Guerra Israele-Palestina: come Gaza ha ribaltato la situazione a discapito dei suoi carcerieri

David Hearst

9 ottobre 2023 – Middle East Eye

La responsabilità dell'assalto di questo fine settimana ricade su tutti coloro che da tempo hanno smesso di considerare i palestinesi come persone

Nelle ultime 48 ore uno Stato abituato a esercitare un controllo totale su sette milioni di palestinesi ha subito una drammatica inversione di ruoli.

I combattenti palestinesi hanno preso il posto dei coloni armati che terrorizzano gli abitanti dei villaggi palestinesi riuscendo a prendere il controllo di alcuni insediamenti coloniali adiacenti a Gaza.

Invece degli abitanti di Huwwara o Nablus o Jenin, traumatizzati ogni notte dagli attacchi dei coloni e dalle incursioni dell'esercito israeliano, sono stati quelli di Sderot a doversi nascondere rannicchiandosi nei loro scantinati e chiedersi quando il loro esercito sarebbe giunto per proteggerli.

I combattenti palestinesi hanno sequestrato decine di soldati e civili israeliani, che ora si trovano negli scantinati di tutta Gaza.

Nessuno dovrebbe vantarsi di questo. Sono stati uccisi civili innocenti; sono state terrorizzate madri incinte e sono morti bambini. L'attacco ha travolto chiunque si trovasse sul suo cammino, indipendentemente dalle appartenenze politiche, dal sesso o dall'età.

Conosco una donna aspramente contraria al trionfalismo nazionalista religioso di destra e convinta sostenitrice dei diritti umani dei palestinesi che è stata trascinata in uno scantinato a Gaza.

Ma le scene sulle quali il mondo ha perso l'uso della parola non sono queste. Sono quelle di soldati israeliani che portano via palestinesi per farli scomparire in galera per periodi indefiniti di detenzione amministrativa.

Secondo gli ultimi rapporti a Gaza potrebbero esserci quasi 100 prigionieri. L'esercito e le forze di polizia meglio equipaggiati del Medio Oriente hanno subito perdite inaudite (l'ultimo bilancio, compresi i civili, è di 600 morti e più di 1.500 feriti)[al 12ott i morti israeliani sono 1200 e i feriti oltre 2700, ndt] mentre sono rimasti bloccati in violenti scontri a fuoco strada per strada nei villaggi e nelle città attorno a Gaza.

Colossale fallimento dell'intelligence

Questa è la prima volta che si assiste a scene del genere dalla guerra del 1948 che diede origine alla prima Nakba e allo Stato di Israele. Per gli israeliani queste scene sono molto peggiori della guerra arabo-israeliana del 1973, scatenata quasi 50 anni fa.

"Nel 1973 abbiamo combattuto con un esercito addestrato", ha detto l'esperto analista israeliano Meron Rapoport a Middle East Eye. "E qui parliamo di persone che non hanno altro che un Kalashnikov. È inimmaginabile. È un fallimento militare e di intelligence dal quale Israele impiegherà molto tempo per riprendersi in termini di fiducia in sé stesso".

Lo sfondamento della recinzione meglio difesa e sorvegliata lungo l'intero confine di Israele e un'incursione di queste dimensioni insieme alla cattura del quartier generale militare della divisione dell'esercito che controlla Gaza rappresentano il peggior fallimento che i servizi di intelligence israeliani hanno subito nella loro storia.

Hamas ha raggiunto l'obiettivo della totale sorpresa. La famosa unità di intelligence militare israeliana, la 8200, in grado di ascoltare ogni conversazione telefonica a Gaza è stata colta di sorpresa, così come lo Shin Bet, il servizio di sicurezza interna.

Gli israeliani si chiedono come il loro esercito abbia potuto

commettere un errore talmente grande da schierare 33 battaglioni nella Cisgiordania occupata per proteggere i coloni lasciando il confine meridionale vulnerabile agli attacchi.

Tutto ciò ha innescato un'onda d'urto delle dimensioni di uno tsunami che ha investito una nazione così abituata a impersonare i Signori della Terra. In realtà sono loro che dovrebbero far scattare le sorprese, non i loro sudditi.

Rinascere più forti

Solo due settimane fa il primo ministro israeliano Benjamin Netanyahu ha sventolato davanti all'Assemblea generale delle Nazioni Unite una mappa in cui tutti i territori palestinesi erano stati cancellati.

"Sono convinto che ci troviamo sulla soglia di una svolta ancora più epica: una pace storica tra Israele e Arabia Saudita. Una pace di questo tipo contribuirà notevolmente a porre fine al conflitto arabo-israeliano", ha affermato Netanyahu.

I funzionari statunitensi non la pensavano diversamente, dal momento che una figura di alto livello dell'amministrazione ha affermato che "da molti anni a questa parte la regione è pressoché stabile".

Come in un unico coro Washington, Tel Aviv e Riad hanno parlato della prospettiva che l'Arabia Saudita firmasse un accordo di normalizzazione con Israele, quasi che questo fosse di per sé la via verso la pace.

Erano tutti diventati così convinti di escludere i palestinesi da questa equazione, come se l'intera popolazione palestinese un giorno avrebbe potuto cancellare la propria bandiera e identità nazionale e avrebbe accettato il ruolo di Gastarbeiter [lavoratore ospite in tedesco, ndt.] nella terra di qualcun altro.

Ora è stato inviato un messaggio molto chiaro: i palestinesi esistono e non sono affatto in procinto di venire sottomessi.

Ogni volta che sono stati annientati come forza combattente, nel 1948, 1967, 1973 e in ogni operazione successiva, rinasceva più forte una nuova generazione di combattenti. E nessuna versione passata di Hamas o Hezbollah è più forte di quelle che Israele si trova ad affrontare oggi.

Hamas ha definito il suo attacco al sud di Israele il diluvio di Al-Aqsa per un'ottima ragione. Questo attacco non è venuto dal nulla.

Lo status quo di Al-Aqsa

L'8 ottobre 1990, esattamente 33 anni fa, un gruppo di coloni e i Fedeli del Monte del Tempio, un gruppo di estrema destra che pretendeva di svolgere un sacrificio rituale sul Monte del Tempio, un atto proibito dal rabbino capo di Israele, tentarono di porre una prima pietra per la costruzione del Terzo Tempio presso la Moschea di Al-Aqsa.

La popolazione palestinese della Città Vecchia oppose resistenza, l'esercito israeliano aprì il fuoco e in pochi minuti vennero uccisi più di 20 palestinesi, con altre centinaia di feriti e arrestati.

Da allora i leader israeliani sono stati continuamente avvertiti di mantenere lo status quo in un luogo sacro rivendicato da entrambe le religioni, e ogni anno hanno ignorato quegli ammonimenti forzando il divieto.

E così anche oggi, quando Al-Aqsa è stata presa d'assalto ripetutamente per consentire ai fedeli ebrei l'accesso al sito islamico dove visite, preghiere e rituali non graditi da parte dei non musulmani sono vietati sulla base di accordi internazionali pluridecennali.

Un tempo queste violente incursioni erano opera di quelli che tra gli ebrei erano considerati gruppi marginali di estremisti. Ora non più. Adesso sono guidati da Itamar Ben Gvir, che sfila con il titolo di ministro della sicurezza nazionale israeliana.

Giorno dopo giorno, con il sostegno dei parlamentari del Likud, come

Amit Halevi, viene elaborata una politica volta a dividere la moschea di Al-Aqsa tra ebrei e musulmani, proprio come fu divisa la moschea Ibrahimi a Hebron negli anni ’90.

Ben Gvir, il ministro con il potere di nominare il capo della polizia israeliana, non ha risparmiato i cristiani dalle sue politiche fasciste. Quando cinque ebrei ortodossi sono stati arrestati dalla polizia con l’accusa di aver sputato contro i fedeli cristiani nella Città Vecchia di Gerusalemme, il ministro ha risposto: “Continuo a pensare che sputare contro i cristiani non sia un reato penale. Penso che dobbiamo intervenire attraverso l’istruzione e l’educazione. Non tutto giustifica un arresto”.

Silenzio internazionale

La pressione continua ad aumentare, sia ad Al-Aqsa che nello spaventoso bilancio quotidiano delle vittime palestinesi, la maggior parte dei quali giovani. Human Rights Watch ha rilevato che nell’arco di più di 15 anni quest’ultimo, fino alla fine di agosto, è stato il più sanguinoso per i minorenni palestinesi nella Cisgiordania occupata, con almeno 34 minori uccisi.

E ciò viene accolto con il silenzio della comunità internazionale, la cui attenzione resta concentrata solo sugli scambi commerciali tra il Mar Rosso e Haifa.

Se c’è qualcuno responsabile dello spargimento di sangue di questo fine settimana e dei massacri di civili che, come è vero che la notte segue il giorno, sono destinati a verificarsi a Gaza mentre l’esercito israeliano lancia un’offensiva di terra, sono tutti i leader stranieri che dicono che Israele condivide i loro valori. Tutti questi leader permettono a Israele di dettare la politica, anche se questa danneggi palesemente la loro.

Qualunque cosa accada nei prossimi giorni e settimane a Gaza, e Israele ha già scatenato una vendetta selvaggia a prescindere dall’assenza di un obiettivo militare, Hamas ha senza dubbio segnato una vittoria significativa.

Ha portato con sé giornalisti e operatori televisivi che hanno registrato tutto ciò che è accaduto. Queste riprese parleranno a ogni giovane palestinese e arabo che le vedrà.

Le riprese mostrano i palestinesi che ritornano nelle terre da cui i loro padri erano stati cacciati. I rifugiati costituiscono il 67% della popolazione di Gaza, provenienti principalmente dalle terre intorno a Gaza che Hamas ha temporaneamente liberato.

Questo fine settimana hanno esercitato con la forza delle armi il diritto al ritorno che era stato tolto dal tavolo delle trattative 23 anni fa.

Le immagini diranno a tutti i palestinesi che la resistenza non è una causa persa contro un nemico estremamente potente. Diranno che la loro volontà di resistere è più potente di quella del loro oppressore.

Lo scenario è cambiato per sempre

Non ho dubbi che ora i civili palestinesi pagheranno un prezzo enorme mentre Israele persegue la sua vendetta biblica. Ai più di due milioni di persone nella Striscia è stata già tagliata l'elettricità.

Ma non ho neanche dubbi che dopo questi eventi le cose non torneranno più come prima.

Dopo aver negato per generazioni l'esistenza della Nakba, i parlamentari israeliani ne stanno ora programmando apertamente un'altra. Ariel Kallner ha twittato: "Cancellate il nemico adesso! Questo giorno è la nostra Pearl Harbor. Impareremo ancora dalle lezioni. Ora un obiettivo: la Nakba!"

Netanyahu non è da meno con il suo appello a tutti i palestinesi di Gaza affinché lascino le loro case, come se ci fosse un posto dove andare.

Se Israele volesse davvero scatenare una guerra regionale un tentativo di ripetere quanto accaduto nel 1948 sarebbe il modo più rapido per farlo. Né l'Egitto né la Giordania lo tollererebbero, e i loro accordi di pace con Israele diventerebbero nulli.

Una guerra regionale coinvolgerebbe il movimento di resistenza meglio equipaggiato della regione: Hezbollah, che domenica ha iniziato uno scontro a fuoco con Israele al confine libanese, potrebbe essere riluttante a farsi coinvolgere ma potrebbe anche esservi trascinato dentro. Hezbollah segnala da tempo che un'incursione di terra a Gaza costituirebbe per loro una linea rossa.

Nel corso dell'anno i leader politici di Hamas hanno visitato Beirut e hanno avuto incontri con il segretario generale di Hezbollah, Hassan Nasrallah. Secondo alcune fonti sarebbe già stata presa una decisione riguardo ad una mobilitazione generale. Da tutto ciò si può supporre che il dito di Hezbollah sia sul grilletto.

Israele dovrà anche fare i conti col fatto che Hamas detiene decine di ostaggi. La Direttiva Annibale, un ordine militare top-secret secondo il quale Israele dovrebbe colpire i propri soldati per evitare che cadano nelle mani del nemico, non è più in vigore.

Né lo è l'idea che a Gaza 2,3 milioni di persone possano essere rinchiuse in una gabbia costrette a seguire una dieta a basso contenuto proteico e che il loro carceriere butti via le chiavi.

Questa è l'esplosione che io e altri avevamo da tempo avvertito sarebbe arrivata. Ho detto che se Israele non avesse invertito la rotta avviando negoziati seri su una soluzione giusta a questa crisi con la concessione ai palestinesi degli stessi diritti degli ebrei ci sarebbe stata una risposta. Ora è successo. Quando tutto sarà finito lo scenario non sarà più lo stesso.

Mentre tre famiglie allargate di Gaza venivano spazzate via dal colpo diretto sulle loro case da parte delle bombe di precisione israeliane, Rishi Sunak, il primo ministro del Paese che ha più responsabilità di ogni altro per questo conflitto, ha detto che la Gran Bretagna è inequivocabilmente dalla parte di Israele, e ha illuminato Downing Street con una stella di David. Nel frattempo il suo ministro degli Interni ha detto che chiunque venga sorpreso a manifestare per le strade in solidarietà con la Palestina sarà arrestato. Di conseguenza il Regno Unito ha abbandonato qualsiasi suo possibile ruolo futuro nel

porre fine a questo terribile conflitto.

La responsabilità di quanto accaduto lo scorso fine settimana ricade su tutti coloro che si sono illusi di pensare che le successive generazioni di leader israeliani avrebbero potuto cavarsela impunemente nel fare quello che volevano. La responsabilità ricade su tutti coloro, compresa la maggior parte dei dittatori arabi, che hanno smesso di considerare i palestinesi come un popolo. Nelle settimane e mesi a venire ognuno imparerà una lezione dolorosa.

Le opinioni espresse in questo articolo appartengono all'autore e non riflettono necessariamente la politica editoriale di Middle East Eye.

(Traduzione dall'inglese di Aldo Lotta)

Ex soldati israeliani rivelano: niente è così integro come un cuore spezzato

Ex soldati israeliani rivelano: niente è così integro come un cuore spezzato

Jim Miles

11 novembre 2021 – Palestine Chronicle

La scorsa settimana (11-04-2021) Independent Jewish Voices [Voci ebraiche indipendenti: organizzazione di eminenti intellettuali britannici che combattono l'opinione che tutti gli ebrei sostengano le politiche del governo israeliano, ndtr.] (IJV – Canada) ha presentato un webinar intitolato "From IDF to IJV", che illustrava la storia di tre ebrei già appartenenti all'esercito israeliano ma che nel corso degli anni e attraverso esperienze simili se pur diverse hanno finito per

collaborare con IJV-Canada.

Il conduttore del programma, Aaron Lakoff, ha sottolineato la "solidarietà senza compromessi" di IJV con le lotte del popolo palestinese per i diritti umani e l'uguaglianza civile in Palestina, in sostanza, in tutta la Palestina storica. IJV è stata una delle prime organizzazioni in Canada a riconoscere e sostenere la campagna del BDS. Per riassumere l'immagine complessiva dello scoprire di essere stati ingannati dalla famiglia, dal governo e dalla società civile, si è fatto riferimento agli scritti ebraici radicali di Kokzter Rebbe [il rabbino Menachem Mendel of Kotzk (1787-1859), ndtr.]: "Niente è così integro come un cuore spezzato". Il suo significato non mi è risultato chiaro fino a quando non ho sentito le tre storie.

I racconti

Tutti e tre i protagonisti risultavano avere delle esperienze simili ma con delle differenze; la principale caratteristica comune era il loro ebraismo laico, per cui la religione insita nell'essere ebrei era sostituita da una fede nel sionismo. L'adesione all'esercito era scontata, incoraggiata da una influente propaganda. Era un esercito come nessun altro, l'esercito più etico del mondo.

La conduttrice del webinar, Lia Tarachansky, ha rilevato come l'esercito sia mutato in tre aspetti significativi: in primo luogo, la maggior parte degli sforzi è stata dedicata all'Unità 8200, il reparto di intelligence dell'esercito, e ai suoi compiti massicci di sorveglianza e *hasbara* [parola in lingua ebraica che indica gli sforzi mediatici per diffondere informazioni positive sullo Stato di Israele e le sue azioni, ndtr.]; successivamente ha menzionato l'uso crescente di un esercito "telecomandato", con l'impiego dell'intelligenza artificiale e la robotica moderne per affrontare qualsiasi presunto nemico; e – cosa più sorprendente, anche se forse non lo è, in linea con quanto avviene negli Stati Uniti – la privatizzazione delle attività dell'esercito nel tentativo di assolvere il governo da responsabilità per i crimini commessi.

Prese di coscienza

Pur accettando inizialmente il loro impegno nell'esercito, con il tempo, a volte rapidamente, questi soldati hanno progressivamente perso le loro illusioni sull'esercito e sulla politica israeliana in generale. Per Daphna Levit, un'ebrea Mizrahi [ebrei originari del mondo arabo, ndtr.], l'esercito presentato nelle scuole

era “sempre qualcosa per cui provavamo ammirazione” e il ruolo dell’esercito costituiva un “impegno glorioso ed eroico” nella misura in cui era “bello morire per il paese” – Dio era diventato Sion. Il suo compito nella guerra del 1967 era quello di scortare gli addetti alle comunicazioni in diverse zone di guerra e, nel far questo, “creare una narrazione” differente da ciò che vedeva. Ha citato in particolare l’immagine dei profughi palestinesi che attraversavano l’Allenby Bridge [importante ponte internazionale che collega la Cisgiordania alla Giordania, ndtr.] verso la Giordania, una scena resa non fedelmente dalla descrizione che le è stata fornita.

Yom Shamash si avventurò in Israele nel 1971, sentendosi “al sicuro” in Israele, che era in pace avendo “neutralizzato” l’Egitto [in seguito al conflitto arabo israeliano del giugno 1967, chiusosi dopo sei giorni con la vittoria di Israele, ndtr.]. Nel descriversi come “un pessimo soldato”, ha raccontato di essere stato distaccato nel deserto del Sinai quando la guerra dello Yom Kippur [conflitto arabo israeliano dell’ottobre 1973, ndtr.] colse “tutti di sorpresa” e che “la mia unità venne decimata”. Iniziò a mettere in discussione il senso di tutto, chiedendosi “per cosa sono morti… per la sabbia?” Venne totalmente sconvolto quando seppe che Golda Meier aveva respinto la richiesta di colloqui di pace da parte di Anwar Sadat. Ha rievocato come, in precedenza, durante il suo addestramento, fosse all’aperto durante un pattugliamento notturno e si fosse reso conto che la strana sensazione sotto i suoi stivali derivava dal “marciare sugli ortaggi” – si stavano addestrando calpestando gli orti dei palestinesi.

Giungendo poco più tardi, Rafi Silver emigrò in Israele nel 1971 e si stabilì in un kibbutz (dove i soldati “erano venerati”) sulle alture del Golan. Provenendo da una famiglia profondamente sionista rimase “intrappolato nel mito dell’esercito” e le sue convinzioni vennero poi “fatte a pezzi dalla realtà”. Al momento di decidere dove arruolarsi, il problema comune era “come entrare in un corpo d’élite”: non mettersi alla prova era motivo di vergogna. Cosa che superò nei primi quindici minuti dell’addestramento iniziale.

Ha rievocato l’”incidente definitivo” che fece cambiare le sue convinzioni radicalmente verso la pace. Nel 1996 prestò servizio in un’unità di riserva che aveva imposto un blocco e un coprifuoco di una settimana in un campo profughi vicino a Betlemme. Ha raccontato che nel buio della notte, cessato il coprifuoco, aveva visto un ragazzo alzarsi dalla posizione accovacciata che i soldati gli avevano ordinato di assumere. Di riflesso, nel buio della notte, teso e impaurito

dal contesto del campo, mosse il dito sul grilletto del suo fucile pronto a sparare. “Ero spaventato.” Un altro membro dell’unità gli intimò di non sparare e alla fine lui disse: “Basta… non ce la faccio più… ho quasi ucciso un ragazzino”.

L’altro

Un forte filo conduttore è costituito dal modo in cui venivano rappresentati i palestinesi. Nessuno dei protagonisti ha avuto rapporti diretti con loro.

Yom ha affermato che ogni giorno vedeva giungere dei palestinesi per lavorare nei parchi israeliani a Gaza, ma di non aver avuto contatti con loro. Ha detto: “Ai soldati israeliani veniva chiesto di fare ogni genere di cose orribili” e quando protestava, gli veniva detto “È l’unico modo per farlo… quelle persone non sono come te”, erano “meno che umani”. Il lavaggio del cervello nell’esercito era volto a creare soldati obbedienti, che non facessero domande, sottolineando che “l’altro non è come te”.

Daphna all’inizio li vedeva solo come fredde vittime di una guerra da cui doveva ricavare una narrazione che sostenesse lo Stato e non la realtà. Nata in Israele, ne aveva “sentito parlare” ma non aveva visto nessun palestinese, fornendo così la sua definizione della natura di “apartheid” di Israele. Un po’ più tardi, mentre lavorava con Physicians for Human Rights [Medici per i diritti umani: ONG con sede negli Stati Uniti che documenta e difende contro le atrocità e le gravi violazioni dei diritti umani, ndtr.], si è imbattuta in una ragazzina in una clinica in cui lavorava. La ragazzina le chiese da dove venisse, e quando le disse di essere israeliana, il viso della ragazzina espresse lo sgomento di trovarsi insieme al “nemico”.

Dopo il suo servizio di leva Rafi è tornato a Gaza come civile nel campo profughi di Jabaliya – e ha visto ciò che non vedeva come soldato: degli esseri umani. Era “stupito” dal fatto che, sebbene ogni palestinese sapesse che era stato nell’esercito, “non ho incontrato l’ostilità o l’odio che mi aspettavo”. Divenne, alla fine, un rapporto umano, e non ideologico.

“Niente è così integro come un cuore spezzato.”

Dopo un’educazione che inculca un particolare dogma ideologico, può essere traumatizzante solo fino a un certo punto vedere quelle convinzioni infrangersi o dissolversi gradualmente.

Questi ex appartenenti all'esercito hanno compiuto un percorso emozionale da una fede convinta nella superiorità della loro religione – il sionismo – e nella maggiore eticità del loro esercito fino a diventare attivisti contro i crimini di guerra e i crimini contro l'umanità israeliani in Palestina. Anche molti altri hanno compiuto questo percorso e si può sperare che molti più cuori saranno spezzati per essere integri.

– Jim Miles è un educatore canadese e un giornalista che collabora regolarmente attraverso articoli di opinione e recensioni di libri con Palestine Chronicles*. Il suo interesse per questo argomento nasce originariamente da una prospettiva ambientalista, che prende in esame la militarizzazione e la sottomissione economica della comunità globale e la sua mercificazione da parte del dominio delle imprese e del governo americano.*

(traduzione dall'inglese di Aldo Lotta)

Cancellando i palestinesi, le reti sociali diffondono un segnale inquietante per il nostro avvenire

Jonathan Cook

sabato 7 novembre 2020 – Middle East Eye

Facebook, Google e Twitter non sono piattaforme neutrali. Controllano lo spazio pubblico informatico per aiutare i potenti e possono cancellare da un giorno all'altro chiunque di noi

Si può percepire un crescente malessere nei confronti dell'impatto nefasto che possono avere sulle nostre vite le decisioni prese dalle imprese che guidano le reti sociali. Benché godano di un monopolio effettivo sullo spazio pubblico virtuale,

queste piattaforme sfuggono da molto tempo ad ogni serio controllo e ad ogni responsabilità.

In un nuovo documentario Netflix, *The Social Dilemma* [Il dilemma del social], ex-dirigenti della Silicon Valley mettono in guardia contro un avvenire distopico. Google, Facebook e Twitter hanno raccolto una grande quantità di dati che ci riguardano per prevedere e manipolare meglio i nostri desideri. I loro prodotti riformulano progressivamente le connessioni dei nostri cervelli per renderci dipendenti dagli schermi e più docili alle pubblicità. Poiché siamo chiusi dentro camere digitali di risonanza ideologica, ne conseguono una polarizzazione e una confusione sociale e politica sempre maggiori.

Come a sottolineare la presa sempre più forte che queste società tecnologiche esercitano sulle nostre vite, il mese scorso Facebook e Twitter hanno deciso di interferire apertamente sulle elezioni presidenziali americane più esplosive a memoria d'uomo censurando un articolo che avrebbe potuto nuocere alle prospettive elettorali di Joe Biden, lo sfidante democratico del presidente uscente Donald Trump.

Dato che quasi la metà degli americani si informa principalmente su Facebook, le conseguenze di una simile decisione sulla nostra vita politica non sono difficili da interpretare. Scartando ogni dibattito sulle presunte pratiche di corruzione e traffico di influenze da parte del figlio di Joe Biden, Hunter, in nome di suo padre, queste reti sociali hanno giocato un ruolo di arbitro autoritario decidendo quello che siamo autorizzati a dire e a sapere.

Il "guardiano di un monopolio"

Il pubblico occidentale si sveglia molto in ritardo di fronte al potere antidemocratico che le reti sociali esercitano su di lui. Ma se vogliamo capire dove alla fine questo ci porta, non c'è uno studio di caso migliore del trattamento molto differenziato riservato dai giganti tecnologici agli israeliani e ai palestinesi.

Il modo in cui i palestinesi sono in rete serve da avvertimento, perché sarebbe in effetti insensato considerare queste imprese mondiali come piattaforme politicamente neutrali e le loro decisioni come puramente commerciali. Sarebbe come interpretare il loro ruolo in modo doppiamente sbagliato.

Di fatto le compagnie che guidano le reti sociali sono oggi delle reti di

comunicazione monopolistiche, alla stregua delle reti elettriche, idriche o telefoniche di una ventina di anni fa. Le loro decisioni non sono quindi più delle questioni private, ma hanno enormi conseguenze sociali, economiche e politiche. È in parte la ragione per la quale il dipartimento di Giustizia degli Stati Uniti ha recentemente avviato un'azione legale contro Google, accusandolo di essere il "guardiano di un monopolio su internet".

Google, Facebook e Twitter non hanno più diritto di decidere arbitrariamente le persone e i contenuti che ospitano sui loro siti di quanto una volta le imprese di telecomunicazioni avessero il diritto di decidere se un cliente doveva essere autorizzato a disporre di una linea telefonica.

Tuttavia, contrariamente alle compagnie telefoniche, le società alla testa delle reti sociali controllano non solo i mezzi di comunicazione, ma anche il loro contenuto. Come dimostra l'esempio dell'articolo su Hunter Biden, possono decidere se i loro clienti possono partecipare a delle discussioni pubbliche fondamentali su quelli che li governano.

Agendo in questo modo nei confronti di Hunter Biden, è come se un'azienda telefonica di una volta non solo ascoltasse le conversazioni, ma potesse anche interromperle se non le piacesse la posizione politica di un determinato cliente.

In realtà è persino peggio. Le reti sociali informano ormai gran parte della popolazione. La censura di un articolo da parte loro è simile piuttosto all'azione di una compagnia elettrica che tolga la corrente a tutti durante una trasmissione televisiva per essere sicura che nessuno la veda.

Una censura occulta

I giganti della tecnologia sono le imprese più ricche e potenti nella storia dell'umanità, la loro ricchezza si misura in centinaia, ormai migliaia, di miliardi di dollari. Ma l'argomento secondo cui sono apolitiche e hanno come solo scopo massimizzare i profitti non ha mai retto.

Hanno tutto l'interesse a promuovere responsabili politici che si schierino dalla loro parte impegnandosi a non infrangere il loro monopolio né a regolamentare le loro attività, o, meglio ancora, promettendo di indebolire gli strumenti che potrebbero impedire loro di diventare ancora più ricche e potenti.

Al contrario, i giganti della tecnologia hanno anche tutto l'interesse ad utilizzare lo spazio informatico per penalizzare e marginalizzare gli attivisti politici che rivendicano una maggiore regolamentazione delle loro attività o del mercato in generale.

A prescindere dalla spudorata eliminazione dell'articolo su Hunter Biden, che ha suscitato la collera dell'amministrazione Trump, le società alla testa delle reti sociali censurano più spesso in modo occulto. Questo potere è esercitato per mezzo di algoritmi, questi codici segreti che decidono se qualcosa o qualcuno compare nei risultati di una ricerca o sulle reti sociali. Se lo desiderano, questi titani tecnologici possono cancellare chiunque di noi da un giorno all'altro.

Non è solo paranoia politica. L'impatto sproporzionato dei cambiamenti di algoritmo sui siti "di sinistra" sul web, i più critici verso il sistema neoliberale che ha arricchito le imprese che guidano le reti sociali, è stato recentemente sottolineato dal Wall Street Journal [quotidiano USA più venduto e che si occupa principalmente di economia, ndtr.].

Il tipo sbagliato di discorso

I responsabili politici capiscono sempre di più il potere delle reti sociali, ragione per cui possono sfruttarlo al meglio per i propri fini. Dopo lo choc della vittoria elettorale di Trump alla fine del 2016, negli Stati Uniti e nel Regno Unito i dirigenti di Facebook, Google e Twitter sono stati regolarmente portati davanti a commissioni parlamentari di sorveglianza.

Queste reti sociali si vedono regolarmente rimproverare dai responsabili politici di essere all'origine di una crisi di "notizie false", una crisi in realtà molto precedente alle reti sociali, come testimonia anche troppo chiaramente la truffa da parte dei responsabili politici americani e britannici che ha messo Saddam Hussein in relazione con l'11 settembre ed affermato che l'Iraq possedeva "armi di distruzione di massa".

I responsabili politici hanno allo stesso modo cominciato ad accusare le società di internet di "ingerenza straniera" nelle elezioni in Occidente, rimproveri in genere rivolti alla Russia, nonostante la mancanza di prove serie che confermino la maggior parte delle loro affermazioni.

Pressioni politiche vengono esercitate non per rendere le imprese più trasparenti e

responsabili, ma per spingerle ad applicare in modo ancora più assiduo restrizioni contro i discorsi sbagliati, che si tratti di razzisti violenti a destra o di detrattori del capitalismo e delle politiche dei governi occidentali a sinistra.

È per questo che diventa sempre più vuota l'immagine originale delle reti sociali come luoghi neutrali di condivisione delle informazioni, come strumenti che permettono di diffondere il dibattito pubblico e incrementare l'impegno civico, o ancora di sviluppare un discorso orizzontale tra ricchi e potenti da una parte e deboli ed emarginati dall'altra.

Diritti informatici differenti

È in Israele che i rapporti tra il settore delle tecnologie e i responsabili statali sono più evidenti. Ciò ha determinato una notevole differenza nel trattamento riservato ai diritti informatici degli israeliani e dei palestinesi. La sorte dei palestinesi in rete lascia presagire un futuro in cui quelli che sono già potenti eserciteranno un controllo sempre maggiore su ciò che dobbiamo sapere e siamo autorizzati a pensare, su chi può continuare ad essere visibile e chi deve essere cancellato dalla vita pubblica.

Israele era già in buona posizione nell'utilizzo delle reti sociali prima che la maggioranza degli altri Stati avesse riconosciuto la loro importanza in materia di manipolazione degli atteggiamenti e delle percezioni della gente. Per decenni Israele ha subappaltato un programma ufficiale di hasbara, o propaganda di Stato, ai propri cittadini e ai propri sostenitori all'estero. Con l'apparizione di nuove piattaforme informatiche, questi sostenitori non vedevano l'ora di espandere il proprio ruolo.

Israele ne poteva trarre un altro beneficio. Dopo l'occupazione della Cisgiordania, di Gerusalemme e di Gaza nel 1967, ha iniziato ad elaborare un discorso sulla vittimizzazione dello Stato, ridefinendo l'antisemitismo per far intendere che ormai questo male affliggesse in particolare la sinistra, e non la destra. Questo "nuovo antisemitismo" non prendeva di mira gli ebrei ma riguardava piuttosto le critiche nei confronti di Israele e il sostegno a favore dei diritti dei palestinesi.

Questo discorso molto discutibile si è dimostrato facile da sintetizzare in piccole frasi adatte alle reti sociali.

Israele definisce ancora correntemente "terrorismo" qualunque resistenza

palestinese alla sua violenta occupazione o alle sue colonie illegali, descrivendo le dimostrazioni di sostegno da parte di altri palestinesi come “incitamento all’odio”. La solidarietà internazionale nei confronti dei palestinesi è definita “delegittimazione” ed equiparata all’antisemitismo.

“Inondare internet”

Già nel 2008 si è scoperto che una lobby mediatica filo-israeliana, Camera, architettava iniziative segrete da parte di sostenitori di Israele per infiltrarsi nell’enciclopedia in rete Wikipedia per modificare delle voci e “riscrivere la storia” da un punto di vista favorevole a Israele. Poco dopo l’uomo politico Naftali Bennett [estrema destra dei coloni, ndtr.] ha contribuito a organizzare corsi di “revisione sionista” di Wikipedia.

Nel 2011 l’esercito israeliano ha dichiarato che le reti sociali costituiscono un nuovo “campo di battaglia” e ha incaricato dei “cyber-guerrieri” di condurre la battaglia in rete. Nel 2015 il ministero degli Affari Esteri israeliano ha organizzato un centro di comando supplementare per reclutare giovani ex-soldati ed esperti tecnologici all’interno dell’Unità 8200, unità di sorveglianza informatica dell’esercito, per condurre la battaglia in rete. Molti di loro hanno in seguito creato imprese di tecnologia avanzata, per cui informatici dello spionaggio hanno fatto parte integrante del funzionamento delle reti sociali.

Act.IL, un’applicazione lanciata nel 2017, ha permesso di mobilitare i sostenitori di Israele perché si “annidassero” in siti che ospitavano critiche verso Israele o sostegno per i palestinesi. Sostenuta dal ministero degli Affari Strategici di Israele, questa iniziativa era diretta da veterani dei servizi di informazione israeliani.

Secondo *Forward*, rivista ebrea americana, i servizi di informazione israeliani sono in stretto rapporto con Act.IL e chiedono aiuto per ottenere che le reti sociali ritirino alcuni contenuti, in particolare dei video. “Il suo lavoro offre finora un quadro impressionante del modo in cui potrebbero plasmare delle conversazioni in rete riguardo ad Israele senza mai farsi vedere”, ha osservato *Forward* poco tempo dopo l’implementazione dell’applicazione. Sima Vaknin-Gil, un’ex- censore dell’esercito israeliano che all’epoca era di stanza al ministero degli Affari Strategici di Israele, ha dichiarato che l’obiettivo era di “creare una comunità di combattenti” la cui missione consisteva nell’ “inondare internet” di propaganda israeliana.

Alleati volenterosi

Grazie a vantaggi in termini di effettivi e di zelo ideologico, di esperienza tecnologica e di propaganda, di influenze nelle alte sfere a Washington e nella Silicon Valley, Israele ha rapidamente potuto trasformare le reti sociali in alleati volonterosi nella sua lotta per emarginare i palestinesi in rete.

Nel 2016 il ministero della Giustizia israeliano si vantava che Facebook, Google e YouTube "si adeguano per il 95% alle richieste israeliane di eliminazione di contenuti," questi ultimi provenienti quasi tutti da palestinesi. Le società che dirigono le reti sociali non hanno confermato questo dato.

L'Anti-Difamation League, un'associazione della lobby filo-israeliana che è solita calunniare le organizzazioni palestinesi e i gruppi ebraici critici con Israele, nel 2017 ha creato un "centro di comando" nella Silicon Valley per sorvegliare quelli che definisce "discorsi di odio in rete". Lo stesso anno la lobby è diventata un "Trusted Flagger " [lett. fidato segnalatore, persona o ente di cui una rete sociale accoglie le indicazioni, ndtr.] per YouTube, cosa che significa che le sue segnalazioni su contenuti da ritirare sono diventate prioritarie.

Durante una conferenza organizzata a Ramallah nel 2018 da 7amleh, un gruppo palestinese di difesa dei diritti in rete, i rappresentanti locali di Google e Facebook non hanno affatto nascosto le rispettive priorità. Per loro era importante evitare di contrariare i governi che hanno il potere di limitare le loro attività commerciali, anche se questi governi si dedicano a sistematiche violazioni del diritto internazionale e dei diritti dell'uomo. In questa battaglia l'Autorità Nazionale Palestinese non ha alcun peso. Israele ha messo le mani sulle infrastrutture della comunicazione e internet dei palestinesi, ne controlla l'economia e le principali risorse.

Dal 2016 il ministero della Giustizia israeliano avrebbe eliminato decine di migliaia di post da parte di palestinesi. Attraverso un processo assolutamente oscuro, Israele individua con i propri algoritmi i contenuti che ritiene "estremisti" e poi ne chiede la cancellazione. Centinaia di palestinesi sono stati arrestati da Israele dopo che avevano pubblicato commenti sulle reti sociali, con la conseguenza di limitare l'attività in rete.

Alla fine dello scorso anno *Human Rights Watch* [nota Ong britannica che si occupa di diritti umani, ndtr.] ha informato che Israele e Facebook spesso non fanno

alcuna differenza tra critiche legittime a Israele e istigazione all'odio. Al contrario, mentre Israele svolta sempre più a destra, il governo Netanyahu e le reti sociali non hanno bloccato l'ondata di messaggi in ebraico che incitano all'odio e alla violenza contro i palestinesi. Come ha rilevato 7anleh, contenuti razzisti o che incitano alla violenza contro i palestinesi sono pubblicati da israeliani quasi ogni minuto.

Account di agenzie di stampa chiusi

Oltre a cancellare decine di migliaia di post di palestinesi, Israele ha convinto Facebook a ritirare gli account delle agenzie di stampa e di giornalisti palestinesi di spicco.

Nel 2018 l'opinione pubblica palestinese si è talmente indignata che, con l'hashtag #FBcensorsPalestine, è stata lanciata una campagna di proteste in rete e di appelli al boicottaggio di Facebook.

Nello stesso modo negli Stati Uniti e in Europa è stato preso di mira l'attivismo solidale con i palestinesi. Le pubblicità di film, come i film stessi, sono stati ritirati ed eliminati dai siti web.

In settembre Zoom, un sito di videoconferenze che ha conosciuto un boom durante la pandemia di COVID-19, si è unito a YouTube e Facebook per censurare un webinar organizzato dall'università statale di San Francisco con la partecipazione di Leila Khaled, icona del movimento della resistenza palestinese, che oggi ha 76 anni.

A fine ottobre Zoom ha bloccato una seconda apparizione prevista di Khaled, questa volta in un webinar dell'università delle Hawaii e dedicato alla censura, come una serie di altri eventi organizzati negli Stati Uniti per protestare contro la sua cancellazione da parte del sito. Con un comunicato pubblicato riguardo alla giornata di lotta, i campus "si sono uniti alla campagna per resistere al soffocamento dei discorsi e delle voci palestinesi nelle imprese e nelle università."

Questa decisione, che costituisce un attacco flagrante alla libertà accademica, sarebbe stata presa in seguito a forti pressioni esercitate sulle reti sociali dal governo israeliano e da gruppi di pressione antipalestinesi, che hanno giudicato "antisemita" il webinar.

Villaggi cancellati dalla mappa

Il livello in cui la discriminazione dei giganti tecnologici contro i palestinesi è strutturale e radicato è stato messo in evidenza dalla lotta condotta da molti anni dagli attivisti per includere i villaggi palestinesi nelle mappe in rete e sui GPS, ma anche per attribuire ai territori palestinesi il nome di "Palestina", in base al riconoscimento della Palestina da parte delle Nazioni Unite.

Questa campagna segna notevolmente il passo, anche se più di un milione di persone ha firmato una petizione di protesta. Sia Google che Apple resistono strenuamente a queste richieste: centinaia di villaggi palestinesi non compaiono sulle loro mappe della Cisgiordania occupata, mentre le illegali colonie israeliane sono identificate nel dettaglio e viene loro accordato lo stesso status delle comunità palestinesi che vi si trovano.

I territori palestinesi occupati sono indicati sotto il nome di "Israele", mentre Gerusalemme est viene presentata come la capitale unificata e indiscussa di Israele, come esso pretende, cosa che rende invisibile l'occupazione della parte palestinese della città.

Queste decisioni sono tutt'altro che neutrali sul piano politico. Da molto tempo i governi israeliani perseguono un'ideologia del "Grande Israele" che esige di cacciare i palestinesi dalle loro terre. Questo programma di spoliazione, inteso ad annettere intere parti della Cisgiordania, quest'anno è stato formalizzato dai progetti sostenuti dall'amministrazione Trump.

Nei fatti Google ed Apple sono conniventi con questa politica, contribuendo a cancellare la presenza visibile dei palestinesi nella loro patria. Come di recente hanno evidenziato George Zeidan ed Haya Haddad, due accademici palestinesi, "quando Google ed Apple cancellano dei villaggi palestinesi dal loro sistema di navigazione identificando in evidenza le colonie, si rendono complici del discorso nazionalista israeliano."

Rapporti usciti dall'ombra

I rapporti sempre più stretti tra Israele e le imprese delle reti sociali si giocano in gran parte dietro le quinte. Ma questi legami sono usciti dall'ombra in modo decisivo lo scorso maggio, quando Facebook ha annunciato che il suo nuovo organo di vigilanza include Emi Palmor, una degli architetti della politica repressiva

in rete condotta da Israele contro i palestinesi.

Questo organo di vigilanza prenderà decisioni che faranno giurisprudenza e contribuiranno a forgiare le politiche di Facebook e di Instagram in tema di censura e di libertà d'espressione. Ma in quanto ex-direttrice generale del ministero della Giustizia [israeliano], Emi Palmor non ha dimostrato alcun impegno in favore della libertà d'espressione in rete.

Al contrario: ha lavorato mano nella mano con i giganti della tecnología per censurare i post dei palestinesi e chiudere i siti d'informazione palestinesi. Ha supervisionato la trasformazione del suo dipartimento in quello che l'organizzazione per la difesa dei diritti dell'uomo *Adalah* ha paragonato al "ministero della Verità" orwelliano.

Le imprese tecnologiche sono ormai arbitre non dichiarate della nostra libertà d'espressione, motivate dal profitto. Non si impegnano a favore di un dibattito pubblico aperto e vivace, di una trasparenza in rete o di una maggiore partecipazione civica. Il loro unico impegno consiste nel mantenere un contesto commerciale che permetta loro di evitare che le norme decise dai principali governi danneggino il loro diritto a guadagnare dei soldi.

La nomina di Palmor evidenzia perfettamente il rapporto inficiato dalla corruzione tra il governo e le reti sociali. I palestinesi sanno benissimo come sia facile per l'industria tecnologica attenuare e far sparire le voci dei deboli e degli oppressi amplificando nel contempo quelle dei potenti.

Molti di noi potrebbero presto conoscere in rete la stessa sorte dei palestinesi.

– Jonathan Cook è un giornalista inglese che vive a Nazareth dal 2001. Ha scritto tre opere sul conflitto israelo-palestinese ed ha ottenuto il premio speciale del giornalismo Martha Gellhorn.

Le opinioni espresse in questo articolo sono dell'autore e non riflettono necessariamente la politica editoriale di Middle East Eye.

(traduzione dal francese di Amedeo Rossi)

Come le tecnologie dello spionaggio israeliano penetrano in modo molto intrusivo nelle nostre vite

Jonathan Cook

Martedì 26 novembre 2019 – Middle East Eye

Israele normalizza nei Paesi occidentali l'uso di tecnologie invasive e oppressive di cui i palestinesi sono vittime da decine di anni

Le armi dell'era digitale sviluppate da Israele per opprimere i palestinesi sono rapidamente riutilizzate in un campo di applicazione molto più ampio, e ciò contro le popolazioni occidentali che considerano tuttavia le loro libertà come acquisite.

Se a Israele già da parecchi anni è stato concesso lo status di "Nazione delle start up", la sua reputazione nel campo delle innovazioni di tecnologia avanzata si è sempre basata su un aspetto oscuro che è vieppiù difficile nascondere.

Qualche anno fa l'analista israeliano Jeff Halper avvertì che Israele aveva giocato un ruolo centrale sulla scena internazionale nella fusione tra le nuove tecnologie digitali e dell'industria della sicurezza interna. Secondo lui il pericolo era che saremmo tutti quanti diventati progressivamente dei palestinesi.

Egli notava che Israele ha effettivamente trattato milioni di palestinesi sottoposti al suo regime militare come delle cavie in laboratori a cielo aperto – e ciò senza doverne rendere conto. I territori palestinesi occupati sono serviti come banco di prova per la messa a punto non solo dei nuovi sistemi d'arma convenzionali, ma anche di nuovi strumenti per la sorveglianza ed il controllo di massa.

Come ha recentemente osservato un giornalista di Haaretz [giornale israeliano di centro sinistra, ndtr.], l'operazione di sorveglianza condotta da Israele contro i palestinesi figura "tra le più vaste di questo tipo al mondo. Include la sorveglianza dei media, delle reti sociali e della popolazione nel suo insieme."

Il Grande Fratello fa affari

Tuttavia quello che è iniziato nei territori occupati non doveva affatto essere limitato alla Cisgiordania, a Gerusalemme est e a Gaza. C'erano semplicemente troppo denaro e influenza da guadagnare commercializzando queste nuove forme ibride di tecnologia digitale offensiva.

Per quanto piccolo sia, Israele è da molto tempo uno dei leader mondiali sul mercato estremamente lucrativo degli armamenti e vende a regimi autoritari i suoi sistemi d'arma "testati sul campo di battaglia", cioè sui palestinesi.

Ora, questo commercio di materiale militare è sempre più eclissato dal mercato dei programmi digitali bellici, cioè gli strumenti che servono a condurre guerre informatiche.

Queste armi di nuova generazione sono molto richieste dagli Stati, che possono utilizzarle non solo contro nemici esterni, ma anche contro dissidenti interni, che siano difensori dei diritti umani o semplici cittadini. Israele può presentarsi a giusto titolo come un'autorità mondiale in questa materia, nella misura in cui controlla ed opprime le popolazioni che vivono sotto il suo dominio. Ma il Paese ha fatto attenzione a non lasciare le sue impronte digitali su gran parte di questa nuova tecnologia degna del Grande Fratello, scegliendo di esternalizzare lo sviluppo di questi strumenti informatici affidandoli agli ufficiali di alto rango delle sue tristemente celebri unità per la sicurezza e l'intelligence militare.

Tuttavia Israele approva implicitamente queste attività fornendo licenze d'esportazione alle imprese che le gestiscono. D'altro canto i maggiori responsabili della sicurezza del Paese sono spesso strettamente legati al lavoro di queste aziende.

Tensioni con la Silicon Valley

Una volta smessa l'uniforme, questi israeliani possono trarre profitto dai loro anni d'esperienza nel campo dello spionaggio a danno dei palestinesi, creando società il cui obiettivo è sviluppare dei programmi informatici per delle applicazioni più generali.

Queste app, che utilizzano una tecnologia di sorveglianza sofisticata di origine israeliana, sono sempre più frequenti nelle nostre vite digitali. Alcune sono state utilizzate in modo relativamente innocuo. "Waze", che sorveglia gli ingorghi del traffico, permette ai conducenti di raggiungere la propria destinazione più rapidamente, mentre "Gett" attraverso il loro telefono mette i clienti in contatto con i taxi che si trovano nei dintorni.

Ma alcune delle tecnologie più segrete prodotte dagli sviluppatori israeliani rimangono molto più vicine al loro format militare originario.

Questi programmi offensivi sono venduti ai Paesi che desiderano spiare i loro stessi cittadini o Stati nemici, come anche a società private che sperano così di conquistarsi un notevole vantaggio sui concorrenti o di manipolare e sfruttare meglio dal punto di vista commerciale i loro clienti.

Una volta integrati nelle piattaforme delle reti sociali, che contano miliardi di utenti, questi programmi spionistici offrono ai servizi statali della sicurezza un raggio d'azione potenziale quasi universale. Ciò implica una relazione a volte tesa tra le società israeliane e la Silicon Valley [centro di ideazione e produzione delle innovazioni digitali negli USA, ndtr.], con quest'ultima che lotta per prendere il controllo di questi programmi "malintenzionati" – come dimostrano due esempi diversi dell'attualità recente.

"Sistema di spionaggio" per telefonini

Indice di queste tensioni, WhatsApp, una piattaforma di reti sociali appartenente a Facebook, molto di recente ha intentato il primo processo di questo tipo davanti a un tribunale californiano contro NSO, la più grande impresa di sorveglianza israeliana.

WhatsApp accusa NSO di attacchi informatici. Nel lasso di tempo di sole due settimane fino all'inizio di maggio esaminato da WhatsApp, NSO avrebbe preso di

mira i telefonini di più di 1.400 utenti in 20 Paesi.

Il programma di spionaggio digitale di NSO, chiamato “Pegasus”, è stato utilizzato contro difensori dei diritti umani, avvocati, responsabili religiosi, giornalisti e operatori umanitari. La Reuter [agenzia di stampa inglese, ndtr.] ha rivelato alla fine di ottobre che alti responsabili di Paesi alleati degli Stati Uniti sarebbero stati anche loro presi di mira da NSO.

Dopo aver preso il controllo del telefono di un utente a sua insaputa, “Pegasus” ne copia i dati e attiva il microfono dell’apparecchio al fine di controllarlo. La rivista “Forbes” [rivista USA di economia, ndtr.] lo ha descritto come “il sistema di spionaggio mobile più invasivo al mondo”.

NSO ha concesso la licenza di utilizzazione del programma a decine di governi, in particolare a regimi noti per le violazioni dei diritti umani come l’Arabia Saudita, il Bahrein, gli Emirati Arabi Uniti, il Kazakistan, il Messico e il Marocco. Amnesty International si è lamentata che i suoi funzionari figurano tra le persone prese di mira dal programma spia di NSO. L’Ong per la difesa dei diritti dell’uomo attualmente sostiene un’azione legale contro il governo israeliano perché ha concesso alla società una licenza d’esportazione.

Rapporti con i servizi di sicurezza israeliani

NSO è stata fondata nel 2010 da Omri Lavie e Shalev Hulio, entrambi ufficiali della famosa Unità 8200 di intelligence militare israeliana. Nel 2014 degli informatori che hanno lanciato l’allarme hanno rivelato che l’unità spiava regolarmente i palestinesi, cercando nei loro telefoni e computer delle prove di comportamenti sessuali devianti, di problemi di salute o di difficoltà finanziarie che potevano essere utilizzate per spingerli a collaborare con le autorità militari israeliane.

I soldati hanno scritto che i palestinesi erano “totalmente esposti allo spionaggio e alla sorveglianza dei servizi di intelligence israeliani. Questi sono utilizzati per perseguitare gli avversari politici e per creare divisioni all’interno della società palestinese reclutando collaboratori e spingendo le diverse componenti della società palestinese le une contro le altre.”

Benché le autorità abbiano concesso a NSO delle licenze d'esportazione, Ze'ev Elkin [del partito di destra Likud, ndtr.], ministro israeliano per la Protezione dell'Ambiente, per Gerusalemme e per l'Integrazione, ha negato "il coinvolgimento del governo israeliano" nello spionaggio di WhatsApp. "Tutti capiscono che non si tratta dello Stato d'Israele," ha dichiarato a una radio israeliana all'inizio di novembre.

Inseguiti dalle telecamere

La settimana in cui WhatsApp ha lanciato la sua azione legale, la catena televisiva americana NBC ha rivelato che la Silicon Valley intende comunque lavorare con delle start-up israeliane profondamente coinvolte negli abusi legati all'occupazione.

Microsoft ha investito parecchio in AnyVision, una società che sviluppa una sofisticata tecnologia di riconoscimento facciale usata dall'esercito israeliano per opprimere i palestinesi.

I rapporti tra AnyVision e i servizi di sicurezza israeliani sono a malapena nascosti. Il consiglio consultivo della società conta tra i suoi membri Tamir Pardo, ex-capo del Mossad, l'agenzia di spionaggio israeliana. Il suo presidente, Amir Kain, era in precedenza alla testa del "Malmab", il dipartimento del ministero della Difesa israeliano incaricato della sicurezza.

Il principale programma di AnyVision, "Better Tomorrow" [Futuro Migliore], è stato soprannominato "Google dell'Occupazione", perché la società sostiene che può identificare e seguire qualunque palestinese grazie alle immagini prodotte dalla vasta rete di telecamere di sorveglianza sistemate dall'esercito israeliano nei territori occupati.

A dispetto degli evidenti problemi etici, l'investimento di Microsoft suggerisce che il suo obiettivo potrebbe essere integrare questo programma all'interno dei suoi. Ciò ha provocato viva preoccupazione tra i gruppi di difesa dei diritti umani.

Shankar Narayan, dell'American Civil Liberties Union [ACLU, ong Usa per la difesa dei diritti e delle libertà individuali, ndtr.], ha messo in guardia in particolare contro un avvenire fin troppo familiare ai palestinesi che vivono sotto

il controllo di Israele: “L’uso generalizzato della sorveglianza facciale sovverte il principio di libertà e genera una società in cui tutti sono seguiti in continuazione, indipendentemente da quello che fanno,” ha dichiarato alla NBC.

“Il riconoscimento facciale è forse lo strumento più perfetto per il controllo totale del governo nei luoghi pubblici.”

Secondo Yael Berda, ricercatore dell’università di Harvard, Israele dispone di una lista di circa 200.000 palestinesi in Cisgiordania che desidera sorvegliare 24 ore al giorno. Le tecnologie come AvyVision sono considerate essenziali per mantenere questo vasto gruppo sotto una sorveglianza continua.

Un ex dipendente di AvyVision ha dichiarato alla NBC che i palestinesi sono stati trattati come cavie. “La tecnologia è stata testata sul terreno in uno dei contesti della sicurezza più esigenti al mondo, e ora noi la utilizziamo sul resto del mercato,” ha dichiarato.

Il 15 novembre Microsoft ha annunciato il lancio di un’indagine sulle accuse secondo cui la tecnologia di riconoscimento facciale messa a punto da AnyVision violerebbe il suo codice etico a causa del suo utilizzo in operazioni di sorveglianza nella Cisgiordania occupata.

Interferenza nelle elezioni

Utilizzare queste tecnologie di spionaggio negli Stati Uniti e in Europa interessa sempre di più il governo israeliano stesso, nella misura in cui l’occupazione dei territori palestinesi è ormai oggetto di una polemica e di un controllo minuzioso nel discorso politico prevalente.

In gran Bretagna i cambiamenti di clima politico sono stati messi in evidenza dall’elezione alla testa del partito Laburista di Jeremy Corbyn, militante di lunga data per i diritti dei palestinesi. Negli Stati Uniti un piccolo gruppo di parlamentari che appoggiano in modo palese la causa palestinese ha di recente fatto il suo ingresso al Congresso, in particolare Rashida Tlaib, la prima donna americana-palestinese a occupare tale ruolo.

Più in generale Israele teme il BDS (Boicottaggio, Disinvestimento e Sanzioni), movimento di solidarietà internazionale che chiede un boicottaggio di Israele, sul

modello del boicottaggio contro il Sud Africa durante l'apartheid, finché non cesserà la repressione del popolo palestinese. Il BDS è in piena espansione, soprattutto negli Stati Uniti, dove si è notevolmente sviluppato in molti campus universitari.

Di conseguenza le imprese informatiche israeliane sono state coinvolte sempre di più nei tentativi intesi a manipolare il discorso pubblico su Israele, in particolare interferendo nelle elezioni all'estero.

Due esempi noti sono per breve tempo finiti sulle prime pagine. Psy-Group, che si presentava come un "Mossad privato in affitto", è stato chiuso l'anno scorso dopo che l'FBI ha aperto un'inchiesta su di esso per aver interferito nelle elezioni presidenziali americane del 2016. Secondo il New Yorker [prestigiosa rivista USA, ndtr.], il suo "Project Butterfly" [Progetto Farfalla] intendeva "destabilizzare e sconvolgere i movimenti antisraeliani dall'interno."

E l'anno scorso la società "Black Cube" [Cubo Nero] è stata accusata di controllo ostile su importanti membri della precedente amministrazione americana guidata da Barack Obama. "Black Cube" sembra essere strettamente legata alle aziende della sicurezza e per un certo periodo i suoi uffici sono stati dislocati in una base militare israeliana.

Vietato da Apple

Un certo numero di altre aziende israeliane cerca di attenuare la distinzione tra spazio privato e spazio pubblico.

"Onavo", una società israeliana di raccolta dati creata da due veterani dell'Unità 8200, è stata acquistata da Facebook nel 2013. L'anno dopo Apple ha vietato la sua applicazione VPN dopo che è stato rivelato che offriva un accesso illimitato ai dati degli utenti.

Secondo un articolo di Haaretz, l'anno scorso il ministro israeliano degli Affari Strategici, Gilad Erdan, che dirige una campagna segreta intesa a demonizzare i militanti del BDS all'estero, ha tenuto regolarmente riunioni con un'altra società, "Concert". Questo gruppo segreto, esentato dalle leggi israeliane sulla libertà d'informazione, ha ricevuto circa 36 milioni di dollari di finanziamenti da parte

del governo israeliano. I suoi dirigenti e i suoi azionisti sono “la crema” dell’élite israeliana per la sicurezza e l’intelligence.

Un’altra società israeliana di primo piano, “Candiru” – che deve il suo nome a un piccolo pesce amazzonico famoso per infiltrarsi segretamente nel corpo umano, dove diventa un parassita – vende principalmente i propri strumenti di pirateria informatica ai governi occidentali, anche se le sue operazioni sono circondate dal segreto.

Il suo personale proviene quasi esclusivamente dall’Unità 8200. A prova dello stretto rapporto tra le tecnologie pubbliche e segrete sviluppate dalle aziende israeliane, il direttore generale di “Candiru”, Eitan Achlow, dirigeva in precedenza “Gett”, l’applicazione dei servizi per i taxi.

L’élite della sicurezza israeliana trae profitto da questo nuovo mercato della guerra informatica, sfruttando – come ha fatto per il commercio di armamenti convenzionali – una popolazione palestinese a sua disposizione e prigioniera su cui può testare la sua tecnologia.

Non è sorprendente che Israele renda progressivamente normale nei Paesi occidentali l’uso di tecnologie invasive e oppressive, di cui i palestinesi sono le vittime da decine di anni.

I programmi di riconoscimento facciale permettono una profilazione razziale e politica sempre più sofisticata. Le operazioni segrete e la raccolta dati e di sorveglianza cancellano le tradizionali frontiere tra gli spazi privati e quelli pubblici. E le campagne di raccolta di informazioni che ne sono il risultato permettono d’intimidire, minacciare e screditare gli oppositori o chi, come la comunità dei difensori dei diritti umani, cerca di mettere i potenti di fronte alle loro responsabilità.

Se questo avvenire distopico continua a svilupparsi, New York, Londra, Berlino e Parigi assomiglieranno sempre di più a Nablus, Hebron, Gerusalemme est e Gaza. E noi finiremo tutti col capire cosa significhi vivere in uno Stato di polizia impegnato in una guerra informatica contro quelli che domina.

Jonathan Cook è un giornalista britannico residente dal 2001 a Nazareth. Ha

scritto tre libri sul conflitto israelo-palestinese. È stato vincitore del Martha Gellhorn Special Prize for Journalism.

Le opinioni espresse in questo articolo impegnano solo il suo autore e non riflettono necessariamente la politica editoriale di Middle East Eye.

(traduzione dall'inglese di Amedeo Rossi)

La sorveglianza sui palestinesi e la lotta per i diritti digitali

Nadim Nashif

23 ottobre 2017, Al-Shabaka

Sintesi

La sorveglianza sui palestinesi è sempre stata parte integrante del progetto coloniale israeliano. Prima della creazione dello Stato di Israele, squadre del gruppo paramilitare sionista Haganah percorrevano i villaggi e le città palestinesi, raccogliendo informazioni sui residenti. Questo controllo sulle vite dei palestinesi è continuato dopo l'occupazione israeliana delle Alture del Golan, della Striscia di Gaza e della Cisgiordania, inclusa Gerusalemme est, nel 1967. Gli strumenti utilizzati comprendevano registri della popolazione, carte di identificazione, rilevamenti catastali, torri di controllo, incarcerazione e tortura.

Benché queste tecniche di controllo poco sofisticate siano ancora oggi in uso, una vasta gamma di nuove tecnologie, come il monitoraggio e l'intercettazione per telefono e via internet, la CCTV [televisione a circuito chiuso, ndt.] e la banca dati

biometrici, ha messo in grado Israele di sorvegliare la popolazione sotto occupazione su scala massiccia e pervasiva. Israele utilizza in particolare i social media per monitorare ciò che i singoli palestinesi dicono e fanno e per raccogliere ed analizzare informazioni sui comportamenti della popolazione palestinese in generale.

In questo documento Nadim Nashif discute l'uso da parte di Israele dei social media come strumento di controllo dei palestinesi. (1) Prende in esame le tattiche israeliane e gli altri ostacoli digitali ai diritti dei palestinesi, inclusa la parzialità di Facebook a favore di Israele attraverso la censura e la mancanza di trasparenza, nonché la nuova legge sui crimini informatici dell'Autorità Nazionale Palestinese (ANP). Nashif conclude fornendo suggerimenti su come i palestinesi possono contrapporsi all'uso dei social media per la sorveglianza e proteggere i propri diritti informatici.

I social media come ambito di sorveglianza

L'esplosione di rabbia palestinese iniziata nell' ottobre 2015 in risposta alle incursioni israeliane alla Moschea di Al-Aqsa ha rappresentato una nuova sfida per l'apparato di sicurezza israeliano. Storicamente, gli individui affiliati ai bracci militari delle fazioni palestinesi, come Fatah, Hamas e il Fronte Popolare per la Liberazione della Palestina, hanno condotto attacchi ai quali Israele ha risposto con la violenza, la distruzione e le punizioni collettive. Per esempio, Israele ha scatenato le sue ultime tre guerre nella Striscia di Gaza, nel 2009, 2012 e 2014, con il pretesto di fermare i lanci di razzi da parte di Hamas.

Questa volta, tuttavia, sono stati adolescenti palestinesi, molti dei quali non appartengono ad alcuna fazione politica o ala militare palestinese, a sferrare gli attacchi. Il governo israeliano ha accusato i social media per questa nuova tendenza e l'intelligence militare israeliana ha rafforzato il monitoraggio degli account dei social media palestinesi. In seguito a ciò, Israele ha arrestato 800 palestinesi a causa dei loro post sui social media, soprattutto su Facebook, la piattaforma più seguita dai palestinesi.

All'inizio di quest'anno Haaretz ha rivelato che questi arresti sono il risultato di un metodo poliziesco basato su algoritmi che creano profili di quelli che Israele vede come probabili attentatori palestinesi. Il programma monitora decine di migliaia di account Facebook di giovani palestinesi, cercando termini come

shaheed (martire), Stato sionista, Al Quds (Gerusalemme) o Al Aqsa. Ricerca anche account che postano foto di palestinesi recentemente uccisi o imprigionati da Israele. Il sistema identifica quindi i "sospetti" basandosi su un possibile atto di violenza, piuttosto che su un attacco reale – o almeno su un piano per realizzare un attacco.[vedi zeitun.info]

Ogni profilo Facebook segnalato come sospetto dal sistema è un potenziale bersaglio di un arresto e la principale accusa di Israele alle persone arrestate è "incitamento alla violenza". Poiché l'incitamento è definito in modo vago, il termine include tutte le forme di resistenza alle politiche ed alle pratiche israeliane. La "popolarità", o il livello di influenza che una persona esercita sui social media, è un fattore che conta nella decisione di Israele di sporgere denuncia contro i palestinesi accusati di incitamento. Per esempio, più alto è il numero di 'like', di commenti e di condivisioni che ha un'utenza, maggiore è la possibilità che le persone vengano denunciate – e più lunga e pesante sarà la condanna.

L'intelligence israeliana inoltre crea falsi account Facebook per tracciare e ottenere accesso a profili Facebook per poter comunicare con palestinesi e ricavare informazioni private che altrimenti essi non condividerebbero. Nell'ottobre 2015, per esempio, parecchi attivisti palestinesi hanno riferito di aver ricevuto messaggi da account Facebook con nomi arabi e fotografie di bandiere palestinesi, che chiedevano i nomi dei palestinesi che partecipano alle proteste.

Inoltre Israele si introduce negli account Facebook per accedere ad informazioni private, come l'orientamento sessuale, le condizioni di salute e mentali e lo status coniugale e finanziario. Un veterano dell'Unità 8200, un corpo d'elite dell'intelligence dell'esercito israeliano, spesso paragonato all'Agenzia per la Sicurezza Nazionale USA, ha testimoniato che questo materiale viene raccolto come mezzo di pressione. "Ogni informazione che possa consentire di ricattare una persona è considerata un'informazione rilevante", ha detto. " Sia che tale individuo abbia un certo orientamento sessuale, tradisca sua moglie o necessiti di cure in Israele o in Cisgiordania – è un bersaglio per essere ricattato." L'intelligence israeliana ha preso di mira soprattutto palestinesi omosessuali, minacciando di pubblicare le loro foto intime per costringerli a collaborare con Israele.

Una simile intrusione nella vita privata dei palestinesi è resa possibile dal fatto

che Israele occupa e controlla l'intera infrastruttura delle telecomunicazioni usata dalle compagnie e dai gestori del servizio di internet palestinesi. La mancanza di qualunque limitazione legale o etica sul punto fino al quale Israele può spingersi nella sorveglianza sui palestinesi nel 2014 ha addirittura portato 43 veterani dell'Unità 8200 ad inviare una lettera al primo ministro israeliano Benjamin Netanyahu per contestare "il continuo controllo di milioni di persone ed un'intrusione profondamente invasiva in quasi tutti gli ambiti della vita."

Il complesso militare industriale del Paese è uno strumento ancor più pervasivo per il controllo digitale sui palestinesi. Israele produce ed esporta un'enorme quantità di tecnologie di sicurezza militare e cibernetica. Secondo un rapporto del 2016 di 'Privacy International', una Ong che indaga sui controlli da parte del governo e sulle imprese che lo consentono, Israele è la sede di 27 imprese di sorveglianza – il più alto numero pro capite di tutti i Paesi del mondo. Nel 2014 le esportazioni israeliane di tecnologie di sicurezza informatica e di sorveglianza all'estero, come il monitoraggio di telefoni e internet, hanno superato le esportazioni di armamenti. Queste tecnologie sono state vendute a regimi autoritari e repressivi in Colombia, Kazakhstan, Messico, Sud Sudan, Emirati Arabi Uniti e Uzbekistan, tra gli altri.

Ambigui legami tra l'esercito israeliano ed il settore tecnologico rafforzano l'importanza del Paese nell'industria della sorveglianza. I veterani dell'Unità 8200 hanno fondato alcune delle principali compagnie israeliane di sicurezza informatica, come le imprese Mer e NSO. I veterani trasferiscono le loro competenze militari e di intelligence sviluppate nell'unità di elite al settore privato, dove non ci sono ostacoli legali relativamente alla sovrapposizione tra industria militare e di sorveglianza.

Facebook: neutrale o di parte?

Facebook si pubblicizza come una piattaforma aperta, al servizio di tutti. Il fondatore e amministratore delegato di Facebook, Mark Zuckerberg, ha detto recentemente: "Lavoro ogni giorno per unire le persone e creare una comunità per tutti. Speriamo di dare voce a tutto il popolo e di creare una piattaforma per tutte le idee."

Gli affari del gigante dei social media con Israele mettono in discussione tale affermazione. Mentre Facebook ha dei chiari protocolli e meccanismi per le

richieste da parte di governi di rimuovere contenuti, e addirittura pubblica un rapporto biennale delle richieste dei governi, l'azienda viene spesso criticata per la sua mancanza di trasparenza e le sue decisioni arbitrarie. Un'inchiesta del *Guardian* ha rivelato le norme riservate di Facebook per limitare argomenti relativi a violenze, discorsi di odio, terrorismo e razzismo – norme che dimostrano la sua parzialità a favore di Israele.

Per esempio, Facebook segnala i sionisti come "gruppo globalmente protetto", il che significa che i contenuti che li attaccano devono essere rimossi. Un'altra regola spiega che "le persone non devono elogiare, sostenere o raffigurare un membro…di un'organizzazione terrorista, o di qualunque organizzazione che abbia lo scopo principale di intimidire una popolazione, un governo, o di usare violenza per resistere all'occupazione di uno Stato riconosciuto a livello internazionale." Di conseguenza, Facebook ha censurato attivisti e giornalisti in territori oggetto di disputa, come Palestina, Kashmir, Crimea e Sahara occidentale. Secondo rapporti dei media, Facebook ha rivisto la definizione di terrorismo per includervi l'uso di violenza premeditata da parte di organizzazioni non governative "allo scopo di raggiungere un obiettivo politico, religioso o ideologico." In ogni caso, la definizione permette di punire coloro che resistono all'occupazione e all'oppressione, mentre non include il terrorismo di Stato e la violenza inflitti ai palestinesi da parte di Israele.

Inoltre nel 2016 la ministra della Giustizia Ayelet Shaked ed il ministro della Pubblica Sicurezza Gilad Erdan hanno annunciato un accordo tra Israele e Facebook per creare delle squadre di monitoraggio e rimozione dei contenuti "che favoriscono l'incitamento [alla violenza]".

Il direttore politico di Facebook, Simon Milner, nega l'esistenza di qualunque accordo speciale tra il suo datore di lavoro e Israele. Ha anche ribadito che tutti gli utenti di Facebook sono soggetti alle stesse politiche per la comunità di utilizzatori. Tuttavia un recente rapporto di Adalah [*organizzazione per i diritti umani e centro legale per i diritti degli arabi in Israele, ndtr.*] rivela che fin dalla seconda metà del 2015 l'ufficio del procuratore generale di Israele ha gestito un'unità informatica in collaborazione con Facebook e Twitter, per rimuovere contenuti online. Il resoconto finale annuale del 2016 dell'unità si fa vanto di aver trattato 2.241 casi e rimosso il contenuto in 1.554 di essi.

La collaborazione tra Israele e Facebook è dovuta probabilmente a molteplici

ragioni. Anzitutto Israele ha una fiorente industria di alta tecnologia e rappresenta un lucroso mercato per Facebook. In secondo luogo, l'ufficio di Facebook a Tel Aviv rende la compagnia più soggetta all'influenza dei decisori israeliani. La nomina di Jordana Cutler, da lungo tempo principale consigliera di Netanyahu, a capo della politica e comunicazione di Facebook nell'ufficio israeliano è un caso emblematico.

Terzo, forse Facebook teme azioni legali. Nel 2015 un'organizzazione filoisraeliana, 'Shurat HaDin-Israel Law Center', ha intentato una causa contro Facebook negli Stati Uniti a nome di 20.000 querelanti israeliani, che accusavano la compagnia di "incitamento ed incoraggiamento alla violenza contro gli israeliani." Il timore di Facebook di un'azione legale è espresso in un documento interno, che è trapelato, relativo ad un contenuto negazionista dell'Olocausto. Il documento spiega che Facebook semplicemente nasconderà o rimuoverà tale contenuto in quattro Paesi – Austria, Francia, Germania e Israele – per evitare cause legali.

Infine, benché Facebook neghi ogni discriminazione tra palestinesi ed israeliani, gli utenti palestinesi raccontano una storia diversa. Per esempio, poco dopo che una delegazione di Facebook aveva incontrato rappresentanti del governo israeliano nel settembre 2016, gli attivisti palestinesi hanno documentato interruzioni degli account personali su Facebook di giornalisti e di organizzazioni di informazione. Gli account di quattro giornalisti dell'agenzia di notizie palestinese Shehab e di tre giornalisti della rete Al Quds News sono stati chiusi. In seguito a proteste online e campagne con gli hashtag #FBCensorsPalestine e #FacebookCensorsPalestine, Facebook si è scusata per l'interruzione, spiegando che si era trattato di un errore.

La nuova legge sui crimini informatici dell'Autorità Nazionale Palestinese

Non è soltanto Israele a reprimere gli utenti palestinesi dei social media: lo fa anche l'ANP, per cassare opinioni politiche sfavorevoli o critiche verso la leadership palestinese. Tuttavia c'è una differenza fondamentale tra la portata del controllo digitale israeliano e le violazioni della libertà di espressione online da parte dell'ANP. Mentre il controllo digitale globale di Israele fa di ogni palestinese un sospetto ed un bersaglio, l'ANP utilizza le informazioni condivise pubblicamente per prendere di mira il dissenso politico.

L’ANP ha recentemente approvato una legge che limita ancor di più la libertà dei palestinesi di esprimersi online. La controversa legge sui crimini informatici è stata firmata dal Presidente palestinese Mahmoud Abbas il 24 giugno 2017, senza alcuna consultazione pubblica con le organizzazioni della società civile palestinese o con i gestori dei servizi internet. E’ stata pubblicata con decreto presidenziale due settimane dopo la firma ed è entrata immediatamente in vigore.

Il pretesto della nuova legge è quello di combattere i reati informatici come l’estorsione per motivi sessuali, la frode fiscale e il furto di identità. Però l’utilizzo di termini vaghi come “armonia sociale”, “modalità pubbliche”, “sicurezza dello Stato” e “ordine pubblico” indica che la legge ha scopi differenti, in particolare eliminare la libertà di espressione online e reprimere ogni critica politica. Essa rende gli utenti palestinesi di internet, specialmente gli attivisti e i giornalisti, passibili di incriminazione da parte dell’ANP, che può interpretare le disposizioni della legge come vuole.

I primi due casi intentati in base alla legge rivelano il suo scopo. In entrambi è stato utilizzato l’art. 20, che stabilisce che ogni utente di internet che possiede o gestisce un sito web che pubblica “notizie che mettono a rischio la sicurezza dello Stato, il suo ordine pubblico, o la sicurezza interna o esterna” può essere arrestato per un anno o multato fino a circa 1.400 dollari. Nel primo caso sono stati arrestati sei giornalisti palestinesi che lavorano per organi di stampa legati ad Hamas in Cisgiordania. Nel secondo caso, i servizi di sicurezza preventiva dell’ANP hanno arrestato Issa Amro, importante difensore dei diritti umani ed attivista politico nonviolento palestinese di Hebron, che aveva protestato con un post su Facebook per l’arresto da parte dell’ANP di un giornalista.

La legge è in netto contrasto con la legge fondamentale di tutela della privacy e della libertà di espressione. Conferisce alle istituzioni dello Stato un ampio potere di monitoraggio, raccolta e conservazione di dati relativi alle attività online di palestinesi nei Territori Palestinesi Occupati (TPO), e di fornire, su loro richiesta, tali informazioni alle autorità preposte all’applicazione della legge. Anche i gestori privati del servizio internet sono obbligati a cooperare con le agenzie di sicurezza raccogliendo, conservando e condividendo i dati informativi sugli utenti per almeno 3 anni, oltre che bloccando qualunque sito web su ordine della magistratura.

L’applicabilità della legge si estende oltre i confini legali dei territori controllati

dall'ANP e consente di perseguire palestinesi che vivono all'estero. Ciò costituisce una reale minaccia per gli attivisti politici palestinesi che vivono all'estero, ma che hanno una notevole influenza sui social media in patria. Comunque la legge non specifica se le autorità possano tentare di ottenere l'estradizione di palestinesi che risiedono all'estero per aver commesso un crimine informatico.

Contrastare il controllo digitale

Mentre la violazione dei diritti digitali dei palestinesi è un caso unico, data l'occupazione militare israeliana, la lotta per questi diritti è globale. I governi, le organizzazioni della società civile, le agenzie di social media e gli utenti di internet hanno tutti un ruolo importante nella protezione della libertà di espressione online e della privacy dal controllo e dalla censura dello Stato.

In Palestina l'ANP deve revocare immediatamente la legge sui crimini informatici. Per adempiere meglio allo scopo che esplicitamente si propone – combattere il crimine informatico – l'ANP dovrebbe consultare le organizzazioni della società civile ed altri importanti attori coinvolti per assicurarsi che ogni legge collegata all'informatica riduca effettivamente i crimini informatici senza violare i diritti politici dei palestinesi e le libertà pubbliche. Invece di reprimere i palestinesi per aver espresso le proprie opinioni politiche, l'ANP dovrebbe cercare di proteggere il suo popolo dagli arresti e dalle incriminazioni da parte di Israele con accuse senza fondamento di incitamento e terrorismo.

I diritti digitali, che sono parte del complesso dei diritti umani, sono un concetto relativamente nuovo nei Territori Palestinesi Occupati. Le organizzazioni palestinesi della società civile hanno la responsabilità di creare consapevolezza circa questi diritti, soprattutto riguardo alla sicurezza digitale. Proteggere gli account di un individuo e mantenere tali le informazioni private dovrebbe essere una priorità, soprattutto per giornalisti ed attivisti. Questo è particolarmente vero nel contesto di un'occupazione in cui l'occupante dispone di potenti capacità di controllo e controlla tutta l'infrastruttura delle telecomunicazioni.

La società civile palestinese ed i media devono anche smascherare e mobilitarsi contro le immorali pratiche di sorveglianza israeliane, la censura e la repressione della libertà di espressione dei palestinesi. Campagne online cresciute dal basso, come #FBCensorsPalestine e #FacebookCensorsPalestine, si sono dimostrate efficaci nell'attaccare le violazioni dei diritti digitali delle aziende di social media,

dovute a prese di posizione faziose, nonostante le dichiarazioni di neutralità. I palestinesi hanno anche bisogno di coalizzarsi con organizzazioni internazionali per i diritti digitali, che possono aiutare a fare pressione sulle aziende di social media e sul governo israeliano perché interrompano le violazioni.

Note:

1. Questo scritto si basa su una tavola rotonda organizzata nel maggio 2017 da Al-Shabaka e dalla Fondazione Heinrich Boell a Ramallah, in collaborazione con "7amleh: Centro arabo per lo sviluppo dei social media". Le opinioni espresse in questo scritto sono dell'autore e non riflettono necessariamente l'opinione della Fondazione Heinrich Boell

(Traduzione di Cristiana Cavagna)

Acquirente fai attenzione: l'impresa israeliana che aiuta i governi a spiare i loro stessi cittadini

Richard Silverstein ,martedì 22 agosto 2017, Middle East Eye

Consentendo ai governi di violare i telefoni dei loro cittadini, un'azienda israeliana di sicurezza informatica ha presumibilmente reso il mondo più pericoloso per gli attivisti a favore dei diritti umani che lottano contro l'impunità delle imprese e degli Stati.

Dato che negli ultimi anni gli smartphone si sono moltiplicati e sono diventati un mezzo di comunicazione indispensabile per tutti noi, si sono moltiplicate anche le

nuove aziende che si dedicano a violare questi telefoni a favore di governi – compresi i servizi militari, dello spionaggio e della polizia.

I clienti di queste imprese innovative utilizzano la nuova tecnologia per sorvegliare criminali e terroristi, per individuare e far fallire i loro piani. Questo è un uso legittimo. Ma ce ne sono altri che sono molto più redditizi per le imprese – e molto meno accettabili per le società democratiche.

Prendiamo per esempio l'attivista per i diritti umani degli Emirati [Arabi Uniti] Ahmed Mansoor. Nell'agosto 2016 ha ricevuto un messaggio ingannevole [phishing message] che sembrava provenire da una fonte fidata. Ma si è insospettito ed ha immediatamente inviato il suo telefono a "Citizen's Lab" [Laboratorio del Cittadino, centro studi interdisciplinare che si occupa del controllo sulle informazioni, ndt.] dell'università di Toronto per un'analisi forense.

Da questa verifica è risultato che le autorità degli Emirati si erano procurate "Pegasus", il più potente programma di malware [sistemi usati per apportare modifiche indesiderate ad un apparecchio informatico, ndt.] mai creato che si possa trovare sul mercato e venduto dall'azienda israeliana "NSO Group".

Se Mansoor avesse aperto il link, esso avrebbe preso il controllo del suo telefono e consentito alla polizia di accedere non solo a tutto quanto vi si trovava (email, contatti e messaggi di testo, per esempio), ma anche alla macchina fotografica, al video e all'audio. La polizia avrebbe sentito e visto tutto quello che faceva e sarebbe stata in grado di prevenire ogni sua azione.

1. Attacchi di "Pegasus"

In un caso collegato del 2016, le autorità degli EAU hanno anche utilizzato "Pegasus" in un tentativo di intrusione che ha preso di mira il giornalista di MEE Rory Donaghy, che informava in modo critico sui soprusi del regime autocratico del Paese. Nel pieno di un'inchiesta su questo attacco, il "Citizen's Lab" ha scoperto che 1.100 attivisti e giornalisti del regno erano stati presi di mira allo stesso modo e che il governo aveva pagato a "NSO Group" 600.000 dollari per questi tentativi [di intercettazione].

Anche se è un prodotto commerciale, "Pegasus" – come molti altri strumenti simili per lo spionaggio ora sul mercato – è chiaramente anche un mezzo politico che

consente a regimi autoritari di spiare i propri cittadini.

Infatti potrei andare anche oltre e dire che “Pegasus” è spesso utilizzato come arma informatica offensiva usata dall’élite mondiale per proteggere i propri interessi e contrastare il legittimo controllo da parte delle Ong e di altre associazioni di attivisti.

“Il governo compra (la tecnologia) e può usarla come vuole,” ha detto a “HuffPost” Bill Marczak, un ricercatore di “Citizen’s Lab” che ha analizzato molte campagne di controllo che secondo lui sono state condotte con “Pegasus”.

“Sono praticamente dei mercanti di armi digitali.”

Nelle ultime settimane il gruppo finanziario privato che possiede “NSO Group”, valutato oggi 1 miliardo di dollari, ha cercato di vendere la compagnia, sollevando grandi questioni tra gli attivisti dei diritti digitali in merito a se un nuovo investitore ridurrà il sospetto uso del sistema di spionaggio dell’azienda contro dissidenti politici ed attivisti da parte di alcuni governi.

2. Dall’esercito alla tecnologia

Ci sono parecchie imprese che creano questo tipo di software maligni in vari Paesi, ma alcune di quelle di maggior successo sono israeliane.

Ciò è principalmente un risultato della “SIGINT-Unità 8200”, la più numerosa dell’esercito israeliano, che spia i segnali elettromagnetici, monitora, intercetta e sorveglia i nemici di Israele in Medio Oriente e in tutto il mondo.

I suoi ufficiali ricevono l’addestramento più sofisticato nello spionaggio ed uso dei segnali e creano la tecnologia più avanzata per farlo. Quando lasciano il servizio attivo trovano le porte aperte nel mondo tecnologico. Possono avere un lavoro molto ben remunerato nelle grandi imprese o utilizzare le competenze che hanno acquisito nell’esercito per fondare un’azienda innovativa propria.

Alcune delle aziende di maggiore successo includono Waze, Wix, Taboola, NICE Systems, Amdocs, Onavo (acquistata da Facebook per 150 milioni di dollari), Checkpoint, Mirabilis e Verint.

Molti dei progetti riguardano la sicurezza informatica, che è quello che l’ “Unità

8200” è stata costituita per debellare nei suoi tentativi di intercettare le comunicazioni delle forze nemiche di Israele. Alcune iniziative sono concentrate sulla protezione della sicurezza informatica. Questi sono i bravi, o i “cappelli bianchi” nella terminologia degli hacker.

Ma altri continuano lungo la direzione che gli hacker dell’”Unità 8200” perseguono durante il servizio militare: sono destinati ad aggirare le funzioni di sicurezza di vari sistemi.

Forse quella che ha avuto più successo tra queste imprese è “NSO Group” che si trova a Herziliya [importante università privata israeliana in stretti rapporti con i servizi di sicurezza, ndt.], il cui motto è “rendi il mondo un posto più sicuro.” Ma l’azienda ha reso sicuramente il mondo molto più pericoloso per un gran numero di attivisti politici e per i diritti umani che lottano contro l’impunità di imprese e governi.

3. Vulnerabilità da miliardi di dollari

“NSO” è stata fondata nel 2010 da due veterani dell’esercito israeliano, Shalev Hulio and Omri Lavie, che non erano stati nell’”Unità 8200” (nonostante informazioni in contrario). Secondo la rivista israeliana “Globes” [quotidiano di informazioni finanziarie, ndt], Lavie ha fatto il militare nei corpi di artiglieria e Hulio nel servizio di ricerca e soccorso.

Alle scuole superiori né Hulio né Lavie erano studenti particolarmente brillanti e, secondo le informazioni del “Globes”, hanno passato un sacco di tempo insieme sulla spiaggia. Dopo aver lasciato l’IDF, hanno deciso di diventare imprenditori di servizi in rete.

“NSO” è la loro terza e di gran lunga più importante iniziativa imprenditoriale di successo. Secondo i fondatori, la sua nascita è avvenuta per puro caso. Vari clienti avevano chiesto loro se ci fosse un modo per prendere il controllo di un cellulare senza avere accesso fisico all’apparecchio reale.

Benché avessero sentito dire che c’era [questa possibilità], non riuscivano a trovare nessun ingegnere informatico che avesse idea di come farlo, finché un giorno, seduti in un caffè, i due udirono per caso parlarne veterani dell’”Unità 8200”. Così nel 2010, proprio quando gli smartphone stavano per essere

trasformati da oggetti per un solo uso in apparecchi quotidiani potenti, multiuso e indispensabili, fondarono “NSO”.

Iniziarono a farsi una clientela tra le forze di polizia di vari Paesi, offrendo la possibilità di spiare criminali sospetti in modi che nessuno aveva mai previsto. Fondarono una succursale per le vendite negli USA, “WestBridge Technologies”, per incentivare la penetrazione commerciale in uno dei loro maggiori mercati potenziali.

Attraverso la “Francisco Partners”, la società di capitale di rischio che nel 2015 ha comprato “NSO”, questa è finita sotto l’egida di un’impresa che possiede una serie di altre compagnie di telecomunicazioni che hanno fornito informazioni sensibili per fare passi avanti nelle possibilità di hackeraggio. Per esempio, “Intelligence Online” [rivista informativa nel campo dell’informatica, ndt.] riporta che Boaz Goldman è presidente del consiglio di amministrazione di “Inno Networks”, che installa reti di comunicazione mobile (3G e 4G). E’ appena entrato nel consiglio di amministrazione di una holding con sede in Lussemburgo che include “NSO Group” in un complicato rapporto finanziario. Questo accordo d’affari fornisce all’azienda di armi informatiche un accesso diretto a grandi reti (SS7 – Signal System 7) utilizzate per trasmettere testi, email, chiamate telefoniche, dati di geo-localizzazione e chiavi di cifratura.

“NSO” ha anche iniziato a crearsi fonti che gli forniscono accesso a prototipi di modelli di cellulari prima che vengano immessi sul mercato, il che gli permette di fare analisi scientifiche in modo che gli ingegneri di “NSO” possano cercare falle di vulnerabilità che consentano un accesso totale ai telefoni che i loro clienti desiderano prendere di mira.

4. Zona grigia

Si potrebbe pensare che i produttori di telefonini intendano proteggere i propri prodotti come Fort Knox [area militare in cui sono conservate le riserve auree e monetarie degli USA, ndt.] e vietarli agli sguardi loschi di hacker come “NSO”. Ma l’impresa opera in una zona grigia e cerca di garantirsi quello di cui ha bisogno da varie fonti sia all’interno che all’esterno delle industrie produttrici.

Prima dei portatili, i criminali comunicavano nel modo in cui lo facevano tutti: con

telefoni fissi, mail o di persona. La tecnologia per intercettare o controllare queste comunicazioni era semplice e primitiva: per i telefoni si usava una "cimice" [microspie per l'ascolto di conversazioni private, ndt.] su una linea telefonica.

La cimice avrebbe dovuto presumibilmente essere approvata da un giudice ed essere messa in funzione con l'aiuto di una compagnia telefonica. C'era un processo di controllo e questo veniva in genere rispettato, almeno nelle società democratiche.

La comunicazione elettronica ha cambiato tutte le regole, aprendo nuove modalità per spiare le singole persone. Si possono intercettare dall'esterno i segnali di comunicazione tra chi parla. "NSO" ne ha approfittato, sviluppando un programma che, una volta scaricato, prenderà il controllo del telefonino di chi lo utilizza.

Così non c'è più bisogno di intercettare telefonate, perché il cliente di "NSO" è effettivamente all'interno dello stesso telefono. Le forze di polizia ed i governi possono distruggere i piani per commettere reati o attacchi terroristici prima che avvengano e preservare l'ordine pubblico.

5. Una breccia delle dimensioni di un camion

Ma c'è un aspetto problematico in questa tecnologia per altri versi benefica: "NSO Group" controlla solo quelli che l'hanno comprata, non l'utilizzatore finale. Il primo cliente può offrirla ad altri individui o enti nel suo governo, o creare un'identità commerciale fittizia per celare l'uso finale che farà di "Pegasus".

"NSO" sostiene di seguire tutte le regole israeliane che governano l'esportazione dei suoi prodotti e vende solo agli alleati di Israele e mai ai suoi nemici. Sostiene anche di vendere solo a governi e mai a singoli individui o ad utilizzatori non autorizzati. Afferma che "Pegasus" è previsto solo per lottare contro criminali e terroristi e mai per essere usato a fini politici.

Tuttavia sottolinea che, una volta che ha venduto il prodotto, non ha il controllo (o per lo meno questo sostiene) su chi usa la tecnologia o sul come. Questa è una breccia abbastanza grande da farci passare un camion Mack [marca che produce negli USA camion enormi, ndt.], e consente ad "NSO" – e a decine di altre

imprese di spionaggio informatico che offrono programmi simili – di evitare la responsabilità sui modi ripugnanti in cui la loro tecnologia viene usata.

Nel caso di Mansoor l'hackeraggio è stato diretto contro un cittadino considerato un criminale dallo Stato. Ma egli non lo è da nessun punto di vista riconosciuto da una società democratica. Non è stato imputato di nessun reato, di aver rapinato qualcuno o di aver messo una bomba. Nel 2011 è stato condannato a tre anni con l'accusa di oltraggio allo Stato (in seguito è stato amnistiato e liberato) – e ciò a quanto pare è stato sufficiente in un regime autocratico come quello degli EAU per considerarlo sospetto.

La tecnologia dell'"NSO" è caduta in cattive mani anche in Messico. Come ha informato il "New York Times", i telefoni di attivisti politici, per i diritti umani e contro la corruzione messicani che stavano facendo un'inchiesta su possibili delitti commessi dal governo e dai suoi agenti sono stati infettati da "Pegasus". Il "Times" afferma che le vittime se ne sono accorte per la prima volta nell'estate 2016.

Una di queste era l'avvocato che rappresenta i genitori di 43 studenti medi uccisi dalla polizia messicana in un caso per cui non è mai stata perseguita. Altri stavano facendo un'inchiesta sulla corruzione di dirigenti d'azienda collusi con rappresentanti eletti.

Secondo mail interne della "NSO" datate a partire dal 2013 e lette dal "New York Times", il governo messicano ha pagato alla "NSO" più di 15 milioni di dollari per tre progetti. Funzionari messicani hanno negato di essere coinvolti nello spionaggio ed hanno aperto un'inchiesta.

Questi usi violano le disposizioni della licenza di esportazione israeliana in base alla quale "NSO" vende i propri prodotti. Ma ci sono scarse possibilità che i funzionari israeliani intervengano in questo caso. Sono interessati a promuovere le esportazioni israeliane, non a limitarle. Né vedono il proprio ruolo come un servizio di censori nei confronti del comportamento delle imprese israeliane.

"Middle East Eye" ha contattato l'agenzia di controllo dell'esportazione per la difesa del Ministero della Difesa israeliano per chiedere di commentare i suoi rapporti con "NSO". Non ha risposto prima che questo articolo venisse pubblicato. Abbiamo anche posto delle domande all'ufficio stampa del Ministero della Difesa, e neppure questo ha risposto a tempo per la pubblicazione.

Per esempio, molti esportatori di armi israeliani sono sospettati di essere impegnati in truffe e altre pratiche corruttive per ottenere contratti per la vendita di armamenti con eserciti stranieri. Poche tra queste imprese sono state messe sotto inchiesta dalle autorità israeliane, benché a parecchie sia stato vietato di fare affari in vari Paesi.

"Citizen Lab" ha detto a "Forbes" che "NSO" ha registrato domini in Israele, Kenya, Mozambico, Yemen, Qatar, Turchia, Arabia Saudita, Uzbekistan, Thailandia, Marocco, Ungheria, Nigeria e Bahrain, suggerendo che "Pegasus" potrebbe essere stato usato in questi Paesi, anche se non ci sono prove evidenti.

Secondo email interne, contratti e proposte di "NSO" visionate dal "New York Times", "NSO" fa pagare ai clienti 650.000 dollari per spiare i proprietari di 10 iPhone, più 500.000 dollari di commissione per la configurazione.

E' evidente quanto questo affare possa essere una miniera d'oro – ed anche perché "NSO" potrebbe essere tentata di allentare le considerazioni etiche per massimizzare il suo profitto potenziale. "Middle East Eye" ha cercato un cofondatore di "NSO" e l'addetto stampa dell'impresa per un commento. Nessuno ha risposto.

Da imprenditori astuti quali sono, Lavie e Hulio hanno deciso di poter giocare da entrambi i lati. E' così che nel 2013 hanno fondato "Kaymera", un'altra azienda tecnologica con sede nell'università di Herzilya destinata a proteggere i clienti contro intrusioni informatiche indesiderate.

Nella maggior parte delle iniziative imprenditoriali, questo passaggio del confine avrebbe fatto scattare l'allarme. Ci potrebbero essere dei vantaggi nel condividere informazioni: non appena un ingegnere dell' "NSO" ha individuato il punto debole di un'impresa, potrebbe condividerlo con "Kaymera" per risolverlo.

Ma con la stessa facilità potrebbe succedere il contrario: "Kaymera" potrebbe informare "NSO" dei punti deboli che ha scoperto nei sistemi informatici o di comunicazione di un cliente. Questa informazione potrebbe effettivamente essere monetizzata a favore di entrambe le aziende. Middle East Eye ha contattato "Kaymera" per avere un commento e l'impresa non ha risposto.

Il problema è che, in uno Stato di sicurezza nazionale come Israele, considerazioni etiche come queste passano in secondo piano rispetto ai benefici

per la sicurezza *e* finanziari.

6. Unicorni e galline dalle uova d'oro

La crescente clientela di "NSO" e i profitti che genera hanno attirato l'attenzione di società di capitale di rischio alla ricerca di opportunità di investimenti lucrosi. Una di queste è stata la società privata di investimenti "Francisco Partners" con sede negli USA.

Nel 2014 la società ha comprato una quota di maggioranza in "NSO" per 120 milioni di dollari. Le migliori società finanziarie investono in un'impresa per un lungo periodo, offrendo non solo un investimento di capitale, ma anche consulenza strategica e gestionale. Ma altre investono a breve termine. "Francisco" è una di queste.

Cosa interessante, "Francisco Partners" e un ramo di "NSO" hanno un passato di rapporti con l'ex consigliere per la sicurezza nazionale dell'amministrazione Trump Michael Flynn, che ha dato le dimissioni in febbraio dopo indiscrezioni sui suoi rapporti con la Russia.

Secondo moduli informativi finanziari, una controllata di "NSO" con sede in Lussemburgo, "OSY Group", ha pagato a Flynn 40.280 dollari per il suo ruolo come membro del consiglio di amministrazione dal maggio 2016 al gennaio scorso. Flynn – che avrebbe lavorato per molte imprese di sicurezza informatica – è stato anche consulente del socio proprietario di "NSO", "Francisco Partners", ma non ha mai rivelato quanto lo hanno pagato.

Un mese prima che Flynn entrasse nel consiglio di amministrazione di "OSY", "NSO Group" ha aperto una nuova branca nella zona di Washington chiamata "WestBridge Technologies" che, secondo l' "Huffington Post", è "in lizza per contratti con il governo federale per prodotti del gruppo "NSO". Assumere Flynn avrebbe messo a disposizione di "NSO Group" una figura con ottimi contatti a Washington, per aiutarla a inserirsi nel mondo notoriamente esclusivo della destinazione dei fondi dei servizi segreti."

"Francisco Partners" ha tenuto "NSO" solo per un anno prima di iniziare a venderla con una valutazione di un miliardo di dollari. Nelle scorse settimane "Blackstone Group", una delle più grandi società finanziarie di Wall Street,

avrebbe accettato di acquistare una quota del 40% in “NSO”.

Un investimento di 400 milioni di dollari da parte di “Blackstone” avrebbe fatto diventare “NSO” un “unicorno” (una startup che ha raggiunto il valore di un miliardo di dollari o più) ed offerto ai suoi fondatori – e a “Francisco Partners” – un enorme guadagno.

Data la maggiore penetrazione nel mercato mondiale che l’investitore “Blackstone” avrebbe fornito a “NSO”, le notizie hanno preoccupato gli attivisti per la libertà nella rete.

“Access Now”, una Ong statunitense che sostiene un internet libero e democratico, ha dato vita ad una petizione on line ed a una campagna con l’intenzione di informare l’opinione pubblica sul modello di attività di “NSO”. “Citizen Lab” si è unito al progetto scrivendo una lettera aperta al consiglio di amministrazione di “Blackstone”, invitandolo a “considerare con attenzione le implicazioni etiche e per i diritti umani” del loro potenziale investimento.

7. “Blackstone” si ritira

Questa settimana sono comparse notizie secondo cui “Blackstone” è uscita dalle trattative con “NSO” senza arrivare ad un accordo. Rispondendo ad una richiesta di commento da parte di “Middle East Eye” nel giorno in cui è stata annunciata la fine dei colloqui, un rappresentante di “Blackstone” ha rifiutato di commentare l’affare. Un’altra società di investimenti, “ClearSky Technologies”, avrebbe accettato di acquistare una quota del 10% in “NSO”. Ma anch’essa ha confermato a “Middle East Eye” che non investirà nell’azienda.

Un portavoce di “NSO” ha rifiutato di discutere con la Reuters [agenzia di stampa inglese, ndt.] dei colloqui o del perché sono saltati.

Ma pare probabile che la polemica generata da “Access Now” e le questioni sollevate dai giornalisti abbiano reso prudente la società sulla responsabilità che si sarebbe accollata.

“Finché ‘Blackstone’ non parla,” ha detto Peter Micek, consulente legale di ‘Access Now’, “non sapremo se hanno ascoltato le voci di difensori dei diritti umani, giornalisti e vittime di reati le cui vite sono state sconvolte dagli strumenti

di ‘NSO Group’”.

“Ma questo accordo defunto dimostrerà ad altri investitori, compreso l’attuale proprietario di ‘NSO’, ‘Francisco Partners’, che non c’è niente da guadagnare – e tutto da perdere – nell’investire nelle violazioni dei diritti umani.”

Tutto ciò mette in luce nuove domande su come “NSO” fa affari e sull’inconsistenza del suo modello etico. Perché, per esempio, “Pegasus” perde il simbolo e il controllo di “NSO” una volta che viene concessa la licenza ad un cliente? Perché l’azienda non può fissare condizioni esplicite nei suoi contratti stabilendo da chi e come sarà utilizzato?

8. Condizioni di utilizzo

Sembra ridicolo che un’impresa, la cui tecnologia è destinata a infiltrarsi e controllare le attività di singole persone prese di mira, non sia in grado di monitorare gli usi a cui vengono destinati i suoi prodotti.

Ovviamente, se “NSO” potesse controllare come i clienti utilizzano i suoi prodotti, potrebbe essere ritenuta responsabile se violano le condizioni di utilizzo. Gli attivisti per i diritti umani presi di mira o imprigionati a causa di “Pegasus” potrebbero forse fare causa per le proprie sofferenze a “NSO” in qualche sede giurisdizionale. Questa sarebbe un’ulteriore ragione per cui “NSO” preferisce non sapere quello che succede una volta che il suo malware lascia i suoi server.

E’ indispensabile che il futuro acquirente ne sia consapevole e risponda a queste preoccupazioni in modo costruttivo. Inoltre gli Stati che sono già clienti di “NSO” devono fare un lavoro molto migliore per monitorare come la tecnologia per la sorveglianza viene utilizzata nelle zone di loro competenza.

Gli Stati che stanno pensando di diventare clienti di “NSO” devono anche fornire tutele per garantire che “Pegasus” venga usato unicamente contro i veri cattivi, ma non contro civili, fautori del benessere pubblico, avvocati, giornalisti o attivisti politici.

Richard Silverstein *scrive sul blog “Tikun Olam”, dedicato a smascherare gli eccessi dello Stato della sicurezza nazionale israeliano. Il suo lavoro è comparso su “Haaretz”, “Forward”, “Seattle Times” e “Los Angeles Times”. Ha contribuito*

alla raccolta di saggi dedicata alla guerra in Libano del 2006, "A Time to Speak Out" [Il momento di far sentire la propria voce] (Verso), e a un altro saggio nella raccolta di prossima pubblicazione "Israel and Palestine: Alternative Perspectives on Statehood" [Israele e Palestina: prospettive alternative di sovranità nazionale] (Rowman & Littlefield).

Le opinioni espresse in questo articolo sono dell'autore e non riflettono necessariamente la politica editoriale di Middle East Eye.

(traduzione di Amedeo Rossi)