Pegasus: lo spionaggio di massa è una realtà

contropiano.org/news/internazionale-news/2021/07/31/pegasus-lo-spionaggio-di-massa-e-una-realta-0141083

July 31, 2021

Pubblichiamo questo contributo di Arundhati Roy, apparso sul *The Guardian* martedì 27 luglio.

La nota attivista indiana, nonché Premio Nobel per la Letteratura, riflette sulla diffusione e la pervasività di uno strumento di controllo di massa come Pegasus, *spyware* prodotto da una ditta israeliana – la NSO Group – venduto a differenti governi e che permette di hackerare con grande facilità i dispositivi informatici di chiunque.

Lo scandolo attorno a questa attività di intelligence di massa piuttosto opaca rende giustizia alla precisa denuncia di alcuni anni fa di Edward Snowden, ex analista della National Security Agency degli Stati Uniti, su quest'aspetto dispopico delle politiche governative.

In una recente intervista al *Guardian* – citata dalla Roy – ha avvertito: "*Se non fai nulla per fermare la vendita di questa tecnologia, non saranno solo 50.000 obiettivi. Saranno 50 milioni di obiettivi, e accadrà molto più velocemente di quanto nessuno di noi si aspetti.*"

La vicenda ormai è nota e mostra due aspetti almeno piuttosto rilevanti: la valenza dell'industria della sicurezza in Israele e delle sue teconlogie belliche che si riverberano sulla vita civile di tutti e la facilità dello spionaggio di massa, nonostante i costi esorbitanti che comporta, da parte die governi senza senza alcuna di fatto capacità di controllo, la applicano senza alcun filtro democratico.

Per ciò che concerne israele, con cui il nostro Paese ha una sviluppata cooperazione in vari settori connessi direttamente od indirettamente all'industria militare, ciò che avviene con Pegasus è simile a ciò che accade con altre tecnologie, come quelle di controllo delle frontiere.

"*Nel Mediterraneo di oggi*" – hanno ben spiegato due attivisti di Sea Watch intervenuti nel corso di una assemblea di inizio giugno a Livorno nell'ambito delle mobilitazioni dei lavoratori portuali contro il traffico delle armi "*non sono solo gli stati NATO che vengono sempre più coinvolti nella gestione delle frontiere; ma anche il capitale militare.*

La frontiera ormai è un'industria militare, un mercato enorme che entro il 2025 varrà oltre 65 miliardi di euro, in cui svolgono un ruolo da protagonista le aziende private specializzate nella progettazione e nel commercio di armi e tecnologie da guerra.

Per fare un esempio rilevante, uno dei paesi all'avanguardia dell'esportazione di apparati di sorveglianza non solo in Europa, ma anche negli USA e in Australia, è Israele. I droni usati da FRONTEX per dare supporto logistico alla cosiddetta Guardia Costiera libica sono stati inventati da Elbit Systems e Israel Aerospace Industries – entrambe aziende israeliane, che gestiscono l'apparato di controllo sul territorio palestinese."

Torniamo a quello che è avvenuto in India.

Avevamo già tradotto a marzo un contributo di una altra attivista di fama internazionale, come Naomi Klein, che rifletteva su "*The Intercept*" su come i giganti della rete, cioè le multinazionali connesse al digitale, fossero dietro la repressione del movimento in India, Stato che è divenuto un laboratorio su larga scala delle tecniche della controrivoluzione digitale contro i movimenti di massa.

Il disastro pandemico indiano era stato descritto a marzo dalla stessa Roy in un articolo che abbiamo tradotto come un vero e proprio crimine contro l'umanità, ha ulteriormente fatto vacillare l'attuale esecutivo retto da una convergenza di interessi tra i nazionalisti indù, i multimiliardari indiani proprietari di svariate attività economiche, e le caste più elevate, aumentando le paranoie del Potere Indiano.

Il tutto con il beneplacito dell'Occidente, per cui l'India è un baluardo nella politica di "contenimento" della Repubblica Popolare Cinese, e quindi nessuno, come hanno fatto gli USA con Cuba, si sogna di denunciarne la catastrofe umanitaria, occultata con sprezzo del ridicolo dalla leadership del Paese Asiatico contro le più banali evidenze empiriche.

Alla luce di quanto si legge qui sotto, sarà difficile non riflettere come l'abuso del concetto di *dittatura* e *creazione del nemico interno* sia stato così male indirizzato negli ultimi tempi anche da intellettuali di un certo rilievo e da alcuni osservatori politici.

Buona Lettura.

*****

Questo non è semplice spionaggio. La nostra intimità è ora allo scoperto

Il progetto Pegasus dimostra che presto potremmo essere governati da Stati che sanno tutto di noi, mentre noi sappiamo sempre meno sul loro conto

In India, l'estate della morte si sta presto trasformando nell'estate dello spionaggio.

La seconda ondata di coronavirus si è arrestata, dopo aver causato 4 milioni di morti in India. I numeri ufficiali ammontano solo a un decimo – 400.000. Nella distopia di Nahendra Modi, mentre il fumo dei forni crematori ancora si diradava e la terra delle tombe si assestava, degli enormi cartelloni sono apparsi nelle nostre strade per dire "*Grazie Modiji*" (un'espressione di gratitudine aniticipata per il "vaccino gratuito" che resta ancora poco reperibile, e che manca al 95% della popolazione).

Per quanto riguarda il governo Modi, qualsiasi tentativo di quantificare il vero numero di morti è una cospirazione contro l'India – come se i milioni di morti fossero attori che giacevano nelle fosse comuni di massa che avete visto dalle foto aeree, o che galleggiavano nei fiumi travestiti da cadaveri, o che si cremavano da soli nei marciapedi delle città, motivati unicamente dal desiderio di rovinare la reputazione internazionale dell'India.

Il governo indiano e i suoi media hanno mosso la stessa accusa contro il consorzio internazionale di giornalisti investigativi di 17 giornali, che hanno lavorato con *Forbidden Stories* e *Amnesty International* per rendere pubblica una storia straordinaria di sorveglianza su scala globale.

L'India appare in questi report a fianco a un insieme di altri Paesi i cui governi hanno acquistato lo spyware Pegasus prodotto dal NSO Group, un'azienda di sorveglianza israeliana. NSO, dal canto suo, ha dichiarato che vende la sua tecnologia solo a governi che hanno superato il vaglio in quanto a rispetto dei diritti umani e che si sono impegnati a usarla solo per fini di sicurezza nazionale – per tenere sotto controllo terroristi e criminali.

Tra gli altri Paesi ad aver superatto il test per i diritti umani dell'NSO ci sono Rwanda, Arabia Saudita, Bahrain, gli Emirati Arabi Uniti e Messico. Quindi chi esattamente ha deciso quale sia la definizione di "terroristi" e "criminali"? L'NSO e i suoi clienti?

Oltre al costo esorbitante dello spyware, circa centinaia di migliaia di dollari per telefono, l'NSO chiede un canone annuale per la manutenzione del sistema pari al 17% del costo totale del programma. C'è sicuramente qualcosa di proditorio in una corporazione straniera che fornisce e mantiene un sistema di sorveglianza che monitora privati cittadini per conto del governo del Paese.

Il team di giornalisti ha esaminato una lista trapelata di 50'000 numeri di telefono. L'analisi ha mostrato che più di 1.000 di questi sono stati selezionati in India da un cliente dell'NSO. Se un numero sia stato hackerato con successo, o sia stato soggetto a tentativi di hacking, lo si può dimostrare solo se i telefoni vengono sottoposti ad un esame forense. In India, molti dei telefoni esaminati sono risultati infettati dallo spyware Pegasus.

La lista trapelata include i numeri di membri di partiti d'opposizione, giornalisti dissidenti, attivisti, avvocati, intellettuali, imprenditori, un ufficiale dissidente della commissione elettorale indiana, un ufficiale dissidente dell'*intelligence*, ministri e le loro famiglie, diplomatici stranieri e anche il primo ministro pakistano, Imran Khan.

Portavoce del governo indiano hanno denunciato la lista come un falso. Osservatori della politica indiana sanno bene che neanche uno scrittore esperto e ben informato sarebbe in grado di costruire una lista così precisa e credibile di persone che il partito al governo considera di interesse o nemiche del proprio progetto politico. E' pieno di dettagli deliziosi, pieno di storie nelle storie. Ci sono nomi inaspettati. Molti tra quelli plausibili non ci sono.

Pegasus, ci viene riferito, può essere installato in un telefono con anche solo una chiamata persa. Immagina. Un carico di spyware invisibile sganciato da una chiamata persa. Un ICBM senza precedenti. Uno in grado di smantellare democrazie e atomizzare società senza il disturbo della burocrazia – nessun mandato, accordo sulle armi, commissioni di inchiesta, nessun tipo di regolamentazione. La tecnologia è neutrale ovviamente. Non è colpa di nessuno.

La collaborazione amichevole tra India e NSO sembra essere iniziata in Israele nel 2017, durante ciò che i media hanno chiamato la "bromance" Modi-Netanyahu – quella volta che si sono arrotolati i pantaloni e si son messi a sguazzare nella spiaggia di Dor. Hanno lasciato ben più che impronte sulla sabbia. E' allora che i numeri sono iniziati ad apparire sulla lista.

Lo stesso anno il budget del Consiglio di Sicurezza Nazionale è decuplicato. La maggior parte della spesa è stata allocata alla cybersicurezza. Nell'agosto 2019, poco dopo la seconda vittoria di Modi come primo ministro, la draconiana legge indiana sull'antiterrorismo, la UAPA (*Unlawful Activities Prevention Act*), con la quale in migliaia sono stati arrestati senza possibilità di cauzione, è stata espansa per includere anche individui, non solo organizzazioni.

Le organizzazioni, d'altronde, non hanno telefonini – dettaglio importante, per quanto teorico. Ma certamente espande il mandato. E il mercato.

Durante il dibattito parlamentare sull'emendamento, il ministro dell'interno, Amit Shah, ha dichiarato: "*Signori, le armi non causano il terrorismo, le radici del terrorismo affondano nella propaganda fatta per diffonderlo… E se questi individui verranno riconosciuti come terroristi, non credo che dei parlamentari debbano avere obiezioni*".

Lo scandalo Pegasus ha causato un putiferio durante la sessione estiva del parlamento. L'opposizione ha richiesto le dimissioni del ministro dell'interno. Il partito di Modi, forte di una maggioranza assoluta, ha schierato Ashwini Vaishnaw – di recente entrato come ministro delle ferrovie, comunicazioni e tecnologie informatiche – a difendere il governo in parlamento. Imbarazzante per lui che anche il suo numero fosse sulla lista trapelata.

Mettendo da parte la sbruffonaggine e il burocratese disorientante delle molte dichiarazioni del governo, non si trova nessuna smentita sull'acquisto e l'uso di Pegasus. Neanche l'NSO ha smentito. Il governo di Israele ha aperto un'inchiesta sulle accuse di abuso dello spyware, così come il governo francese. In India la pista dei soldi ci condurrà, prima o poi, alla pistola fumante.

Ma dove ci porterà questa pistola fumante? Consideriamo questo: ci sono 16 attivisti, avvocati, sindacalisti, professori e intellettuali, molti di loro dalit (la casta degli "intoccabili", *ndt*), che sono stati imprigionati per anni in quello che è conosciuto come il caso Bhima-Koreagon (BK).

Sono accusati, incredibilmente, di aver cospirato per incitare le violenze avvenute tra dalit e gruppi di caste privilegiate nel gennaio 2018, quando decine di migliaia di dalit si sono radunati per commemorare il 200esimo anniversario della battaglia di Bhima-Koregaon (nella quale i soldati dalit hanno combattuto per sconfiggere i Peshwa, un regime tirannico bramino).

I numeri di telefono di 8 dei 16 BK accusati, e i numeri di alcuni dei loro famigliari più stretti, sono apparsi sulla lista. Se tutti o alcuni dei loro telefoni siano stati oggetto di hacking, tentati o riusciti, non si può sapere, perché i loro telefoni sono in custodia della polizia e non disponibili per esaminazioni forensi.

Negli anni alcuni di noi sono diventati esperti nelle modalità sinistre che il governo di Modi è pronto ad adottare per fermare coloro che considera suoi nemici – ed è più che semplice sorveglianza.

Il *Washington Post* ha recentemente pubblicato un report di *Arsenal Consulting*, un'azienda digitale forense del Massachusetts, che ha esaminato copie elettroniche dei computer di due dei BK accusati, Rona Wilson e Surendra Gadling.

Gli investigatori hanno scoperto che entrambi i loro computer sono stati infiltrati da un hacker non identificato, e che documenti incriminanti sono stati nascosti nei loro hard drive. Tra questi, per aggiungere pathos, c'era una lettera assurda che delineava un piano banale per assassinare Modi.

Le gravi implicazioni contenute nella relazione di Arsenal non hanno spinto il sistema giudiziario indiano o la sua stampa tradizionale ad agire diversamente. Al contrario. Mentre lavoravano duramente per insabbiare e contenere le possibili ricadute del rapporto, uno degli accusati della BK, un sacerdote gesuita di 84 anni, padre Stan Swamy, che aveva trascorso oltre trent'anni nello Jarhkland tra le tribù che abitano la foresta e lottano contro la conquista aziendale delle loro terre d'origine, moriva atrocemente dopo essere stato infettato dal coronavirus in prigione. Al momento del suo arresto aveva il morbo di Parkinson e il cancro.

Allora, cosa dobbiamo fare di Pegasus? Liquidarla cinicamente come una nuova iterazione tecnologica di un gioco secolare in cui i governanti hanno sempre spiato i governati sarebbe un grave errore. Questo non è un normale spionaggio. I nostri telefoni cellulari rappresentano il nostro io più intimo. Sono diventati un'estensione del nostro cervello e del nostro corpo.

La sorveglianza illegale attraverso i telefoni cellulari non è una novità in India. Ogni Kashmir lo sa e lo sanno anche la maggior parte degli attivisti indiani. Tuttavia, cedere ai governi e alle società il diritto legale di invadere e prendere il controllo dei nostri telefoni significa sottometterci volontariamente alla violazione della nostra privacy.

Le rivelazioni del progetto Pegasus mostrano che la potenziale minaccia di questo spyware è più invasiva di qualsiasi forma precedente di spionaggio o sorveglianza. Più invasivo anche degli algoritmi di Google, Amazon e Facebook, all'interno dei quali milioni di persone vivono la loro vita e giocano i loro desideri. È più che avere una spia in tasca. È come se si fornissero le informazioni più nascoste del nostro stesso cervello.

Spyware come Pegasus mettono a rischio politico, sociale ed economico non solo l'utente di ogni telefono infetto, ma l'intera cerchia sociale dei propri amici, famiglie e colleghi.

La persona che probabilmente ha riflettuto in modo più approfondito di chiunque altro sulla sorveglianza di massa è il dissidente ed ex analista della National Security Agency degli Stati Uniti Edward Snowden. In una recente intervista al *Guardian*, ha avvertito: "*Se non fai nulla per fermare la vendita di questa tecnologia, non saranno solo 50.000 obiettivi. Saranno 50 milioni di obiettivi, e accadrà molto più velocemente di quanto nessuno di noi si aspetti*." Dovremmo prestargli attenzione.

Ho incontrato Snowden a Mosca quasi sette anni fa, nel dicembre 2014. Era trascorso circa un anno e mezzo da quando era diventato informatore, disgustato dalla sorveglianza di massa indiscriminata dei suoi cittadini da parte del suo governo. Aveva fatto la sua grande fuga nel maggio 2013 e si stava lentamente abituando alla vita come fuggitivo.

Daniel Ellsberg (dei *Pentagon Papers*), John Cusack (di *John Cusack*) ed io ci siamo recati a Mosca per incontrarlo. Per tre giorni, ci siamo rintanati in una stanza d'albergo con il gelido inverno russo che premeva contro i vetri delle finestre, per parlare di sorveglianza e spionaggio.

Dove ci porterà questa pista? Quanto lontano? Quando è scoppiata la notizia del progetto Pegasus, sono tornato indietro e ho guardato la trascrizione della nostra conversazione registrata. Si trattava di poche centinaia di pagine. Mi ha fatto rizzare i capelli.

Snowden, che aveva appena trent'anni allora, era cupamente profetico: "*La tecnologia non può essere ripristinata, la tecnologia non va da nessuna parte … sarà più economico, sarà più efficace, sarà più disponibile. Se non facciamo nulla, ci troveremo come sonnambuli in uno stato di sorveglianza totale in cui abbiamo sia un super-Stato che ha una capacità illimitata di applicare la forza, sia una capacità illimitata di sapere e dunque di dirigere in modo molto specifico quella forza- e questa è una combinazione molto pericolosa. Questa è la direzione del prossimo futuro.*

In altre parole, andiamo nella direzione di essere governati da Stati che sanno tutto ciò che c'è da sapere sulle persone e di cui la gente sa sempre meno. Questa asimmetria può andare solo in una direzione. Malvagità. E la fine della democrazia.

Snowden ha ragione. La tecnologia non può essere ripristinata. Ma non deve funzionare come un'industria legittima e non regolamentata, che travolge profitti, sboccia e fiorisce sulle autostrade transcontinentali e pulsanti del libero mercato. Bisogna legiferare contro questi rischi.

Ma dove ci porta tutto questo? Nel mondo della buona politica vecchio stile, direi. Solo un'azione politica può fermare o mitigare questa minaccia.

Perché questa tecnologia, quando viene utilizzata, se non legalmente, illegalmente, esisterà sempre all'interno della complicata matrice che descrive i nostri tempi: nazionalismo, capitalismo, imperialismo, colonialismo, razzismo, castismo, sessismo.

Questo rimarrà il nostro campo di battaglia, indipendentemente da come si sviluppa la tecnologia. Dovremo tornare a un mondo in cui non siamo controllati e dominati dal nostro intimo nemico: i nostri telefoni cellulari.

Dobbiamo cercare di ricostruire le nostre vite, le nostre lotte e i nostri movimenti sociali al di fuori del regno asfissiante della sorveglianza digitale. Dobbiamo spodestare i regimi che stanno dispiegando questi strumenti contro di noi.

Dobbiamo fare tutto il possibile per stringere la presa sulle leve del potere, per ricucire quanto ci hanno strappato e riprenderci ciò che ci hanno sottratto.

31 Luglio 2021

Ultima modifica: 30 Luglio 2021, ore 21:35 stampa