per restare a galla.

**Da un Sussurro a un Urlo**

Quando a Pavel Durov gli fu portato via per la prima volta VKontakte dal Cremlino e fuggì dalla Russia, fu salutato in Occidente come un eroe, un moderno Sakharov che ha combattuto per la libertà e ha pagato il prezzo con i suoi affari. Anche la comunità americana di criptovalute e privacy lo ha abbracciato. Ma non ci volle molto perché la relazione si inasprisse e il colpevole principale era Signal, un'app per telefoni cellulari crittografata creata da una piccola azienda opaca chiamata Open Whisper Systems, alias Quiet Riddle Ventures LLC.

Inventato da un sedicente crittografo radicale che si chiama Moxie Marlinspike (sebbene il suo vero nome possa essere o meno Matthew Rosenfeld o Mike Benham), Signal è stato portato alla vita con i finanziamenti dell'Open Technology Fund supportato da BBG (che ha pompato quasi 3 milioni di dollari dal 2013) e sembra fare affidamento sui continui finanziamenti governativi per la sopravvivenza. Nonostante gli stretti legami del servizio con un'organizzazione scorporata dalla CIA, le luci principali della privacy e della comunità

crittografica americana sostengono l'app. "Uso Signal ogni giorno. #notesforFBI, "Snowden ha twittato a legioni di follower che sono usciti e hanno scaricato l'app in massa. Marlinspike ha sfruttato al massimo l'elogio di Snowden, mettendo in evidenza l'approvazione del leaker sul sito web della sua azienda: "Usa qualsiasi cosa di Open Whisper Systems".

In gran parte grazie all'approvazione e al supporto di Snowden, Signal è diventata l'app di chat crittografata preferita tra giornalisti, organizzatori politici e attivisti americani, dagli anarchici ai marxisti a Black Lives Matter. In questi giorni, è anche l'app di pianificazione sicura di prima scelta per i raduni dell'opposizione che prendono di mira Trump. L'app ha persino fatto grandi passi nella Silicon Valley, con Marlinspike che lavora con il management di Facebook e Google per convincerli ad adottare l'architettura di crittografia dell'app di chat nei loro programmi di chat mobile, incluso WhatsApp. Non sorprende che l'adozione di Signal da parte di Facebook nel suo programma WhatsApp abbia ottenuto consensi da BBG; i manager del negozio di propaganda si vantavano che gli strumenti per la privacy finanziati dal governo sarebbero stati ora utilizzati da un miliardo di persone.

Nonostante i continui legami di Open Whisper con il governo degli Stati Uniti, i massimi esponenti della privacy e della comunità crittografica americana hanno iniziato a mettere in guardia le persone dall'usare qualsiasi altra cosa. Ciò include Telegram, che utilizza una tecnica crittografica personalizzata progettata dal fratello di Pavel Durov, Nikolai, un matematico. Persino Snowden si è preso la responsabilità di allontanare le persone da Telegram, consigliando attivisti politici, giornalisti, dissidenti, informatori - in breve, tutti - di utilizzare Signal o addirittura WhatsApp di Facebook. "Per impostazione predefinita, è meno sicuro di @WhatsApp, il che lo rende pericoloso per i non esperti", ha twittato in risposta a una domanda di un sostenitore curioso di Telegram.

Ma per un'app progettata per nascondere le persone agli occhi indiscreti del governo degli Stati Uniti, l'architettura di Signal ha messo in pausa alcuni esperti di sicurezza e crittografia. Il suo algoritmo di crittografia dovrebbe essere impeccabile, ma il back-end dell'app funziona come un servizio cloud su Amazon, che è a sua volta un importante appaltatore della CIA. Il programma richiede inoltre che gli utenti colleghino l'app a un numero di cellulare reale e diano accesso all'intera rubrica: uno strano comportamento per un'app che dovrebbe nascondere le identità delle persone. Signal dipende anche da Google e Apple per la fornitura e l'installazione dell'app sul telefono delle persone, ed entrambe le società sono partner di sorveglianza della NSA. "Di solito Google ha accesso root al telefono, c'è il problema dell'integrità. Google sta ancora collaborando con la NSA e altre agenzie di intelligence ", ha scritto Sander Venema, uno sviluppatore che forma giornalisti sulla sicurezza. "Sono abbastanza sicuro che Google potrebbe fornire un aggiornamento o una versione appositamente modificata di Signal a obiettivi specifici per la sorveglianza e non sarebbero più saggi se installassero malware sui loro telefoni". E dato il marketing ristretto di Signal per attivisti politici e giornalisti, l'app funziona come una bandiera: potrebbe crittografare i messaggi, ma tagga anche gli utenti come persone con qualcosa da nascondere, un grande e grosso cartello che dice: "GUARDAMI, PER FAVORE".

E comunque, Signal o no Signal, se il tuo nemico era il governo degli Stati Uniti, non importava davvero quale app di crittografia hai usato. Un recente dump di documenti sugli

strumenti di hacking della CIA pubblicati da WikiLeaks ha rivelato che il Mobile Devices Branch dell'agenzia ha sviluppato ogni sorta di gadget per acquisire i dati del telefono, anche quando è messo in quarantena dai firewall di app come Signal e WhatsApp o persino Telegram. "Queste tecniche consentono alla CIA di aggirare la crittografia di WhatsApp, Signal, Telegram, Wiebo, Confide e Cloackman hackerando i telefoni" intelligenti "su cui girano e raccogliendo il traffico di messaggi e audio prima dell'applicazione della crittografia", ha scritto WikiLeaks.

Durov ha ammesso che la crittografia ha i suoi limiti. Tuttavia, mentre raccontava come Snowden avesse parlato a voce bassa di Telegram, Durov era frustrato e sconcertato. Dice che lui e suo fratello erano molto cauti nello scegliere tecniche di crittografia promosse da esperti americani, in particolare da quando i documenti della NSA trapelati da Snowden hanno rivelato che la NSA ha segretamente pagato RSA, un'influente azienda di sicurezza informatica, per utilizzare una tecnica imperfetta che la NSA sapeva come decifrare. I fratelli Durov si chiedevano se la stessa cosa potesse accadere ora con altri popolari algoritmi di crittografia. Sono diventati ancora più preoccupati quando Telegram ha iniziato a attirare attacchi pubblici ai social media da parte di esperti di crittografia americani. "Hanno basato le loro critiche sul nostro approccio non su una reale debolezza, ma esclusivamente sul fatto che non abbiamo utilizzato gli algoritmi che stavano promuovendo", ha detto. "Dal momento che non sono riusciti a impegnarsi in alcuna conversazione significativa sulla crittografia, abbiamo iniziato a renderci conto che c'era un altro programma che stavano spingendo piuttosto che trovare la verità o massimizzare la sicurezza".

Ma gli attacchi sono continuati. Non solo Snowden ei suoi alleati crittografici stavano dicendo alle persone di fidarsi di Facebook, una società che opera sotto sorveglianza e collabora con la NSA; stavano anche promuovendo un'app finanziata attivamente dall'ala politica estera dello stato di sicurezza nazionale degli Stati Uniti. Semplicemente non aveva alcun senso.

Durov era sbalordito. Mentre eravamo seduti a parlare, mi ha detto che non riusciva a capire come le persone potessero fidarsi di un'arma presumibilmente anti-governativa che era stata finanziata dallo stesso governo degli Stati Uniti da cui avrebbe dovuto proteggere i suoi utenti.

Siamo entrati in un mondo da incubo della paranoica teoria dei giochi.

Gli ho detto che condividevo il suo sconcerto. In tutti i miei rapporti su questo gruppo di cripto-radicali finanziati da uno spinoff della CIA, ho posto una semplice domanda a cui nessuno poteva rispondere adeguatamente: se app come Signal rappresentassero davvero una minaccia al potere di sorveglianza della NSA, perché il governo degli Stati Uniti continuerebbe a finanziare loro? Non ho potuto fare a meno di pensare a come questo allineamento tra governo e potere aziendale sarebbe stato accolto dall'establishment tecnologico e dai media negli Stati Uniti se qualcosa di simile fosse accaduto nell'ex Unione Sovietica: immagina se il KGB avesse finanziato uno speciale crypto fax e disse ad Aleksandr Solzhenitsyn e agli scrittori dissidenti di samizdat di usarlo, promettendo che era totalmente al riparo dagli agenti del KGB. Quindi immagina che Solzenicyn non solo

crederebbe al KGB, ma direbbe a tutti i suoi amici dissidenti di usarlo: "È totalmente sicuro". Gli sforzi del KGB sarebbero stati ridicolizzati senza pietà nell'Occidente capitalista, mentre Solzenicyn sarebbe stato etichettato come un collaboratore nel peggiore dei casi, o un fantoccio nel migliore dei casi. Per quanto ridicola sia questa fusione di interessi tecnologici e statali sotto la rubrica della dissidenza, in America questo piano può in qualche modo volare.

Mentre esponevo questa analogia, Durov annuì d'accordo. "Non credo sia una coincidenza che entrambi comprendiamo quanto sia ingenuo questo tipo di pensiero e che entrambi siamo nati in Unione Sovietica".

**Fidarsi della Forza**

L'accordo politico non era esattamente quello che mi aspettavo quando mi sono preparato per incontrare Pavel Durov. Da quello che avevo letto sulla stampa, la nostra politica e la nostra visione del mondo non potevano essere più lontane. Era un libertario, un ragazzo che lanciava banconote da 5.000 rubli ai pedoni solo per vederli arrampicarsi e combattere per raccoglierli, qualcuno che ha twittato che Hitler e Stalin non erano diversi il giorno in cui la gente in tutta l'ex Unione Sovietica ha celebrato la loro vittoria sulla Germania nazista.

Tuttavia, a livello personale, era simpatico e persino umile. Per qualcuno nel mondo delle criptovalute, era anche inaspettatamente realistico sui limiti della crittografia, non mostrando nessuna delle credenze simili a un culto nella tecnologia che si vede nel movimento per la privacy americano. Ma c'era anche qualcos'altro: era un combattente.

Inizia con il semplice fatto che stava pubblicamente facendo coming out per dettagliare il tentativo dell'FBI di corrompere la sua squadra e fare pressioni su Telegram affinché lavorasse segretamente con l'agenzia - nonostante le dichiarazioni di non responsabilità di Durov e gli sforzi per minimizzare la rivelazione, è stato un grosso problema. Nonostante sia stato cacciato dalla Russia, non si è unito all'apparato di sicurezza degli Stati Uniti, ma ha scelto invece di combattere una guerra su due fronti. È stata una mossa insolita e impressionante. La maggior parte delle persone che si scontrano con la politica in Russia e si trovano a cercare sicurezza in Occidente poiché i dissidenti moderni di solito si allineano con gli obiettivi di propaganda dell'Occidente, schierandosi acriticamente con gli interessi e i giocatori americani, non importa quanto sgradevoli. Pensa a Pussy Riot che fugge dalla Russia e critica Vladimir Putin, mentre fa servizi fotografici con il segretario di Stato Hillary Clinton.

Per quanto riguarda la sua crittografia, beh, non c'è alcuna garanzia che Telegram si dimostrerà più sicuro dei suoi rivali della Silicon Valley. D'altra parte, non c'è modo che la ricerca della privacy online finanziata dalle spie e guidata dal profitto dell'Occidente possa produrre una qualsiasi ragionevole approssimazione della cosa reale.

Nel nostro mondo post Snowden, abbiamo esternalizzato la nostra politica sulla privacy alle app crittografiche. In questo modo, siamo entrati in un mondo da incubo della teoria dei giochi paranoica, un luogo in cui le persone normali non hanno un vero potere e devono riporre la loro fiducia nelle persone e nelle organizzazioni che alimentano gli algoritmi che

rendono questa tecnologia crittografica. Alla fine, tutto si riduce alla fiducia. Ma ci si può davvero fidare di qualcuno di queste persone e organizzazioni? Il giovane magnate russo sui pattini con il Cremlino? L'ex spia americana in fuga e si nasconde in Russia? Boutique di app crittografiche finanziate dall'ala del cambio di regime del Dipartimento di Stato? Google e Facebook, che collaborano con la NSA?

Confuso? Non sai di chi fidarti? Bene, questo è lo stato del nostro movimento per la privacy oggi.

*di Yasha Levine - Settembre 2017*

*Yasha Levine è una giornalista investigativa ed ex redattore del quotidiano The eXile con sede a Mosca . È l'autrice di Surveillance Valley: The Secret Military History of the Internet dove di scopre che: Internet è stato costruito dal governo per spiare i cittadini, in patria e all'estero.*

In *Surveillance Valley* (pdf in inglese), Yasha Levine ripercorre la storia di Internet fino ai suoi inizi come strumento dell'era del Vietnam per spiare i guerriglieri e i manifestanti contro la guerra, un progetto di rete informatica militare che alla fine prevedeva la creazione di un sistema globale di sorveglianza e previsione. Levine mostra come gli stessi obiettivi militari che hanno guidato lo sviluppo della prima tecnologia Internet siano ancora oggi al centro della Silicon Valley. Spie, campagne di controinsurrezione, imprenditori hippie, app sulla privacy finanziate dalla CIA. Dagli anni '60 agli anni 2010: questa storia rivelatrice e travolgente ti farà riconsiderare ciò che sai sullo strumento più potente e onnipresente mai creato.

RI

***https://t.me/realeinformazione***