Pandemia szpiegowania

10 maja 2020

Epidemia COVID-19 inspiruje władze wielu krajów do wykorzystywania aplikacji na smartfony, by śledzić osoby zarażone i ich kontakty lub by ostrzegać zdrowych przed zarażonymi, gdyby się do nich zbliżali. Jedynymi dobrze sprawdzonymi i skutecznymi aplikacjami tego typu są produkcje izraelskie, gdyż Izraelczycy dysponują zniewolonym narodem – palestyńskim, który nieustannie śledzą na różne sposoby. Jest on idealnym, zbiorowym królikiem doświadczalnym, co zapewnia izraelskiej marce NSO zainteresowanie wielu dyktatorskich rządów i tajnych służb, w tym komercyjnych. Problem: zainteresowanie produktami NSO wyraża Unia Europejska.

Na Zachodzie padają najróżniejsze pomysły „wzmocnienia bezpieczeństwa epidemiologicznego", np. łączenia smartfonowych aplikacji z obowiązkiem noszenia przez zarażonych elektronicznej opaski GPS, jakie niektórzy skazani muszą nosić nad kostką (np. rządy indyjski i francuski), a same aplikacje mogą służyć do przesyłania najróżniejszych danych, nie tylko tych, które mają być jawne dla użytkowników. Naturalnie stosowanie GPS w aplikacjach śledzących zwykłych ludzi budzi kontrowersje, choć stosują to na razie tylko niektóre kraje azjatyckie, ale i aplikacje oparte na Bluetooth, teoretycznie bardziej anonimowe, mogą być dwóch rodzajów: działać w sieciach zdecentralizowanych lub centralizowanych. W tym drugim przypadku nie ma przeszkód, by efektywnie kontrolować ruchy tłumów lub jednostek oraz ich kontakty.

Np. armia szwajcarska wspólnie z firmą Ubique rozwija aplikację wykorzystującą Bluetooth pod roboczą nazwą „DP3D", która ma być (od połowy maja) całkowicie anonimowa i zdecentralizowana. Telefony użytkowników mają ostrzegać, gdyby doszło do jakiegoś bliższego spotkania z kimś zarażonym i

informować, co robić. Inną drogę wybrali Niemcy i Francuzi: pracują nad aplikacją „StopCOVID”, która miałaby działać już na początku czerwca i jednak centralizować dane. Oczywiście mówi się ciągle o anonimowości, lecz będzie ona powiedzmy dość względna, bo w każdej chwili centralny operator będzie mógł dojść o czyj telefon chodzi, nawet jeśli oficjalnie przed tym się broni. Minister cyfryzacji w rządzie Macrona zapewnia, że „nie ma co filozofować, bo chodzi o ludzkie życie”, co ma zamknąć usta opozycji.

Kariera „Fleminga”

Weźmy np. wielkie kraje, jak Indie i Brazylia. 1 maja, w dzień Święta Solidarności Ludzi Pracy, indyjski minister spraw wewnętrznych ogłosił dekret rządowy, według którego wszyscy pracownicy, bez względu na to, czy pracują dla przedsiębiorstw państwowych czy prywatnych, są zobowiązani do instalacji aplikacji, która ma notować wszelkie kontakty z osobami zarażonymi. Jeśli brać pod uwagę oficjalne dane, rozmiar epidemii COVID-19 w Indiach jest mniej niż anegdotyczny (mniej niż promilowy), a jednak setki milionów pracujących zostaną poddane kontroli aplikacji łączącej wykorzystanie Bluetooth z GPS. Dyrekcje przedsiębiorstw i właściciele są z tego obowiązku zwolnieni, muszą tylko dopilnować, by „100 proc.” ich podwładnych załadowało „Aarogya Setu” („droga do zdrowia”), jak nazywa się ów programik.

Już 1 maja pobrały go 83 miliony ludzi, żeby nie stracić pracy. Dziś ta liczba zbliża się do 200 milionów, czyli „minimalnego celu” rządu, od którego aplikacja miałaby być „naprawdę” skuteczna. Z tymi „100 proc.” to chyba rodzaj metafory, bo tylko ok. 40 proc. ludzi w Indiach ma przenośne telefony. Tu wyjściem mają być „tanie” nadajniki GPS na nogę lub rękę, ale do objęcia ogółu pracowników jeszcze daleko. Tak się składa, że ultranacjonalistyczny rząd indyjski ma doskonałe stosunki z ultranacjonalistycznym Izraelem (łączy je silnie pogarda dla muzułmanów), a „Aarogya Setu” bardzo

przypomina „Fleming” – ostatnie informatyczne dziecko NSO Group. Tak się też składa, że izraelskie ministerstwo obrony, dowodzone teraz przez Naftalego Bennetta z neofaszystowskiej Nowej Prawicy, które zajmuje się sprzedażą produktów NSO, nie ujawnia wszystkich swoich transakcji międzynarodowych. „Fleming”ma tę przewagę nad rozwijanymi aplikacjami zachodnimi, że jest gotowy.

Gdy pod wpływem strachu wywołanego wiadomościami o epidemii w Indiach doszło do serii pogromów antymuzułmańskich, wieści o „Flemingu” zaczęły nadchodzić też z Brazylii, gdzie prezydent Jair Bolsonaro, który długo opierał się rygorom kwarantanny, musiał jednak wystąpić w maseczce, pod naciskiem stanowych gubernatorów. Dla niego taka aplikacja (Brazylia dysponuje już „Pegazem”) mogłaby załatwić sprawę epidemii i jednocześnie jeszcze bardziej zacieśnić stosunki z Izraelem. W polskich mediach trudno znaleźć informację, że na każdej, dosłownie każdej manifestacji zwolenników prezydenta-rasisty z jego udziałem, królują trzy flagi: oprócz narodowej, izraelska i amerykańska. Ma to ilustrować „brazylijskie marzenie” zwolenników Bolsonaro tęskniących za przywróceniem junty wojskowej oraz ich ambicje ustrojowe: połączenie izraelskiego reżimu apartheidu z amerykańską plutokracją, pod okiem generałów.

Skrzydła „Pegaza”

NSO Group wyleciała ponad palestyński horyzont w roku 2012, na skrzydłach „Pegaza”, swego flagowego produktu do dzisiaj. Przeszedł on znaczną ewolucję od kiedy trafił się pierwszy klient, prawicowy rząd Meksyku, który kupił ów program (zakwalifikowany przez władze izraelskie jako „broń”) za ok. 20 milionów dolarów. Oficjalnie Izrael sprzedawał tę broń różnym państwom „do walki z terroryzmem i przestępczością”, lecz służyła ona raczej do walki z opozycją polityczną, dziennikarzami, działaczami społecznymi i aktywistami organizacji pozarządowych.

„Pegaz” daje całkowite panowanie nad czyimś telefonem i nie sposób go wykryć programami antywirusowymi – wykrycie jego obecności to skomplikowana praca dla specjalistów. Przyjmuje się, że kupiło go od 30 do 45 państw, lecz w sumie są to dane niezbyt pewne. Niektóre reżimy same się do tego przyznają, przy innych wychodzi to przypadkiem. Wiadomo np., że kupiła go Arabia Saudyjska, bo miał go w telefonie Dżamal Chaszodżdżi, dziennikarz pokrojony na kawałki na zlecenie tamtejszego tyrana Mohammeda ben Salmana.

Co do Europy, obecność „Pegaza” wykryto dotąd tylko w kilku krajach: we Francji, w Grecji, na Łotwie, w Polsce, w Szwajcarii i Wielkiej Brytanii. To nie musi znaczyć, że rządy tych krajów kupiły „Pegaz”. Np. Indie śmiało to przyznały, ale w Europie nikt się tym specjalnie nie chwali, tym bardziej, że NSO Group ma na plecach już sporo procesów. Oczywiście wyjdzie z nich obronną ręką, ale jednak. Ostatnio najgłośniejszą sprawą jest hackowanie za pomocą „Pegaza” telefonów użytkowników WhatsApp, wykryte przez specjalistów tej firmy. Ktoś trzymał na krótkiej smyczy co najmniej 1400 osób: wysokich funkcjonariuszy rządowych, dziennikarzy i obrońców praw człowieka, a wszystko przechodziło przez serwery NSO usytuowane w Los Angeles.

Jednostka 8200

NSO Group powstała 10 lat temu z inicjatywy byłych oficerów Cahalu, tzw. Jednostki 8200, która zajmuje się wojnami elektronicznymi i szpiegowaniem sieciowym (produkcją wirusów itd.). Jej weterani ogłosili triumfalnie w Ha’aretz w 2014 r., że „populacja palestyńska pod władzą naszej armii jest całkowicie wystawiona na szpiegowanie i nadzór wywiadu”. Wszystko wskazuje, że „antyCOVIDowy Fleming” jest dzieckiem tej samej jednostki, ściśle powiązanej z NSO. Jego kontrolą i rozpowszechnianiem zajmuje się Szin Bet – tajna, izraelska służba bezpieczeństwa wewnętrznego.

„Fleming” nie jest tak „ciężki” ani tak skomplikowany jak „Pegaz”, ale daje dokładną geolokalizację, sprawdza pobierane i wysyłane pliki, może uruchamiać kamerę. Taka wersja tego programu była testowana od początku roku na tych Palestyńczykach, którzy z z terytoriów okupowanych przyjeżdżają do Izraela do pracy. Każdy kto chciał mieć zezwolenie na pracę musiał to zainstalować, inaczej wojsko nie przepuszcza przez punkty kontrolne. Powstała z tej aplikacji wersja eksportowa, jeszcze lżejsza, lecz jej zastosowanie w Izraelu budzi duże kontrowersje.

Walka naukowa

„Sprawy ochrony zdrowia i życia” przekonały rząd państwa żydowskiego do masowej inwigilacji obywateli izraelskich, co spotkało się z kontrą dwóch środowisk. Z jednej strony organizacje ochrony praw człowieka podały rząd do sądu z powodu „zagrożenia totalitarnego” i pogwałcenia praw obywatelskich, z drugiej nacjonaliści są oburzeni, że aplikację przeznaczoną pierwotnie do śledzenia gojów, stosuje się wśród Żydów. Sąd Najwyższy gra z Knesetem w rodzaj ping-ponga w tej sprawie, parlament musi przegłosowywać przedłużanie stosowania aplikacji. Oprócz ostrzegania, ma ona ciekawą funkcję: wyświetla zarażonym stopień ich zakażenia koronawirusem w skali od 1 do 10, dzięki współpracy z ministerstwem zdrowia.

W listopadzie ub. roku NSO Group, by przeciwdziałać swej wątpliwej sławie, zatrudniła b. dyplomatę Gérarda Arauda, b. ambasadora Francji w Tel-Awiwie i Waszyngtonie. Przekonuje on teraz w Europie, że NSO szanuje prawa człowieka i życie prywatne i że „Fleming” działa wyłącznie na rzecz ogólnego zdrowia. Raczej mu się udało, bo ambasador Unii Europejskiej w Izraelu Emanuele Giaufret ogłosił w kwietniu, że 27 państw Unii „wykorzystuje badania naukowe i technologiczne do walki z COVID-19”, co zawiera „projekty współpracy z Izraelem”. Izraelczycy dostali już zresztą część ze 150 milionów dolarów,

które Unia przeznaczyła na „walkę naukową” z COVID-19.

„To, co dzieje się Palestynie, nie zostaje w Palestynie” – głosi grupa badawcza Who Profits, zajmująca się zjawiskiem rozwoju inwigilacji elektronicznej przy okazji kryzysu epidemicznego, w kontekście zbrodniczej, izraelskiej okupacji Palestyny. Wydawało się, że państwom Unii izraelskie programy szpiegowskie nie będą tak imponować jak Bahrajnowi, Kazachstanowi, czy Stanom Zjednoczonym, lecz dzieje się inaczej. Według Johna Scotta-Railtona, naukowca z Uniwersytet Toronto kierującego pracami Citizen Lab, „Chodzi o ekstremalnie cyniczną próbę ze strony NSO wejścia na rynek masowej inwigilacji”.

Autorstwo: Jerzy Szygiel
Źródło: Strajk.eu