

FUGA DA WHATSAPP

di Lucina Paternesi e Alessia Marzi

collaborazione di Alessandra Borella

immagini di Alfredo Farina, Alessandro Spinnato e Tommaso Javidi

grafica di Giorgio Vallati

montaggio di Lorenzo Sellari

LUCINA PATERNESI FUORICAMPO

Il primo pensiero del mattino, l'ultimo della giornata: trascorriamo online lo stesso tempo che dedichiamo al sonno, una media di 7 ore. Non solo i social. Nell'era della pandemia tutte le nostre comunicazioni si sono spostate qui, sempre a portata di mano ma sempre più difficili da custodire. E il nostro telefono si è trasformato in un'arma: come durante una guerra le nostre conversazioni vengono cifrate, cioè decifrabili solo da chi ne conosce il codice. Dai tempi in cui criptare messaggi era un crimine, oggi tutte le app che usiamo per inviare messaggi garantiscono comunicazioni riservate. I nostri messaggi privati sono al sicuro, ma lo siamo anche noi?

SIGFRIDO RANUCCI IN STUDIO

Bentornati. Signal, Telegram, WhatsApp, le app di messaggistica. Solo da WhatsApp inviamo ogni giorno un centinaio di miliardi di sms. Solo che qualche mese fa WhatsApp ha informato i propri utenti che sarebbero mutate le condizioni di servizio, ha diramato un'informativa che ha creato letteralmente il panico. C'è stata una migrazione sulle altre app, ne hanno beneficiato Signal e Telegram, gli utenti sono andati alla ricerca dell'app più sicura, ma qual è l'app più sicura? La nostra Lucina Paternesi ha cercato di capirlo intanto con un'intervista esclusiva a lui, a mister Signal.

LUCINA PATERNESI FUORICAMPO

Chilometri di spiagge e palme, dove la cultura latina incontra quella a stelle e strisce, Venice Beach, la spiaggia più alternativa di Los Angeles, è diventata la patria della controcultura high tech americana.

La rivoluzione di Signal nel mondo della comunicazione via chat ha avuto inizio proprio qui. Vicino eppure mai così lontano dai paradigmi della Silicon Valley. È l'anti-WhatsApp per eccellenza. E dietro Signal c'è lui. Nome in codice Moxie Marlinspike, crittografo, hacker etico, marinaio. Da sempre lontano dalle telecamere, sembra più un personaggio mitologico che il capo di un'applicazione da milioni di utenti.

MOXIE MARLINSPIKE - CEO DI SIGNAL

Quando le persone condividono qualcosa con i propri amici, noi vogliamo che le condividano veramente solo con gli amici. Non con un mucchio di inserzionisti, con hacker stranieri o con i governi. Cerchiamo di riportare un po' di normalità su internet.

LUCINA PATERNESI

E qual è il vostro modello di business?

MOXIE MARLINSPIKE - CEO DI SIGNAL

Qui a Signal abbiamo un grande vantaggio, non ci sono investitori a cui dobbiamo dire grazie e, beh lo sai, non abbiamo pubblicità. La tecnologia che abbiamo costruito fa esattamente ciò che dice di fare

LUCINA PATERNESI FUORICAMPO

Grande amico di Edward Snowden, Moxie è stato a capo della sicurezza di Twitter e creatore del protocollo di crittografia end-to-end TextSecure, poi implementato dentro

Whatsapp. Ma quando ormai WhatsApp era stata acquistata da Zuckerber, uno dei fondatori, Brian Acton, abbandona Facebook per disaccordi sulle politiche aziendali sulla privacy e mette sul piatto 50 milioni di dollari a tasso zero. Nasce così la Signal Foundation.

MOXIE MARLINSPIKE - CEO DI SIGNAL

Siamo una fondazione no-profit che si sostiene grazie alle donazioni di chi decide di usare l'app o il nostro protocollo. Non possiamo vendere Signal per guadagnare soldi.

LUCINA PATERNESI FUORICAMPO DOC. IN GRAFICA

Da strumento di nicchia a fenomeno sempre più di massa. Fino a diventare il principale strumento di comunicazione nelle proteste del movimento Black Lives Matter, Eppure, con una certa frequenza, a Signal arrivano richieste di consegna dei dati degli utenti da parte delle autorità giudiziarie.

MOXIE MARLINSPIKE - CEO DI SIGNAL

Ogni volta che riceviamo richieste per indagini in corso le pubblichiamo sul nostro sito. I dati che ci vengono richiesti, come username, indirizzo collegato al numero di telefono, la localizzazione, sono informazioni che società come Google hanno. Noi invece conserviamo solo la data di creazione dell'account e l'ultimo accesso.

LUCINA PATERNESI FUORICAMPO

Durante le proteste della comunità afroamericana, Signal ha rilasciato un aggiornamento che prevede la possibilità di oscurare i volti quando si condividono fotografie, così da aggirare eventuali tentativi di individuazione dei manifestanti da parte delle forze dell'ordine.

MOXIE MARLINSPIKE - CEO DI SIGNAL

Negli ultimi anni, siamo stati costantemente tracciati, spiati, seguiti. È per questo motivo che in Gran Bretagna stiamo anche testando i pagamenti online. Vogliamo creare un ecosistema in cui l'utente si può sentire libero di condividere, scrivere e acquistare senza sapere che tutto ciò gli si ritorcerà contro.

LUCINA PATERNESI FUORICAMPO

L'aria è cambiata perché gli utenti hanno aumentato la consapevolezza di quanto sia fragile la propria privacy. Non è un caso che a due passi dalla Silicon Valley, a San Francisco, sia nato un movimento d'opinione che ha portato all'approvazione di una legge di iniziativa popolare sulla privacy del tutto simile al nostro regolamento europeo.

RICHARD ARNEY - CO-AUTORE CALIFORNIA PRIVACY RIGHTS ACT 2020

La nostra campagna ha preso le mosse proprio grazie al coinvolgimento dei lavoratori della Silicon Valley. Sono loro i primi ad essere spaventati dall'enorme abuso di informazioni.

LUCINA PATERNESI FUORICAMPO

Per provare a frenare la raccolta indiscriminata e l'abuso di dati ci sono voluti anni. E soprattutto ci sono voluti i soldi dei più ricchi tra gli uomini d'affari e investitori del pianeta. Che vivono proprio qui, nella baia di San Francisco. E che si sono spesi per una campagna di comunicazione senza precedenti, come l'ex manager del fondo BlackRock Richard Arney.

RICHARD ARNEY - CO-AUTORE CALIFORNIA PRIVACY RIGHTS ACT 2020

Anche la polizia californiana ha supportato la nostra proposta, è bastato mostrare l'elenco con i nomi e gli indirizzi personali di ogni singolo poliziotto, disponibili online a

pagamento. Online si trovavano anche i nomi di chi è in riabilitazione dalla droga e gli elenchi di chi vuole abortire. Per non parlare poi dei furti di dati.

LUCINA PATERNESI FUORICAMPO

L'ultimo, solo in ordine temporale, ha fatto finire online i dati sensibili, come nome e numero di telefono, di mezzo miliardo di utenti di Facebook, che avevano inserito il cellulare al momento dell'iscrizione come fattore di verifica in caso di smarrimento della password. Gli elenchi sono circolati nel dark web per mesi, disponibili a pagamento. Ma qualche settimana fa sono stati resi pubblici, in chiaro, anche quelli di oltre 35 milioni di italiani

SIGFRIDO RANUCCI IN STUDIO

Anche lavoratori della Silicon Valley hanno preso consapevolezza del mostro che hanno contribuito a creare, ma solo quando sono diventati loro stessi delle vittime. Ora è considerata un'app sicura Signal, è rassicurante perché? Perché non raccoglie dati, non geolocalizza e perché mantiene criptati i messaggi anche quando sono in pancia al telefonino. Ed è proprio l'inventore di Signal, mister Moxie Marlinspike, che è l'inventore del protocollo TextSecure che consente l'invio di un messaggio da un dispositivo all'altro criptografato e consente l'impossibilità ad un terzo di intercettare il messaggio, di vedere in chiaro i contenuti. Ecco e adesso su Signal girano cento milioni di utenti ma la maggior parte sono arrivati dopo che a marzo scorso era stata diramata da WhatsApp un'informativa che informava, appunto, i propri utenti, di un possibile abbinamento tra le utenze business, quelle di Facebook. Ora, solo l'idea di essere abbinati, di un'interazione tra le app di Zuckerberg ha fatto scappare molti utenti, cercando delle app più sicure, ma quanto sono più sicure Telegram e Signal?

LUCINA PATERNESI FUORICAMPO

L'effetto di un'informativa poco chiara è stato come un boomerang per WhatsApp. E sono tanti gli utenti che hanno deciso di scaricare nuove applicazioni. A guadagnarci di più sono state Telegram e Signal. L'applicazione russa dei fratelli Durov a metà gennaio dichiarava il sorpasso dei 500 milioni di utenti attivi. Anche l'applicazione di messaggistica supportata da Edward Snowden ha visto schizzare il numero di download in poche ore.

LUCINA PATERNESI

Professore qual è l'app di messaggistica più sicura?

STEFANO ZANERO - PROFESSORE ASSOCIATO INGEGNERIA ELETTRONICA POLIMI

La caratteristica principale in cui le applicazioni differiscono è quella che viene chiamata crittografia end-to-end, protegge un messaggio da un dispositivo all'altro dispositivo, escludendo tutto quello che c'è di mezzo. Chiamiamola E, Whatsapp e Signal applicano la crittografia end-to-end su tutte le comunicazioni. Telegram e Messenger di Facebook la applicano solo dove viene richiesta e nel caso specifico di Telegram non è applicata sui canali.

LUCINA PATERNESI FUORICAMPO

Nata in ambito militare, la crittografia oggi dovrebbe proteggere tutte le nostre comunicazioni, foto e video che inviamo. Ma quando inviamo un messaggio a un altro dispositivo, può essere intercettato da terzi?

Consulente delle procure italiane nel campo delle acquisizioni digitali, Stefano Fratepietro ha associato un tablet a un'antenna wifi.

STEFANO FRATEPIETRO - TESLA CONSULTING

La particolarità di questa rete wireless è che in questo momento la sto intercettando. Iniziamo con Telegram. Ciao, come stai... Inviato. La trasmissione avviene all'interno di questo tunnel non leggibile, ma il messaggio è in chiaro. Se invece crei una chat privata anche lo stesso messaggio viene cifrato.

LUCINA PATERNESI

La famosa chat segreta di Telegram.

STEFANO FRATEPIETRO - TESLA CONSULTING

La famosa chat segreta di Telegram, esatto.

LUCINA PATERNESI

Chiunque è in mezzo?

STEFANO FRATEPIETRO - TESLA CONSULTING

Non potrà mai leggere quello che ci siamo scambiati.

LUCINA PATERNESI FUORICAMPO

Questa combinazione di cifre, numeri e simboli è il primo livello di crittografia sulla rete. In questo modo il testo di un messaggio sarà comprensibile solo sul dispositivo del mittente e del destinatario. Un'altra combinazione di caratteri mostra sullo schermo cosa accade quando mandiamo un messaggio su WhatsApp.

LUCINA PATERNESI

E la cifratura riguarda anche foto e video e anche le comunicazioni che avvengono nei gruppi.

STEFANO FRATEPIETRO - TESLA CONSULTING

Esattamente, qualsiasi contenuto inviato via messaggio. Adesso facciamo la stessa cosa utilizzando l'applicazione Signal. "Ciao", inviato.

STEFANO FRATEPIETRO - TESLA CONSULTING

Anche in questo caso, canale e dati cifrati, e solo quando viene ricevuto il messaggio dallo smartphone viene decifrato.

LUCINA PATERNESI FUORICAMPO

Ma la crittografia non serve quando ci infettano il cellulare o quando un dispositivo finisce nelle mani sbagliate. Grazie ad alcuni software che si trovano sul mercato è possibile acquisire tutto ciò che è nel database di uno smartphone e copiarlo.

STEFANO FRATEPIETRO - TESLA CONSULTING

I messaggi vengono salvati in chiaro all'interno di un database del dispositivo, pertanto chi acquisisce quella memoria di quel dispositivo può andare a leggere quello che ci siamo scritti. Ad eccezione di Signal.

LUCINA PATERNESI FUORICAMPO

Sfruttando le vulnerabilità insite in queste applicazioni di messaggistica, spiare le nostre comunicazioni è semplicissimo.

STEFANO FRATEPIETRO - TESLA CONSULTING

Ci sono svariati software che vengono utilizzati anche dalle forze dell'ordine, noi oggi usiamo Ufed di Cellebrite, che è un'azienda israeliana, una delle leader mondiale su questa tecnologia. Andremo a farci una copia speculare di quello che c'è sul tablet.

LUCINA PATERNESI

Quanto costa un software così?

STEFANO FRATEPIETRO - TESLA CONSULTING

Dagli 8mila dollari in su, più rinnovi annuali a canone che si aggirano intorno ai 4 mila, 5 mila dollari.

LUCINA PATERNESI

Lo possono acquistare tutti?

STEFANO FRATEPIETRO - TESLA CONSULTING

Tutti quelli che hanno una partita Iva.

LUCINA PATERNESI

Che cosa si vede?

STEFANO FRATEPIETRO - TESLA CONSULTING

Per quanto concerne la parte di WhatsApp e Telegram tutto quello che è stato ricevuto.

LUCINA PATERNESI

Foto video, messaggi vocali.

STEFANO FRATEPIETRO - TESLA CONSULTING

Tutto, come se stessi leggendo il tuo smartphone in quel momento. Non c'è Signal.

LUCINA PATERNESI

Perché se tutti e tre utilizzano la crittografia end-to-end solo Signal ci tiene al riparo?

STEFANO FRATEPIETRO - TESLA CONSULTING

Perché Signal è l'unica che applica la cifratura anche sul database.

SIGFRIDO RANUCCI IN STUDIO

Insomma WhatsApp e Signal applicano la messaggistica crittografata end to end, significa che quando inviano un messaggio da un dispositivo all'altro questo è coperto e c'è l'impossibilità da parte di un terzo di intercettarlo: vedrebbe non i contenuti, ma solo dei numeri. Mentre invece Telegram lo può applicare questo meccanismo esclusivamente se si opta per la cosiddetta chat segreta. Poi invece che cosa accade, che se invece un telefonino viene infiltrato da un software sofisticato come quello israeliano di cui abbiamo parlato, anche i messaggi inviati con la crittografia possono essere intercettati, letti, perché vengono letti e copiati da questo software. Resiste ancora Signal, che però è costretto a capitolare in presenza di trojan o spyware molto sofisticati che sono quelli che sostanzialmente fanno lo screenshot secondo per secondo dell'immagine del nostro telefonino, dello schermo del nostro telefonino oppure studiano i movimenti della tastiera. Ma quali informazioni hanno su di noi i padroni della messaggistica? Vediamo cosa ha in possesso Durov, che è il patron di Telegram, l'inventore, è scappato dalla Russia per evitare intrusioni di Putin, si è rifugiato a Dubai. Ma è riuscito a evitare Putin? Ha 500 milioni di utenti.

LUCINA PATERNESI FUORICAMPO

Per ogni chat che avviamo WhatsApp raccoglie una miriade di dati, l'ID del device e dell'user, dati pubblicitari, cronologia degli acquisti, posizione approssimativa, indirizzo email, numero di telefono, dati diagnostici e informazioni di pagamento. Facebook anche informazioni sulle ricerche, foto o video, salute e fitness.

STEFANO ZANERO - PROFESSORE ASSOCIATO INGEGNERIA ELETTRONICA POLIMI

I dati principali sono fondamentalmente due, il contenuto della comunicazione e il fatto che c'è stata la comunicazione, noi informatici lo chiamiamo il metadato. Ora, WhatsApp sappiamo che li raccoglie, ce lo dice, era scritto anche nella famosa informativa maldestra. Nel caso di Messenger ci sono sicuramente i metadati e sicuramente anche i messaggi che ci scambiamo e questo di nuovo non è una sorpresa fa parte del modello di Facebook.

LUCINA PATERNESI FUORICAMPO

L'unico dato personale che Signal conserva è il numero di telefono, che non viene mai associato all'identità dell'utente.

STEFANO ZANERO - PROFESSORE ASSOCIATO INGEGNERIA ELETTRONICA POLIMI

Signal non è un'azienda, quindi so che non ha nessun utilizzo per quei metadati.

LUCINA PATERNESI FUORICAMPO

Telegram invece raccoglie dati minimi come informazioni di contatto e user ID, ma che cosa ci fa?

STEFANO ZANERO - PROFESSORE ASSOCIATO INGEGNERIA ELETTRONICA POLIMI

Telegram mi dice: "il nostro modello di business non è la pubblicità", ma me lo dice Telegram.

LUCINA PATERNESI

Come mai se non è più sicuro, tutti si sono riversati su Telegram?

STEFANO ZANERO - PROFESSORE ASSOCIATO INGEGNERIA ELETTRONICA POLIMI

Il fatto di non essere Facebook, dal punto di vista del rispetto della privacy o del trattamento dei dati

STEFANO ZANERO - PROFESSORE ASSOCIATO INGEGNERIA ELETTRONICA POLIMI

È diventato un vantaggio.

STEFANO ZANERO - PROFESSORE ASSOCIATO INGEGNERIA ELETTRONICA POLIMI

Certamente.

LUCINA PATERNESI FUORICAMPO

Ma chi c'è dietro l'applicazione Telegram?

KAREN KAZARYAN - ANALISTA ASSOCIAZIONE RUSSA PER LE COMUNICAZIONI ELETTRONICHE

Pavel Durov è Telegram e senza di lui Telegram non esisterebbe.

LUCINA PATERNESI FUORICAMPO

Filosofo, ribelle, imprenditore milionario, Pavel Durov si batte per la libertà nonostante il pugno duro del Cremlino. Una via di mezzo tra Mark Zuckerberg e Edward Snowden. In un Paese che da anni sta intensificando la sua campagna di controllo su internet.

MICHAEL TRETYAK - AVVOCATO DIGITAL RIGHTS CENTER

C'è una proposta di legge che impone a ogni azienda con più di 500mila visitatori online di aprire un ufficio di rappresentanza a Mosca e trasferire tutti i dati in server localizzati in Russia.

ANDREI SOLDATOV - GIORNALISTA AGENTURA.RU

Ogni azienda di telecomunicazioni che si vuole insediare qui, per legge, deve fornire una "back-door" ai servizi di sicurezza russi. Ti serve per ottenere la licenza.

LUCINA PATERNESI FUORICAMPO

Ad appena vent'anni Pavel Durov ha creato il primo social network russo, V-Kontakte, molto più diffuso di Facebook. Già nel 2011, durante la più grande protesta mai vista dopo la dissoluzione dell'Urss, Durov mostra i muscoli contro il governo.

ANDREI SOLDATOV - GIORNALISTA AGENTURA.RU

I servizi di sicurezza gli intimarono di chiudere alcuni gruppi di protesta su V-Kontakte. Durov non solo rifiuta, ma pubblica anche lo scambio con cui l'FSB aveva cercato di estorcergli alcune informazioni. Anche durante gli scontri di piazza Maidan a Kiev, decide di non rivelare informazioni personali sugli attivisti.

LUCINA PATERNESI FUORICAMPO

Le continue ingerenze da parte di uomini vicini a Putin lo costringono ad abbandonare la sua creatura. Pavel Durov rassegna le dimissioni, abbandona la Russia e V-Kontakte finisce in mano al magnate russo Usmanov, proprietario della holding di Gazprom che al tempo controllava direttamente il gruppo Mail.ru. Nasce così Telegram.

ANDREI SOLDATOV - GIORNALISTA AGENTURA.RU

Telegram nasce con la promessa di non condividere le informazioni non solo con i servizi segreti russi, ma con quelli di qualsiasi altro Paese, e di essere uno strumento sicuro, protetto, impenetrabile.

MATTEO FLORA - COFONDATORE CENTRO HERMES PER LA TRASPARENZA E DIRITTI DIGITALI

La fortuna di Telegram sta nel fatto che le persone pensano di essere anonime e garantite, che è molto diverso dall'essere anonimi e garantiti. L'anonimato è dato dalla non volontà di consegnare alle autorità i dati degli utenti.

LUCINA PATERNESI FUORICAMPO

Appena qualche mese fa, quando in Italia i vaccini erano un miraggio, proprio su Telegram sono apparsi alcuni canali dedicati al mercato nero delle fiale. Ci scrivono dalla Turchia e ci promettono di farci arrivare in 24 ore fiale di Pfizer, Moderna, Astrazeneca persino il Remdesivir. I prezzi variano da 85 a 130 dollari a fiala.

MATTEO FLORA - COFONDATORE CENTRO HERMES PER LA TRASPARENZA E DIRITTI DIGITALI

Telegram si è trovata ad essere la piattaforma di elezione per i fuoriusciti, i reietti, i paria.

LUCINA PATERNESI FUORICAMPO

Nessuna trasparenza su algoritmi e funzionamento perché la fiducia se l'è conquistata sul campo. Ci dobbiamo fidare, intanto, però, Durov ha spostato i suoi affari a Dubai.

MICHAEL TRETYAK - AVVOCATO DIGITAL RIGHTS CENTER

Uno come Pavel Durov è accolto a braccia aperte. Gli sceicchi locali hanno liquidità e cercano di far diventare gli Emirati la Silicon Valley del futuro.

LUCINA PATERNESI FUORICAMPO

La catena societaria di Telegram si snoda tra le isole Vergini britanniche, il Belize e gli Emirati Arabi Uniti, dove Pavel Durov ha scelto di vivere oggi. Resta il problema di come sopravvivere economicamente per un'app che ha deciso di non raccogliere e vendere dati.

ALESSIA MARZI

Ma qual è il modello di business di Telegram?

MICHAEL TRETYAK - AVVOCATO DIGITAL RIGHTS CENTER

Proprio all'inizio di quest'anno hanno raccolto un miliardo di dollari in obbligazioni convertibili.

ALESSIA MARZI

All'iniziativa, però, ha partecipato anche il fondo d'investimento russo.

MICHAEL TRETYAK- AVVOCATO DIGITAL RIGHTS CENTER

Beh, la cosa non è passata inosservata perché il fondo russo ha pubblicizzato la vicenda come se avesse investito direttamente in obbligazioni Telegram.

ALESSIA MARZI

È una sorta di partecipazione indiretta?

MICHAEL TRETYAK- AVVOCATO DIGITAL RIGHTS CENTER

Fondamentalmente era una rivendita, di cui non erano a conoscenza. Quando questi bond diventeranno azioni, il fondo russo potrebbe trovarsi ad essere addirittura proprietario di Telegram.

SIGFRIDO RANUCCI IN STUDIO

Insomma alla fine i russi sono riusciti ad infilarsi in una porticina. È un'operazione finanziaria realizzata in partner con altri fondi, anche se la loro partecipazione è minore, ma insomma chi è che ha tirato poi le fila? Il fondo sovrano degli Emirati, che sta guardando con attenzione particolare al post petrolio, sta guardando, dicevamo, in particolare, alla ricchezza dei dati. D'altra parte uno che ha una piattaforma, come Durov, che gestisce i dati di 500 milioni di persone, non può che far gola. Anche lui ha dovuto capitolare alle logiche di mercato e rischia a questo punto anche qualche ingerenza politica di qualche Stato. Insomma bisogna solo, poi, alla fine, scegliere quale. Chi vuole attaccarsi alla privacy a tutti i costi non può che o fidarsi del padrone dell'app di messaggistica oppure ricorrere al vecchio, saggio, intramontabile pizzino di carta.