23.05.2020, 06:17 Warszawa (PAP)

Aplikacje w walce z pandemią – krok w stronę powszechnej inwigilacji? (wywiad)

Niedawno Polska dołączyła do krajów, w których powstała smartfonowa aplikacja informująca, że użytkownik zbliżył się do osoby o dużym ryzyku przenoszenia koronawirusa. O tym, jak skuteczne są tego typu programy i czy stwarzają zagrożenie dla prywatności, mówi PAP dr Szymon Wierciński.

Rozmówca PAP jest ekspertem w dziedzinie strategii cyfrowej innowacji z Akademii Leona Koźmińskiego w Warszawie.

Nauka w Polsce: Do walki z pandemią dołączyli informatycy. W Polsce powstała już rządowa aplikacja ProteGO Safe. Jakie jest dokładnie jej zadanie?

Dr Szymon Wierciński: Powstały już dwie aplikacje, których inicjatorem była strona rządowa. Jedna, obecnie obowiązkowa apka „Kwarantanna domowa", ma sprawdzać, czy osoba na kwarantannie rzeczywiście przebywa w miejscu, które zadeklarowała. Teraz nasz rząd, a także rządy innych krajów oraz firmy technologiczne, w tym Google i Apple, pracują nad aplikacjami, które informują, czy ktoś znalazł się w pobliżu zakażonej koronawirusem osoby.

PAP: Jak tego typu program realizuje to zadanie?

S.W.: Aplikacja korzysta z technologii Bluetooth, która pozwala na bezpośrednią komunikację dwóch urządzeń znajdujących się blisko siebie. Teoretycznie można z pomocą tej łączności określić odległość między urządzeniami, a więc także ich właścicielami. Warto podkreślić, że aplikacja cały czas ewoluuje, zmieniają się założenia co do jej funkcjonowania, ma zostać dostosowana do ulepszonego standardu wdrażanego wspólnie przez Apple i Google, więc trudno jest przewidzieć, jak będzie funkcjonowała za miesiąc czy pół roku.

PAP: Ale już widać potencjalne problemy, prawda?

S.W.: Po pierwsze, stosuje się tutaj duży skrót, według którego kontaktowi telefonów odpowiada kontakt ludzi. A przecież można np. telefon zostawić w domu lub przełączyć go w tryb samolotowy. Problematyczne jest też mierzenie odległości. Jeśli np. na drodze fal z routera od Wi-Fi stoi duże akwarium, sygnał jest znacznie słabszy. Człowiek także jest w pewnym sensie zbiornikiem z wodą. Jeśli więc dwie osoby będą stały blisko siebie, ale będą miały telefony w kieszeniach po przeciwnych stronach, efekt będzie podobny, jakby znajdowały się w większej odległości od siebie. A co, jeśli spotkają się na światłach w samochodzie? Na przykład kierowca jednego pojazdu i pasażer drugiego mogą znajdować się

blisko siebie, a jednak nie będą mieli z sobą praktycznie żadnego kontaktu. I dochodzi jeszcze element związany z nadawaniem sygnału w interwałach, co dodatkowo komplikuje sprawę, ponieważ kontakt będzie zarejestrowany, jeśli akurat trafimy na sygnał lub spędzimy z drugą osobą dłuższy moment.

PAP: Technologia Bluetooth ma jednak zapewniać poszanowanie dla prywatności, ponieważ telefony kontaktują się w tym przypadku bezpośrednio i nie trzeba np. sprawdzać, ani nigdzie przesyłać danych o geograficznym położeniu.

S.W.: Tutaj się zaczynają lekkie schody. Obecna aplikacja przetwarza sporą część danych po stronie serwera i nie do końca wiadomo, co się z nimi dzieje. Działanie systemu jest scentralizowane, tak jak w modelu singapurskim. Tam niezależni eksperci nie mieli wglądu w to, jak wygląda kod wykonujący kluczową czynność, czyli odznaczenie kluczy, które miały kontakt z zakażonym. Musimy tutaj ufać Ministerstwu Cyfryzacji, chociaż zapowiedzieli już, że kod po stronie serwera również poddadzą kontroli i opublikują go na licencji otwartej. W drugiej fazie współpracy Apple oraz Google (a to przecież ich systemy umożliwiają ministerstwu tworzenie autorskiego rozwiązania) telefony będą mogły rejestrować kontakt nawet bez instalowania dodatkowych aplikacji. Jednak, nawet gdyby aplikacja była doskonała i przetwarzałaby wszystkie dane wyłącznie w telefonie, nie dawałoby to całkowitej ochrony.

PAP: Dlaczego nie?

S.W.: Wyobraźmy sobie, że ktoś bierze udział w jakimś proteście i zostaje zatrzymany przez policję. A ta, korzystając z kilku źródeł informacji, w tym z zarejestrowanych w aplikacji kluczy, mogłaby sprawdzić, z kim dana osoba się kontaktowała podczas działania aplikacji. Program działa w taki sposób, że co jakiś odstęp czasu generuje nowy tzw. tymczasowy klucz identyfikacyjny, który będzie rejestrowany przez telefony w pobliżu. Jeżeli ten klucz będzie aktywny przez dłuższy okres, to użytkownik będzie zostawiał informacje o swoim przemieszczaniu się na innych urządzeniach.

PAP: To wszystkie kłopoty?

S.W.: Dochodzi do tego jeszcze jeden problem. Gdyby ministerstwo nie weryfikowało w żaden sposób zgłoszonych w aplikacji zakażeń, cały system mógłby przestać działać po kilku chwilach. Przy danych zdrowotnych wpisywanych samodzielnie mogą pojawić się dowcipnisie, którzy zadeklarują zły stan zdrowia. Wtedy wszyscy, którzy znaleźliby się w ich pobliżu, byliby zaznaczeni jako osoby o wysokim ryzyku infekcji. Kolejnym problemem jest wymóg stosowania aplikacji „Kwarantanna domowa", o której rozmawialiśmy wcześniej. Jest ona właśnie przykładem takiego półdobrowolnego rozwiązania, dla którego alternatywą jest ostracyzm społeczny związany z codziennymi wizytami policji w trakcie kwarantanny.

PAP: Wspomniał Pan o połączeniu z serwerem. Na czym polega tutaj zagrożenie?

S.W.: Tworzone przez ministerstwo rozwiązanie ma charakter hybrydowy, czyli nadawanie kluczy odbywa się na poziomie centralnym, na serwerze, ale nie będzie tam kompletu danych

potrzebnych do identyfikacji konkretnego użytkownika. Nie zmienia to faktu, że inne firmy, dysponując informacjami na temat adresów IP urządzenia i karty SIM przypisanej do użytkownika, mogłyby taką bazę uzupełnić i zdeanonimizować użytkowników aplikacji. Ja bym w ogóle szerzej rozpatrywał sprawę prywatności.

PAP: Co Pan ma na myśli?

S.W.: Należałoby zapytać, na ile jesteśmy w stanie pozwalać na ingerowanie w naszą prywatność. Już dzisiaj do każdej karty SIM przypisane są dane konkretnej osoby. Wszystkie nasze dane geolokalizacyjne są więc i tak przechowywane przez firmy telekomunikacyjne. Tymczasem Polska ileś lat z rzędu bije rekordy w liczbie zapytań różnych instytucji publicznych do sektora telekomunikacyjnego o dostęp właśnie do danych geolokalizacyjnych czy billingowych. Dzisiaj w razie potrzeby np. policja może sprawnie określić lokalizację danego telefonu. Dzięki temu, na przykład, gdy dostanie informację, że ktoś grozi samobójstwem, może na miejsce szybko wysłać patrol.

PAP: Jednocześnie większość ludzi używa wielu innych aplikacji, które sporo o nas wiedzą.

S.W.: Firmy reklamowe są zainteresowane różnorodnymi danymi na nasz temat. Google czy Facebook i inne prywatne podmioty gromadzą wszystkie możliwe dane. Niedawno nawet rząd USA zaczął się zastanawiać, czy Google nie zmonopolizowało rynku online, bo każdą osobę korzystającą z ich usług ocenia pod kątem kilku tysięcy parametrów. Pytanie o nową aplikację jest więc trochę głębsze: czy akceptujemy tworzenie nowego źródła danych na nasz temat. Być może dzisiaj nie będzie ono wykorzystywane w niewłaściwych celach, ale sięgnijmy pamięcią ok. 10 lat wstecz. Po rozpracowaniu systemu iPhone'a okazało się, że był w nim plik przechowujący wszystkie dane geolokalizacyjne. Mnóstwo ludzi wtedy protestowało. Teraz nikt nie protestuje, że ma na telefonie może z dziesięć aplikacji, które wysyłają różnego typu dane do prywatnych firm. Nasuwa mi się pytanie – co będzie za kolejną dekadę?

PAP: Czego możemy się obawiać?

S.W.: Dorośnie kolejne, młode pokolenie oswojone już z myślą, że np. taka apka do walki z epidemią to norma i za chwilę będziemy używali pięciu innych zbierających jeszcze więcej informacji.

PAP: Czy możemy więc mówić o pełzającym rozwoju inwigilacji?

S.W.: To się już dzieje. Pojawiają się np. informacje o systemach monitoringowych, rozpoznających twarz. Kilka lat temu w serialu „Czarne lustro" pojawił się motyw aplikacji, w której każdy obywatel mógł przyznać wybraną liczbę gwiazdek innym osobom. Na tej podstawie zmieniał się status danego człowieka. Niedługo później, w innej formie, lecz podobnie działający system Chiny wprowadziły w rzeczywistości. W USA działa Facebook czy Google, a Snowden (Edward Snowden – amerykański demaskator, były pracownik CIA - przyp. PAP) pokazał, że służby bezpieczeństwa mają pełen wgląd w dane o obywatelach. Pojawia się pytanie, w którą stronę to wszystko zmierza i jaki jest limit? Bo jeżeli nie ma limitu, to już teraz

możemy odwiesić prywatność na kołek i nie zastanawiać się, czy ktoś nasze dane będzie wykorzystywał. Przyspieszymy świat o parę lat, wyeliminujemy kilka epidemii, czy rozwiążemy parę problemów związanych z terroryzmem.

PAP: Chyba jednak nie jest Pan zwolennikiem takiego rozwiązania...

S.W.: Pytanie, czy chcemy iść w tym kierunku. Niektórzy mówią jednak, że już zrezygnowaliśmy z prywatności, kiedy wzięliśmy do ręki pierwszy telefon komórkowy, bo łączył się z co najmniej trzema stacjami bazowymi. Na tej podstawie można już określić położenie aparatu z dokładnością do kilku metrów. Po wprowadzeniu sieci 5G, być może ta dokładność wzrośnie z uwagi na większą gęstość anten.

PAP: Liczba zbieranych informacji też może rosnąć. Mówi się już np. o czujnikach medycznych umieszczanych w ciele.

S.W.: Niedawno pojawiło się doniesienie o pracach nad czipem dostosowanym do obecnej pandemii. Taki niewielki układ mógłby wykrywać koronawirusa, ale też markery glukozy, nowotworów albo różnego typu infekcji. Mógłby łączyć się z urządzeniem mobilnym i przesyłać do niego dane. To dobre rozwiązanie na przykład dla osób z cukrzycą. Powstaje jednak pytanie o dobrowolność. Aplikacja ProteGo Safe jest dobrowolna. Pomijając teorie spiskowe i kierując się tylko rozsądkiem, trzeba jednak zastanowić się, kto nam da gwarancję, że np. taki czip nie będzie kiedyś obowiązkowy.

PAP: Na razie ludzie są zachęcani do instalowania aplikacji. To nie wygląda groźnie.

S.W.: Były już jednak dwa inne pomysły, z których się wycofano na wcześniejszym etapie prac nad projektowaniem aplikacji. W pierwszym z nich apka miała być powiązana z numerem telefonu. To łamało zasadę anonimowości. Według drugiego, osoby z aplikacją mogły być uprzywilejowane przy na zakupach w galeriach handlowych czy przy korzystaniu z usług publicznych, a to już oznaczało taką półobowiązkowość. Teraz więc zastanawiamy się, czy powinna ona być całkowicie dobrowolna czy pośrednio obowiązkowa. Za 5-10 lat podstawą może natomiast stać się pośredni obowiązek, a dyskutować będziemy o obowiązku całkowitym.

PAP: Czy ma Pan jakieś rady dla potencjalnych użytkowników – unikać takiej aplikacji, instalować i się nie przejmować? Używać, ale uważać?

S.W.: Nie chciałbym być tutaj tym złym posłańcem zniechęcającym do korzystania z rozwiązań podnoszących nasze bezpieczeństwo. Być może po zaadoptowaniu standardów wprowadzanych przez Apple i Google aplikacja faktycznie zacznie działać w modelu rozproszonym i będzie w maksymalny sposób chronić nasze dane. Ale z drugiej strony ta dyskusja miałaby sens, gdybyśmy nie zezwalali korporacjom i innym mniejszym firmom na śledzenie naszych lokalizacji, wzorców zachowań, budowania profili osobowości, które potem są wykorzystywane do serwowania nam spersonalizowanych reklam i wiadomości.

PAP: Według Pana więc instalować, czy nie instalować?

S.W.: Jeśli jesteście Państwo świadomymi użytkownikami i przy aktualizacji systemu operacyjnego w telefonie przeczytaliście Państwo regulamin zanim go zaakceptowaliście, to do momentu zaadoptowania lepszych standardów prywatności odradzałbym instalowanie ProteGo. Jeśli jednak akceptujecie regulaminy w innych aplikacjach z automatu, bez czytania, to poziom prywatności w kolejnej aplikacji, którą dołożycie do całego ekosystemu, nie ma większego znaczenia.(PAP)

Rozmawiał Marek Matacz

mat/ agt/