Israele inasprisce la sorveglianza sui palestinesi in Cisgiordania con un sistema di riconoscimento facciale

Israele inasprisce la sorveglianza sui palestinesi in Cisgiordania con un sistema di riconoscimento facciale

Elizabeth Dwoskin

Lunedì 8 novembre 2021 – Washington Post

Hebron, Cisgiordania – Secondo la descrizione del progetto data da soldati israeliani da poco congedati, l'esercito israeliano sta conducendo nella Cisgiordania occupata un vasto tentativo di sorveglianza per monitorare i palestinesi implementando il riconoscimento facciale con una sempre più diffusa rete di telecamere e telefonini.

Il progetto di sorveglianza, sviluppato negli ultimi due anni, sfrutta in parte una tecnologia per smartphone chiamata "Blue Wolf", che raccoglie le foto dei volti di palestinesi e li abbina a una banca dati di immagini così estesa che un ex-soldato l'ha descritta come un segreto "Facebook dei palestinesi" dell'esercito. L'applicazione lampeggia con colori diversi per avvertire i soldati se una persona deve essere fermata, arrestata o lasciata andare.

Per costruire la banca dati utilizzata da "Blue Wolf", lo scorso anno i soldati hanno fatto a gara nel fotografare palestinesi, compresi bambini e anziani, con premi per il maggior numero di foto raccolte da ogni unità. Non si sa quale sia il numero di persone fotografate ma, come minimo, sono nell'ordine delle migliaia.

Il programma di sorveglianza è stato descritto in interviste del *Washington Post* a due ex-soldati israeliani e in resoconti separati che loro e altri quattro soldati da poco congedati hanno fornito al gruppo israeliano di solidarietà *Breaking the Silence* e in seguito condiviso con *The Post*. Buona parte del programma non era

stato reso noto in precedenza. L'esercito israeliano ha ammesso l'esistenza del progetto in un opuscolo in rete, ma le interviste con gli ex-soldati offrono la prima descrizione pubblica della portata e del funzionamento del programma.

Oltre a "Blue Wolf" l'esercito israeliano ha installato telecamere per la scansione dei volti nella città divisa di Hebron per aiutare i soldati ai checkpoint a identificare i palestinesi prima ancora che esibiscano le loro carte d'identità. Una vasta rete di telecamere a circuito chiuso, denominata "Hebron Smart City" [Hebron Città Intelligente], fornisce in tempo reale il monitoraggio della popolazione della città e, come ha affermato un ex-soldato, può a volte spiare all'interno delle case private.

Gli ex-soldati che sono stati intervistati per questo articolo e che hanno parlato con *Breaking the Silence*, un'associazione di solidarietà composta da veterani dell'esercito israeliano che si oppongono all'occupazione, hanno descritto il programma di sorveglianza a condizione di mantenere l'anonimato per timore di ripercussioni sociali e professionali. L'associazione afferma di avere in progetto di rendere pubblica la sua ricerca.

I testimoni affermano che l'esercito ha detto loro che l'attività è un notevole miglioramento delle possibilità di difendere Israele contro i terroristi. Ma il progetto dimostra anche come le tecnologie della sorveglianza, tanto dibattute nelle democrazie occidentali, sono già utilizzate dietro le quinte in luoghi in cui le persone hanno meno libertà.

"Mettiamola così: non mi sentirei tranquilla se lo usassero nel supermercato (della mia città natale)," ha affermato una soldatessa israeliana appena congedata che ha prestato servizio in un'unità dell'intelligence. "La gente si preoccupa delle impronte digitali, ma questo è molto più grave." Ha detto a *The Post* di sentirsi motivata a parlare perché il sistema di sorveglianza di Hebron è una "totale violazione della privacy di un intero popolo".

Secondo gli esperti dell'associazione per i diritti civili digitali AccessNow, l'uso della sorveglianza e del riconoscimento facciale da parte di Israele sembra essere una delle applicazioni più estese ed elaborate di tale tecnologia da parte di un Paese che intende controllare una popolazione sottomessa.

In risposta alle domande sul programma di sorveglianza, l'esercito israeliano (IDF) ha affermato che "abituali operazioni per la sicurezza" sono "parte della

lotta contro il terrorismo e degli sforzi per migliorare la qualità della vita della popolazione palestinese in Giudea e Samaria" (Giudea e Samaria è nome ufficiale israeliano per la Cisgiordania).

"Naturalmente non possiamo fare dichiarazioni sulle capacità operative dell'esercito israeliano in questo contesto," aggiunge il comunicato.

Secondo l'organizzazione di sostegno "Surveillance Technology Oversight Project" [Progetto per il Controllo della Tecnologia di Sorveglianza] l'uso ufficiale di tecnologie per il riconoscimento facciale è stato vietato da almeno una decina di città USA, tra cui Boston e San Francisco. E questo mese il parlamento europeo ha sollecitato il divieto dell'uso da parte della polizia del riconoscimento facciale in luoghi pubblici.

Ma quest'estate uno studio del Government Accountability Office [Ufficio per la Responsabilità del Governo] degli USA ha scoperto che 20 agenzie federali hanno affermato di utilizzare sistemi di riconoscimento facciale e che sei agenzie delle forze dell'ordine affermano che la tecnologia ha contribuito a identificare persone sospettate di aver violato la legge durante rivolte civili. E l'Information Technology and Innovation Foundation, un gruppo commerciale che rappresenta le imprese tecnologiche, ha manifestato disaccordo riguardo alla proposta europea di divieto, affermando che danneggerebbe i tentativi delle forze dell'ordine di "rispondere efficacemente alla delinquenza e al terrorismo."

In Israele una proposta da parte di funzionari di polizia di introdurre telecamere di riconoscimento facciale in luoghi pubblici ha incontrato una ferma opposizione e l'agenzia governativa incaricata di proteggere la privacy si è espressa contro la proposta. Ma nei territori occupati Israele applica criteri diversi.

"Mentre i Paesi sviluppati in tutto il mondo impongono restrizioni alla fotografia, al riconoscimento facciale e alla sorveglianza, la situazione descritta [a Hebron] costituisce una gravissima violazione dei diritti fondamentali come il diritto alla privacy, in quanto i soldati sono incentivati a raccogliere quante più foto possibile di uomini, donne e bambini palestinesi in una sorta di competizione," afferma Roni Pelli, avvocatessa dell'Associazione per i Diritti Civili di Israele dopo aver saputo del progetto di sorveglianza. "L'esercito deve immediatamente smettere," dice.

Ultime tracce di privacy

Yaser Abu Markhyah, un palestinese di 49 anni padre di quattro figli, afferma che la sua famiglia ha vissuto a Hebron per cinque generazioni e che ha imparato a fare i conti con i checkpoint, le restrizioni ai movimenti e i frequenti interrogatori dei soldati da quando Israele ha conquistato la città durante la guerra dei Sei giorni nel 1967. Ma sostiene che recentemente la sorveglianza ha tolto alla gente le ultime tracce di privacy. "Non ci sentiamo più a nostro agio a socializzare, perché le telecamere ci stanno sempre filmando," afferma Abu Markhyah. Dice che non lascia più giocare i figli fuori, davanti a casa, e che parenti che vivono in quartieri meno controllati evitano di andarlo a trovare.

Hebron è stata a lungo un punto critico per la violenza, con un'enclave di coloni israeliani estremisti pesantemente protetti nei pressi della Città Vecchia circondati da centinaia di migliaia di palestinesi, e la gestione della sicurezza è divisa tra l'esercito israeliano e l'amministrazione palestinese.

Nel suo quartiere di Hebron, nei pressi della Tomba dei Patriarchi, luogo sacro per musulmani ed ebrei, sono state montate telecamere di sorveglianza ogni 100 metri, anche sui tetti delle case. Afferma che il monitoraggio in tempo reale sembra essere in aumento. Qualche mese fa, racconta, sua figlia di 6 anni ha fatto cadere un cucchiaino dal terrazzo sul tetto di casa e, benché la strada sembrasse vuota, poco dopo sono arrivati a casa sua dei soldati e hanno detto che sarebbe stato denunciato per aver lanciato pietre.

Issa Amro, abitante della città e attivista che guida il gruppo "Friends of Hebron" [Amici di Hebron], indica una serie di case vuote nel suo isolato. Afferma che le famiglie palestinesi se ne sono andate a causa delle restrizioni e della sorveglianza.

"Vogliono rendere la nostra vita così difficile che ce ne andremo per conto nostro, così potranno arrivare più coloni," sostiene Amro.

"Le telecamere," dice, "hanno solo un occhio, per vedere i palestinesi. Sei filmato dal momento in cui esci di casa al momento in cui rientri."

Incentivi per le foto

Secondo i sei ex-militari che sono stati intervistati da *The Post* e da *Breaking the Silence* il progetto Blue Wolf combina un'applicazione per il cellulare con una banca dati di informazioni personali accessibile attraverso dispositivi mobili.

Uno di loro ha detto a *The Post* che questa banca dati è una versione ridotta di un'altra grande banca dati, chiamata "Wolf Pack" [Branco di Lupi], che contiene il profilo praticamente di ogni palestinese in Cisgiordania, comprese foto degli individui, le loro storie familiari, l'istruzione e il livello di pericolosità di ognuno. Questo soldato da poco congedato ha avuto esperienza diretta di "Wolf Pack", che è accessibile solo su computer fissi in contesti più protetti (benché questo ex-soldato descriva la banca dati come "Facebook dei palestinesi", non è collegata a Facebook).

Un altro ex-soldato dice a *The Post* che alla sua unità, che nel 2020 pattugliava le strade di Hebron, è stato chiesto di raccogliere quante più foto di palestinesi possibile durante una certa settimana utilizzando un vecchio cellulare fornito dall'esercito, facendo le foto durante missioni quotidiane che spesso duravano otto ore. I soldati caricavano le foto attraverso la app Blue Wolf installata sui telefonini.

Questo ex-soldato afferma che i bambini palestinesi tendevano a mettersi in posa per le foto, mentre le persone anziane, soprattutto le donne, spesso facevano resistenza. Descrive l'esperienza di obbligare le persone ad essere fotografate contro la loro volontà come traumatica per lui.

Le foto prese da ogni unità arrivavano alle centinaia per ogni settimana, e un ex-soldato afferma che era previsto che l'unità ne facesse almeno 1.500. Le unità dell'esercito in tutta la Cisgiordania competevano per i premi, ad esempio una serata libera concessa a chi faceva più foto, dice l'ex-soldato.

Spesso, quando un soldato scatta la foto di qualcuno, l'applicazione registra la corrispondenza con un profilo già esistente nel sistema Blue Wolf. Allora, secondo i cinque soldati e una schermata del sistema ottenuta da *The Post*, l'applicazione lampeggia in giallo, rosso o verde per indicare se la persona deve essere fermata, immediatamente arrestata o lasciata passare.

Il grande sforzo di costruire la banca dati Blue Wolf con le immagini è diminuito negli ultimi mesi, ma le truppe continuano ad usarla per identificare i palestinesi, afferma un ex-soldato.

Un altro ex-soldato ha detto a *Breaking the Silence* che una diversa applicazione per cellulare, chiamata "White Wolf", è stata sviluppata per essere utilizzata da coloni ebrei in Cisgiordania. Benché ai coloni non sia consentito arrestare la

gente, i volontari della sicurezza possono utilizzare White Wolf per scansionare il documento di riconoscimento di un palestinese prima che entri in una colonia, per esempio per lavorare nell'edilizia. Nel 2019 l'esercito ha ammesso l'esistenza di White Wolf in una pubblicazione israeliana di destra.

"I diritti sono semplicemente irrilevanti"

Nell'unico caso noto, l'esercito israeliano ha fatto riferimento alla tecnologia Blue Wolf in giugno in un opuscolo in rete con cui invitava i soldati a partecipare a "una nuova squadra" che "vi trasformerà in un 'Blue Wolf'". L'opuscolo afferma che la "tecnologia avanzata" comprenderebbe "telecamere intelligenti con sofisticati sistemi di analisi" e "sensori che possono individuare e segnalare in tempo reale le attività sospette e gli spostamenti di persone ricercate."

In un articolo del 2020 sul suo sito l'esercito citava anche "Hebron Smart City". L'articolo, che mostra un gruppo di soldatesse chiamate "sentinelle" davanti a schermi di computer con visori per la realtà virtuale, descrive il progetto come una "pietra miliare" e una tecnologia "rivoluzionaria" per la sicurezza in Cisgiordania. L'articolo afferma che "in tutta la città è stato installato un nuovo sistema di telecamere e radar" che può documentare "qualunque cosa avvenga nei dintorni" e che "riconosce qualunque movimento o rumore insolito."

Nel 2019 Microsoft ha investito in una nuova impresa israeliana per il riconoscimento facciale chiamata AnyVision, che secondo NBC e la rivista economica israeliana *The Market* [Il Mercato] stava lavorando con l'esercito per costituire una rete di telecamere di sicurezza intelligenti che utilizzano la tecnologia della scansione facciale in tutta la Cisgiordania (Microsoft ha affermato di essere uscita dall'investimento in AnyVision durante gli scontri di maggio tra Israele e l'organizzazione di miliziani Hamas a Gaza).

Sempre nel 2019 l'esercito israeliano ha annunciato l'introduzione di un progetto pubblico di riconoscimento facciale, con tecnologia fornita da AnyVision, nei principali posti di controllo in cui i palestinesi entrano in Israele dalla Cisgiordania. Il progetto utilizza postazioni per scansionare documenti di identità e volti simili a quelle aeroportuali utilizzate per controllare i viaggiatori che entrano negli Stati Uniti. Secondo informazioni di stampa il sistema israeliano è utilizzato per verificare se un palestinese ha il permesso per entrare in Israele, ad esempio per lavorare o per andare a trovare parenti, e per tenere sotto controllo

chi sta entrando nel Paese. Questo controllo è obbligatorio per i palestinesi, come lo è quello negli aeroporti americani per gli stranieri.

Secondo un ex-soldato che ha partecipato al progetto e quattro abitanti palestinesi, a differenza dei controlli al confine il monitoraggio a Hebron avviene in una città palestinese senza informare la popolazione locale. L'ex-soldato ha detto a *The Post* che le telecamere ai checkpoint possono riconoscere anche i veicoli, anche senza registrare le targhe, e li abbina ai rispettivi proprietari.

Oltre a preoccupazioni riguardanti la privacy, una delle principali ragioni per cui la sorveglianza con il riconoscimento facciale è stata limitata in altri Paesi è che molti di questi sistemi hanno dimostrato livelli di precisione molto variabili, e alcune persone sono state messe a repentaglio perché identificate in modo errato.

L'esercito israeliano non ha fatto commenti riguardo alle preoccupazioni sollevate sul'uso di tecnologie per il riconoscimento facciale.

La Information Technology and Innovation Foundation [gruppo di analisi sulle politiche pubbliche USA relative all'industria e alla tecnologia, ndtr.] ha affermato che gli studi che dimostrano che questa tecnologia è inadeguata sono stati sopravvalutati. Contestando la proposta europea di divieto, l'associazione afferma che sarebbe meglio dedicarsi a sviluppare garanzie di un uso corretto della tecnologia da parte delle forze dell'ordine e standard di qualità dei sistemi di riconoscimento facciale utilizzati dal governo.

Tuttavia in Cisgiordania questa tecnologia è solo "un altro strumento di oppressione e sottomissione del popolo palestinese," afferma Avner Gvaryahu, direttore esecutivo di *Breaking the Silence*. "Mentre la sorveglianza e la privacy sono una priorità nella discussione pubblica a livello mondiale, qui vediamo un altro vergognoso assunto del governo e dell'esercito israeliani secondo cui quando si tratta di palestinesi i diritti umani fondamentali sono semplicemente irrilevanti."

Elizabeth Dwoskin

Lisa è entrata al *Washington Post* come corrispondente dalla Silicon Valley nel 2016, inviata del giornale nella zona. Si è concentrata sulle reti sociali e il potere dell'industria tecnologica in una società democratica. In precedenza è stata la prima cronista a tempo pieno del *Wall Street Journal* [prestigioso quotidiano

economico statunitense, ndtr.] ad essersi occupata di intelligenza artificiale e dell'impatto degli algoritmi sulla vita delle persone.

(traduzione dall'inglese 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)