LA NUOVA Bussola Quotidiana
DIRETTORE RICCARDO CASCIOLI
FATTI PER LA VERITA'

CYBER SPIONAGGIO

Caso Pegasus: siamo tutti spiati. Prendiamone atto

ATTUALITà 20-07-2021

Gianandrea Gaiani

Per il presidente della Commissione europea Ursula von der Leyen la vicenda che vede protagonista il software-spia Pegasus prodotto dalla società israeliana di cyber intelligence NSO Group "è totalmente inaccettabile, se vera", eppure da almeno 22 anni

dovremmo esserci tutti abituati a intercettazioni e spionaggio delle comunicazioni effettuati a danno, non solo di categorie professionali, ma soprattutto di aziende, leader e governi.

Era il 1999 quando esplose lo scandalo Echelon che evidenziò come le potenze anglosassoni vincitrici della seconda guerra mondiale spiassero le comunicazioni telefoniche mondiali, incluse quelle degli alleati, attraverso il club ristretto di intelligence noto come “Five Eyes” (USA, Gran Bretagna, Canada, Australia e Nuova Zelanda). E nel 2013 il Datagate, scatenato dalle rivelazioni di Edward Snowden, rivelò i programmi di sorveglianza di massa della National Security Agency spiegando come statunitensi e britannici avessero accesso diretto a e-mail e utenze telefoniche istituzionali e private dei principali leader europei e mondiali.

Difficile quindi trovare nuove occasioni per scandalizzarsi troppo per il “caso Pegasus”, tecnologia israeliana ma con molti prodotti similari nel mondo, usata da diversi Paesi per hackerare i telefoni e spiare migliaia di persone in tutto il mondo attraverso i cellulari: nel mirino politici, giornalisti, attivisti per i diritti umani, manager di primo piano. La notizia è stata diffusa dal *Washington Post* sulla base di un'inchiesta condotta con altri 16 media. I telefoni fanno parte di una lista di oltre 50mila utenze, individuate in Paesi "noti per impegnarsi nella sorveglianza dei cittadini e noti anche per essere Stati clienti dell'azienda israeliana NSO Group", scrive il *Washington Post*. Molti numeri sarebbero associati a 10 dei 20 Stati nella lista: Azerbaijan, Bahrain, Ungheria, India, Kazakistan, Messico (15mila utenze), Marocco (10mila numeri di telefono), Bahrein, Ruanda, Emirati Arabi. Tra le prime reazioni all’inchiesta del giornale statunitense si registra quella dell'ufficio del primo ministro ungherese Viktor Orban, ovviamente subito finito nell’occhio del ciclone e nel mirino dei commentatori politically correct.

"In Ungheria, gli organi statali autorizzati a utilizzare strumenti in incognito sono regolarmente monitorati da istituzioni governative e non governative", ha affermato l'ufficio del premier. "Avete fatto le stesse domande ai governi degli Stati Uniti d'America, del Regno Unito, della Germania o della Francia?" - chiede con ironia la nota di Budapest. Oltre 180 giornalisti di *Financial Times* (incluso il direttore), *Wall Street Journal* , della *Cnn*, del *New York Times*, *Al Jazeera*, *France 24*, *Radio Free Europe*, *El Pai's*, *Associated Press*, *Le Monde*, *Bloomberg*, *Agence France-Presse*, *Economist* e *Reuters*, ma anche attivisti per i diritti umani, sindacalisti, politici, figure religiose e avvocati in tutto il mondo sarebbero stati controllati da governi tramite lo spyware Pegasus che la società produttrice sostiene venga fornito solo a forze dell'ordine e agenzie di intelligence, con

lo scopo di combattere il crimine.

Pegasus è un malware capace d'infettare iPhone e Android da cui è in grado di estrarre messaggi, foto ed email, come anche registrare chiamate e attivare microfoni. L'utente oggetto dello spionaggio lo installa inconsapevolmente aprendo un pacchetto dati o un link ricevuto sul proprio telefono: lo stesso meccanismo adottato in Italia per hackerare il telefono di Palamara. Sul database di Pegasus pare siano stati rivenuti, secondo il *Guardian*, anche i numeri di sindacalisti, funzionari governativi, uomini d'affari, presidente, ministri e premier.

Gli analisti francesi di *Forbidden Stories* e del *Security Lab* di Amnesty international hanno confermato che alcuni giornalisti d'inchiesta sono stati realmente tenuti sotto controllo. Tra questi figura Umar Khalid, leader indiano della Democratic Students' Union in carcere dallo scorso anno. Nel corso del processo, l'accusa ha presentato documenti che erano nel telefono personale dell'imputato, senza spiegare in che modo vi fosse entrata in possesso. Dall'inchiesta emerge che sono stati tenuti sotto sorveglianza anche i familiari e i colleghi di Jamal Khashoggi (nella foto Hatice Cengiz, fidanzata di Khashoggi, che era spiata con Pegasus), il giornalista ucciso all'interno dell'ambasciata saudita di Istanbul nel 2018. E' stato spiato per ben tre anni invece il telefono di Khadija Ismayilova, una delle più importanti reporter dell'Azerbaigian per le sue inchieste atte a rivelare corruzioni e abusi del presidente Ilham Aliyev. Il governo di Baku è accusato di aver messo sotto controllo almeno 48 cronisti. Ismayilova ha già scontato 18 mesi di reclusione e attualmente vive in esilio in Turchia. Inoltre nella lista di Pegasus appare del numero di Cecilio Pineda Birto, un giornalista messicano assassinato nel 2017. Il suo smartphone non è mai stato ritrovato e quindi non è stato possibile confermare la presenza dello spyware, tuttavia sussiste il sospetto che il mandante del suo omicidio lo abbia spiato per scoprire a quale indirizzo inviare il sicario.

Sistemi di spionaggio come Pegasus sono oggi molto diffusi e la loro tecnologia non può certo venire detenuta in esclusiva. Per questo la minaccia per i cittadini è in costante crescita indipendentemente dal fatto che vengano impiegati da regimi, segretamente da governi democratici, strutture private al servizio più o meno esplicito di istituzioni o da organizzazioni eversive e criminali. Del resto tutti noi oggi utilizziamo il telefono per fare acquisti di ogni tipo e quindi i dati di ogni semplice cittadino hanno un valore commerciale rilevante: questo significa che potremmo venire spiati, pur senza rappresentare una minaccia per un governo, una nazione o un sistema politico, senza necessariamente essere reporter d'inchiesta o dissidenti.

Dovremmo semmai puntare allo sviluppo di tecnologie in grado di proteggere gli

apparecchi telefonici dagli spyware ed evolverci verso un modello culturale opposto a quello frenetico-compulsivo con cui oggi approcciamo social media e smart phone.