volerelaluna LA POLITICA PUNTOACAPO

Israele e il sistema spia Pegasus

Autore: Loretta Mussi

Il ruolo strategico a livello economico, politico, militare della tecnologia informatica più avanzata nei rapporti di Israele con i più diversi paesi del mondo (dittature o democrazie che siano) è un fatto ben noto, macroscopico, non solo tollerato o considerato fisiologico, ma spesso considerato un indicatore dello sviluppo scientifico di Israele. Quanto segue, che riprende con un minimo di dettaglio ciò che è emerso nelle ultime settimane su **NSO-Pegasus**, non dice nulla di sostanzialmente nuovo dal punto di vista strettamente tecnico. Indica tuttavia uno dei modi in cui lo Stato di Israele occupa, nello scenario internazionale, spazi di illegalità che violano i diritti fondamentali in qualsiasi ambito della convivenza umana.

L'esistenza del gruppo NSO e del suo spyware (sistema spia) **Pegasus è giunta alla conoscenza della più vasta opinione pubblica in seguito all'assassinio di Jamal Khashoggi**, il cui telefono, insieme a quello di familiari e amici, risultò essere intercettato dallo spyware Pegasus, sebbene NSO abbia sempre negato che la sua tecnologia sia stata "in alcun modo" utilizzata per l'omicidio. In realtà Pegasus ha una diffusione globale ed è stato oggetto, negli anni, di denunce e azioni legali. Mentre, infatti, ufficialmente è venduto per combattere il crimine e il terrorismo, in realtà viene usato per controllare conversazioni e messaggi di attivisti, giornalisti, oppositori e politici, compresi esponenti di governo e capi di stato. D'altronde è risaputo che gli strumenti di spionaggio informatico sono spesso progettati per la repressione, indipendentemente da ciò che affermano le aziende produttrici e gli stati acquirenti.

Israele è al centro del commercio di sistemi spia e il gruppo NSO è una delle 27 società di sorveglianza elettronica con sede nel Paese, che lo pongono al top mondiale nel settore. Come per le armi che vende, anche i sistemi spia vengono usati e "testati" regolarmente contro i palestinesi prima di essere venduti a governi, per lo più, autoritari. NSO è stato fondato nel 2010 e impiega, tra gli altri, anche ex membri della famigerata unità 8200 dell'intelligence militare, nota per la sua attività di spionaggio elettronico dei palestinesi. L'azione di tale unità non si esercita solo sugli attivisti ma anche, e diffusamente, su persone qualsiasi, allo scopo di scoprire abitudini e aspetti imbarazzanti della loro vita, da utilizzare al momento opportuno, «per ricattarle e costringerle a diventare spie», com'è stato rivelato, anni fa, da alcuni refusenik.

La testata giornalistica online londinese indipendente ***Middle East Eye*, nel ripercorrere le accuse fatte a NSO** (Zeitun, 21 luglio 2021), cita tra i governi acquirenti una serie di paesi che non sono per nulla rispettosi dei diritti umani come Qatar, Arabia Saudita, Emirati Arabi Uniti, Nigeria, Bahrein, Messico, Turchia, Tailandia, Kenya, Azerbaigian, Uzbekistan, Mozambico, Togo, Marocco, Yemen, Ungheria. A quanto noto, Pegasus è stato venduto inoltre a Spagna, Francia e Stati Uniti. In quest'ultimo paese, l'FBI ha indagato a lungo NSO mentre importanti società tecnologiche ne hanno chiesto il

perseguimento per la sua pericolosità, tanto che recentemente il Dipartimento di Stato ha inserito NSO nella lista delle società bandite per ragioni di sicurezza nazionale e di tutela degli interessi di politica estera.

Un'indagine congiunta condotta da Front Line Defenders (FLD), Amnesty International e Citizen Lab (laboratorio interdisciplinare dell'Università di Toronto per ricerca, sviluppo e politica strategica di alto livello) su 75 dispositivi IPhone appartenenti a difensori dei diritti umani palestinesi ha rivelato che sono stati spiati almeno sei dispositivi e che con ogni probabilità l'infezione proveniva da *Pegasus. Alcuni dei dispositivi colpiti erano di proprietà di attivisti appartenenti alle sei organizzazioni della società civile palestinese che il Ministro della Diesa israeliano ha incriminato proprio nei giorni successivi alla pubblicazione dei risultati dell'indagine.* Gli stessi attivisti e ricercatori delle organizzazioni sopracitate e di Middle East Eye risultano essere stati colpiti da Pegasus.

Recentemente Forbidden Stories e Amnesty International hanno fornito a 17 gruppi editoriali, tra cui *Washington Post* e *The Guardian*, un elenco dei numeri di telefono presi di mira, portando all'identificazione di più di 1.000 persone in oltre 50 paesi. Tra queste, membri della famiglia reale saudita, almeno 65 dirigenti aziendali, 85 attivisti per i diritti umani, 189 giornalisti ? tra cui reporter, editori e dirigenti del *Financial Times*, della CNN, del *New York Times*, dell'*Economist*, della *Associated Press* e della *Reuters* – e più di 600 politici e funzionari di governo, tra cui, come già detto, capi di stato e primi ministri.

Infine anche Whatsapp ha fatto causa ad NSO per aver cercato di sorvegliare illegalmente e rubare informazioni ad oltre 1400 tra giornalisti, attivisti per i diritti umani e altri in 20 Paesi.

Rispetto alle accuse e ai fatti riportati NSO afferma di non sentirsi responsabile del modo in cui gli Stati, "clienti sovrani", utilizzano la sua tecnologia. E ripete, invariabilmente, che opera esclusivamente in conformità alle leggi e ai protocolli del Ministero della Difesa e sotto la costante supervisione dello stesso.

Come Stato parte del **Patto internazionale sui diritti civili e politici (ICCPR**), Israele avrebbe l'obbligo di garantire il diritto alla privacy e alla libera espressione delle opinioni, senza interferenze arbitrarie e illegittime. Ma sappiamo che Israele non rispetta tali principi, essendo spesso parte in causa, e che, finora, non ha attuato nessuna regolamentazione sulle sue industrie di sorveglianza e spionaggio, cui è consentito quindi di operare impunemente.

Oltre 180 organizzazioni della società civile ed esperti indipendenti, si sono mossi recentemente perché la comunità Internazionale si attivi nei confronti di NSO e in generale dell'industria della sorveglianza privata, che operano al di fuori di ogni controllo e in modo irresponsabile. Gli effetti di una sorveglianza condotta al di fuori di ogni quadro giuridico, senza controllo e trasparenza sono infatti devastanti. Così si è espresso *Front Line*

Defenders l'*8 novembre 2021:* «*Quando Pegasus viene installato sul telefono di una persona, l'hacker ha accesso completo a messaggi, e-mail, contenuti multimediali, microfono, fotocamera, password, chiamate vocali su applicazioni di messaggistica, dati sulla posizione, chiamate e contatti del telefono. Lo spyware permette inoltre di attivare la fotocamera e il microfono del telefono e di spiare le chiamate e le attività di un individuo».*

Questo significa che l'impatto va ben oltre il soggetto preso di mira fino a colpire persone estranee, con effetti a cascata su altri diritti, come la libertà di espressione e di associazione. Inoltre, in assenza di protezione e garanzie, i soggetti colpiti ? difensori dei diritti umani e giornalisti ad esempio – finiscono per autocensurarsi, anche laddove la sorveglianza non operi. **Le organizzazioni chiedono quindi una moratoria, su vendita, trasferimento e uso dello spyware Pegasus di NSO Group,** in particolare, ma non solo, fino a quando l'ONU non avrà effettuato un'indagine indipendente e approfondita sulle sue operazioni in Palestina e altrove. Ed esortano la comunità internazionale a intraprendere azioni immediate affinché Israele, Stato di origine di Pegasus, si conformi ai suoi obblighi ai sensi del diritto internazionale. Purtroppo Israele non rispetta il diritto internazionale, anzi lo nega, poiché sa di poter godere di una pressoché totale impunità, in ogni campo. È questa impunità che dobbiamo scalfire.