Dlaczego aplikacja nie ochroni nas przed COVID-19?

5 maja 2020

W środę (29 kwietnia 2020 r.) rządzący znów postawili Internet na nogi, zapowiadając pierwszy krok w kierunku rozmrożenia gospodarki: otwarcie centrów handlowych. Jednak pod jednym warunkiem: ludzie szturmujący sklepy mieli być zachęcani do instalowania rządowej aplikacji ProteGO Safe, która szacuje ryzyko zarażenia Covid-19. Ministerstwo Rozwoju opublikowało wytyczne, z których wynikało, że do sklepów będzie mogło wejść więcej osób, o ile będą posiadać aplikację.

Już w czwartek, po pierwszej internetowej burzy, kontrowersyjny pomysł znikł z wytycznych Ministerstwa Rozwoju, ale sama aplikacja została udostępniona w sklepie Google Play (w App Store dostępna jest okrojona wersja) i prowokuje wiele pytań. Czy jest bezpieczna i zgodna z RODO? Czy jest zgodna z założeniami rozwiązania, które 10 kwietnia ogłosiły Google i Apple? A może założenia aplikacji zmienią się, kiedy w połowie maja technologiczny duet udostępni zapowiadane API? Po jakie jeszcze środki rząd sięgnie, żeby zachęcać obywateli do jej instalowania?

Obserwując działania rządu, które jeszcze nie układają się w spójną strategię walki z pandemią, nie możemy też uciec od pytania o skuteczność aplikacji. Czy to narzędzie nie odwróci uwagi od ważniejszych środków i nie uśpi czujności ludzi?

Ten tekst jest pierwszą próbą udzielenia odpowiedzi na pytania o aplikację ProteGO Safe, w oparciu o kod i dodatkowe wyjaśnienia, które były opublikowane na Githubie w momencie jego tworzenia (1-4 maja). Jak pokazują doświadczenia ostatnich dni, projekt cały czas ewoluuje. Na parę godzin przed zamknięciem tekstu otrzymaliśmy ważne wyjaśnienia ze strony Ministerstwa Cyfryzacji, które przywołujemy w

odpowiednich miejscach. Jeśli te zapewnienia zostaną wdrożone w kolejnej wersji oprogramowania, niektóre z sygnalizowanych przez nas w tym tekście ryzyk zostaną zniwelowane. Nie rezygnujemy jednak z ich omówienia, ponieważ dotyczą aktualnej wersji aplikacji, już dostępnej dla użytkowników smartfonów z Androidem. Uważamy, że użytkownicy powinni mieć świadomość, z czym się wiąże jej zainstalowanie na telefonie.

Co to jest ProteGO Safe i jak działa?

Według Ministerstwa Cyfryzacji „ProteGO Safe to aplikacja, która pomoże nam w wychodzeniu z najostrzejszych obostrzeń związanych z pandemią". Pełni dwie główne funkcje. Pierwsza – to wspomaganie profilaktyki i możliwość wstępnej oceny stanu zdrowia. Druga – wykorzystująca technologię Bluetooth – rejestruje fakt „spotkania" z innymi urządzeniami i na bazie tego oraz stwierdzonych przypadków zachorowań wyświetla ostrzeżenie o ryzyku zarażenia koronawirusem oraz wskazówki, jak się zachować w takiej sytuacji.

Urządzenia z zainstalowaną aplikacją ProteGO Safe będą emitować, za pośrednictwem Bluetootha, sygnał odbierany przez inne urządzenia z tą samą aplikacją. Telefony przebywające w bliskiej odległości przez ustalony czas będą wymieniać się tymczasowymi kodami – przypadkowymi ciągami znaków, które nie ujawniają tożsamości ich właścicieli, ale pozwalają ustalić, że w danym przedziale czasu właściciele konkretnych urządzeń spotkali się w fizycznej przestrzeni. Dzięki technologii Bluetooth „powstanie zatem swoista sieć połączeń pomiędzy użytkownikami telefonów komórkowych".

Aplikacja będzie w sposób automatyczny szacować ryzyko zarażenia dla każdego użytkownika na podstawie jego osobistej historii spotkanych urządzeń i zweryfikowanych medycznie przypadków zarażenia wirusem z tej sieci społecznej. A następnie przypisywać mu status: zielony („droga wolna") albo

czerwony („poddaj się kwarantannie!”) (informacja z 3 kwietnia 2020 r.). Nadal czekamy na ujawnienie logiki algorytmu wykorzystywanego do szacowania ryzyka, w szczególności przyjętych przez polskie władze założeń co do odległości między urządzeniami i czasu, który jest wystarczający, by doszło do ryzyka zakażenia.

Czy aplikacja jest bezpieczna dla użytkowników i „zgodna z RODO”?

Według zapewnień Ministerstwa Cyfryzacji „aplikacja nie inwigiluje, nie zbiera i nie udostępnia danych użytkowników. Informacje o napotkanych urządzeniach nie zawierają żadnych danych o ich właścicielach, są anonimowe i zakodowane, a do tego przechowywane tylko w telefonie, przez dwa tygodnie. Później są usuwane. Jeśli nie wierzycie, można to sprawdzić w kodzie źródłowym”.

Ministerstwo podkreśla też (w informacji z 29 kwietnia 2020 r.), że „użytkownicy ProteGO Safe są anonimowi. Do tego, aby ją uruchomić nie jest wymagane jakiekolwiek uwierzytelnienie, np. podanie numeru telefonu” (zmiana w stosunku do informacji z 3 kwietnia 2020 r., w której podano, że „instalując aplikację trzeba będzie zarejestrować się swoim numerem telefonu i włączyć Bluetooth”), a „aplikacja jest budowana zgodnie z zasadami wynikającymi z ogólnego rozporządzenia o ochronie danych osobowych (RODO), w tym minimalizacji danych, privacy by design, privacy by default, prawidłowości, integralności oraz poufności.(…) Bazujemy na wytycznych Europejskiej Rady Ochrony Danych Osobowych, Komisji Europejskiej oraz Toolbox opracowanym w ramach sieci eHealth działającej przy Komisji Europejskiej”.

Te zapewnienia nie wytrzymują jednak konfrontacji z głosami niezależnych programistów (także tych, którzy zaangażowani byli w przygotowywanie ProteGO – pierwszej wersji aplikacji rozwijanej w modelu open source, o której pisaliśmy w

kwietniu).

Odnosząc się do wersji 3.0.3 aplikacji ProteGO Safe (aktualnej w dniu przygotowywania tego tekstu), poniżej opisujemy:

– ryzyko deanonimizacji i odtworzenia mapy powiązań społecznych;

– zagrożenie dla bezpieczeństwa użytkowników (stale włączony Bluetooth);< - ryzyko związane z automatycznym podejmowaniem decyzji, które mogą mieć istotne skutki dla ludzi korzystających z aplikacji.

Ryzyko deanonimizacji i odtworzenia mapy powiązań społecznych przez administrację publiczną

W dokumentacji projektu czytamy: „Serwer ProteGO Safe generuje UID i listy Temp ID do rotacji identyfikatorów tymczasowych". Ten niezbyt przejrzysty opis oznacza, że identyfikatory, którymi przez Bluetooth przedstawiają się urządzenia z aplikacją, nie są losowe, lecz nadawane przez serwer. Aplikacja stoi więc w rozkroku między rekomendacjami Komisji Europejskiej (pełna anonimowość użytkowników) a rozwiązaniem TraceTogether stosowanym w Singapurze (tam użytkownicy identyfikowani są numerem telefonu). O ile więc operator serwera (zapewne Ministerstwo Cyfryzacji) nie może mieć pewności, komu przydzielił wskazany identyfikator, o tyle brakujące informacje dostarczy operator sieci komórkowej, który ma przecież możliwość rejestrowania ruchu sieciowego (serwer zna źródłowy numer IP, operator może powiązać go z kartą SIM i abonentem).

„Aplikacje contact tracing można napisać w sposób taki, żeby operator danych nawet gdyby chciał, to nie mógłby ich nadużyć (np. zdeanonimizować i śledzić użytkowników). Można też pisać w modelu scentralizowanym, który nie dość, że musi zakładać

pełne zaufanie społeczności do operatora danych, to nie ubezpiecza operatora od nadużyć w przypadku ataku przez „trzecią stronę". ProteGO Safe wybrało tę drugą opcję" – Jakub Kaluzny, SecuRing (źródło: LinkedIn).

Rozwiązanie przyjęte w wersji 3.0.3 ProteGO Safe ma charakter hybrydowy: jest jednocześnie scentralizowane (bo kluczowe dla działania aplikacji operacje mają miejsce na serwerze) i rozproszone (operator serwera nie ma wszystkich potrzebnych informacji, żeby zdeanonimizować użytkowników aplikacji).

Skąd taka dziwaczna hybryda? Aplikacja ProteGO Safe korzysta z biblioteki programistycznej OpenTrace, będącej darmową implementacją protokołu zastosowanego w singapurskiej aplikacji TraceTogether. Tymczasem twórcy aplikacji TraceTogether już pracują nad jej dostosowaniem do (opisanych niżej) założeń przyjętych przez Google i Apple, a więc nad zmianą modelu na rozproszony.

Podobne zapewnienia dostaliśmy też ze strony Ministerstwa Cyfryzacji (komunikat przesłany 3 maja): „Skupiamy się w 100% na zintegrowaniu aplikacji ProteGO Safe z rozwiązaniem Google i Apple, jak tylko będzie ono gotowe – mówi minister cyfryzacji Marek Zagórski. Jeżeli z jakiegoś powodu to rozwiązanie nie zostanie finalnie udostępnione w najbliższym czasie, będziemy kontynuować modyfikowanie wersji aplikacji opartej o TraceTogether, ale tylko w modelu maksymalnie zdecentralizowanym i spójnym z DP-3T, które także cały czas analizujemy. Będzie to rozwiązanie przejściowe – tylko na czas, dopóki nie będziemy mogli użyć rozwiązania Google i Apple" – dodaje szef MC.

To bardzo dobra wiadomość. Pozostanie przy scentralizowanym modelu przetwarzania danych, przyjętym w wersji 3.0.3 ProteGo Safe, stwarzałoby realne ryzyko dla prywatności użytkowników. W tym modelu nie można wykluczyć, że któraś z kolejnych wersji aplikacji – w imię skuteczniejszej kontroli nad wirusem – zaczęłaby raportować lokalizację użytkownika oraz listę

zarejestrowanych interakcji. Jeśli rozwój narzędzia poszedłby w tym kierunku, rządzący dowiedzieliby się nie tylko gdzie i kiedy przebywaliśmy, lecz także w czyim towarzystwie. Jedyną skuteczną ochroną przed tym scenariuszem jest odseparowanie aplikacji wydawanej przez Ministerstwo Cyfryzacji od unikalnych identyfikatorów urządzeń, zarówno nadawanych jak i odebranych. Takie właśnie założenia realizuje opisany niżej protokół Exposure Notification.

„Jeśli aplikacja pozostanie przy założeniach modelu scentralizowanego, to nie ma możliwości zabezpieczenia przed wykorzystaniem danych przechowywanych na serwerach Ministerstwa Cyfryzacji do innych celów, na przykład śledzenia lokalizacji i kontaktów między osobami zdrowymi. Należałoby zmienić model działania systemu na rozproszony, tworzony zgodnie z zasadą privacy by design – w takim modelu ryzyko de-anonimizacji można ograniczyć do akceptowalnego poziomu" – Jarek Potiuk, Principal Software Engineer, Open Source Committer.

Tymczasem aktualna wersja aplikacji wydaje się niedopracowana. To dodatkowy powód, żeby ją poprawić i tak szybko, jak to możliwe, wypuścić kolejną wersję. Literówki w komunikatach ekranowych sugerują, że przed umieszczeniem aplikacji w sklepie kod nie był poddany przeglądowi. Brakuje opisu zmian w kolejnych wersjach, a funkcja SafetyNet (zabezpieczenie aplikacji przed uruchomieniem na zrootowanych urządzeniach) zostaje znienacka wprowadzona, by po kilku dniach – bez słowa komentarza – zniknąć.

Dla obecnej wersji aplikacji nie broni się też teza Ministerstwa, że „informacje o napotkanych urządzeniach nie zawierają żadnych danych o ich właścicielach". ProteGo Safe 3.0.3 rozsyła przez Bluetooth również informacje o producencie i modelu telefonu. Jeśli ktoś korzysta z unikalnego urządzenia (np. niedostępnego powszechnie w Polsce modelu OnePlus 3), przez cały czas będzie można go jednoznacznie zidentyfikować, niezależnie od zmiennego identyfikatora tymczasowego. Jest to

cecha biblioteki programistycznej OpenTrace wykorzystanej w ProteGO Safe: realizowany przez nią protokół pozostaje niezgodny z postulatami ochrony prywatności, jednak zakres transmitowanych informacji nie został zawężony.

Ryzyko dotyczące bezpieczeństwa i prywatności użytkowników

W opisie aplikacji ProteGo Safe czytamy: „w nieodległej przyszłości […] upoważniony przedstawiciel organu zdrowia zaproponuje użytkownikowi aplikacji zweryfikowanie aplikacji poprzez podanie upoważnionemu przedstawicielowi organu zdrowia kodu z aplikacji". Nigdzie w dokumentacji nie mamy jednak przejrzystego opisu tego procesu, z podziałem na uczestników procesu i rodzaj przekazywanych między nimi informacji. Z tego powodu nikt nie jest w stanie zweryfikować zgodności specyfikacji z powstającym produktem – specyfikacja zwyczajnie nie istnieje.

Co gorsza, w obecnej chwili nie istnieje też kod odpowiedzialny za wysyłkę danych ani za alarmowanie użytkownika o ryzyku infekcji. Kod działający na serwerze ProteGO Safe nie został upubliczniony, więc nie wiadomo, na jakim etapie prac znajduje się ten element systemu. Ma to tym większe znaczenie, że według opisu to algorytmy po stronie serwera mają rozstrzygać, kto ma zostać poinformowany o kontaktach z osobą o potwierdzonej diagnozie.

Twórcy przedstawiają też kontrowersyjną tezę, jakoby analiza „jakości" kontaktu pomiędzy urządzeniami (a więc odległości i czasu, które przekładają się na ryzyko zarażenia) musiała być wykonywana na serwerze centralnym. Uzasadniają to „potrzebą rozszerzenia wykorzystywania aplikacji o urządzenia starsze, na których taka analiza byłaby trudna lub niemożliwa". Stoimy na stanowisku, że obliczeniom wymaganym dla rozproszonego rozwiązania, promowanego przez Google i Apple, podoła programowalny kalkulator, nie mówiąc o przeciętnym smartfonie

(por. dokumentacja Exposure Notification, str. 15).

Dodajmy, że pomysł powiększenia limitu dopuszczalnych osób w sklepie o posiadaczy aplikacji (który pojawił się w wytycznych Ministerstwa Rozwoju dla centrów handlowych, by dzień później zniknąć bez wyjaśnienia) był całkowitą niespodzianką także dla programistów pracujących nad projektem. Wytyczne przewidywały skanowanie kodu QR przy wejściu do sklepu – jednak tu również zabrakło opisu przepływu danych i oceny prywatności rozwiązania.

W odpowiedzi na krytykę ze strony społeczności technologicznej Ministerstwo Cyfryzacji zapewnia (w komunikacie z 3 maja): „Jesteśmy otwarci na wszelkie uwagi, propozycje poprawek, audyty. Na każdym etapie prac publikujemy kod źródłowy aplikacji. Właśnie po to, by ci, którzy się na tym znają, mogli go przeanalizować i jeśli będzie taka potrzeba – wskazali, co możemy zrobić lepiej – mówi minister cyfryzacji Marek Zagórski.(…) Na prośbę społeczności, potwierdzamy, że także tzw. backend umożliwiający funkcjonowanie ProteGO Safe, będzie opublikowany na licencji otwartej. To oznacza, że każda przyszła zmiana w specyfikacji będzie publikowana na gwarantującej transparentność licencji AGPL lub Apache 2.0” – dodaje Justyna Orłowska.

Czekamy zatem na ten kolejny krok, licząc na przejrzysty opis procesów, które wzbudziły nasz niepokój. Jednocześnie trzeba jednak pamiętać, że użytkownik aplikacji nigdy nie będzie miał pewności, jakie operacje faktycznie zachodzą po stronie serwera. Dlatego tak ważną sprawą jest wybór protokołu, który obroni się nawet przy założeniu złej woli operatora serwera.

Ryzyko związane z automatycznym podejmowaniem decyzji (algorytm

oceniający ryzyko zarażenia)

Działanie aplikacji typu ProteGo Safe wymaga profilowania użytkowników i to w oparciu o szczególną kategorię danych osobowych, czyli informacje o stanie ich zdrowia. Na podstawie historii „spotkań" z innymi urządzeniami algorytm będzie szacował ryzyko tego, czy osoba mogła zostać zarażona koronawirusem. Na tej podstawie aplikacja będzie przyznawać każdemu użytkownikowi odpowiedni status (czerwony albo zielony). Z prawnego punktu widzenia to nic innego, jak automatyczne podejmowanie decyzji na podstawie profilowania, o którym mowa w art. 22 RODO. Nie jest dla nas jasne, czy taka decyzja (przyznanie użytkownikowi „czerwonego" statusu w aplikacji) będzie pociągać za sobą skutki prawne, np. interwencję organów administracji sanitarnej i obowiązek poddania się kwarantannie.

Zgodnie z RODO automatyczne podejmowanie decyzji w oparciu o profilowanie dopuszczalne jest wyłącznie na podstawie zgody osoby, której dane dotyczą, lub gdy profilowanie wynika z przepisów. Według obecnych założeń, przyjętych przez Ministerstwo Cyfryzacji, ten drugi scenariusz nie wchodzi w grę, ponieważ aplikacja ma być dobrowolna. Sęk w tym, że aby zgoda na wykorzystanie danych była ważna, nie może ona zostać w żaden sposób wymuszona. Takim wymuszeniem byłoby np. uzależnienie dostępu do przestrzeni publicznej lub usług handlowych od faktu korzystania z aplikacji, a tym bardziej od możliwości przedstawienia „zielonego" statusu na telefonie.

Ale to nie koniec prawnych komplikacji, jakie wiążą się z automatycznym podejmowaniem decyzji. Na gruncie RODO osobie, której dotyczy taka automatyczna decyzja, przysługuje prawo do uzyskania interwencji ludzkiej, czyli możliwość odwołania się do kogoś, kto zweryfikuje, czy prawidłowo doszło do przyznania konkretnego koloru i czy algorytm jednak się nie pomylił. Prawo musiałoby przewidywać takie gwarancje prawne dla użytkowników aplikacji, jeśli przyznawany przez algorytm

status miałby pociągać za sobą istotne skutki (np. uprzywilejowanie przy wejściu do galerii handlowych czy ograniczenia w korzystaniu z usług publicznych).

Wreszcie, automatyczne podejmowanie decyzji to nie tylko problemy prawne. To przede wszystkim ogromne ryzyko błędów (na gruncie statystyki zwanych *false positives*), o których piszemy więcej niżej (w części „Czy ProteGo Safe ma szansę realnie pomóc w walce z epidemią?").

ProteGO Safe a protokół Google i Apple

10 kwietnia konkurujący na co dzień giganci technologiczni ogłosili zawieszenie broni na potrzeby walki z pandemią i wspólne rozwiązanie o nazwie Exposure Notification. To znaczące wsparcie aplikacji do contact tracingu, które z projektu zupełnie karkołomnego czyni go choć trochę realnym. Dzięki specjalnym uprawnieniom przyznanym przez Google i Apple aplikacje takie jak ProteGo Safe mają szansę funkcjonować lepiej niż inne aplikacje działające w tle, które „usypiają" wraz z urządzeniem (czyli przestają emitować sygnał z identyfikatorem).

Projekt zakłada dwie fazy:

Faza 1. Google i Apple publikują protokoły (API), które opracowanym przez instytucje publiczne zajmujące się ochroną zdrowia aplikacjom do monitorowania kontaktów pozwalają na działanie między urządzeniami z systemami operacyjnymi Android i iOS, a przy tym chronią prywatność użytkowników. Podczas instalowania aplikacji, przed jej uruchomieniem, użytkownicy będą pytani o zgodę na regulamin. Firmy planują udostępnienie protokołu w maju.

Faza 2. W kolejnych miesiącach protokół zostanie udostępniony na poziomie systemu operacyjnego, co pozwoli na jego szerokie

rozpowszechnienie – kluczowe dla skutecznego działania contact tracingu. Po zainstalowaniu aktualizacji systemu operacyjnego i wyrażeniu zgody przez użytkownika system będzie wysyłał i odbierał sygnały Bluetooth, tak samo jak w fazie pierwszej, ale bez konieczności instalowania aplikacji.

Rozwiązanie przygotowywane przez Apple i Google, według zapewnień tych firm, będzie współdziałać tylko z autoryzowanymi aplikacjami (wydawanymi pod szyldem publicznych instytucji), które dodatkowo spełniają następujące kryteria:

– szanują wybór użytkownika (a więc są instalowane dobrowolnie),

– zapisują dane wyłącznie na telefonie (nie ma zatem mowy o centralnych bazach danych,

– posługują się anonimowymi, tymczasowymi identyfikatorami (nie kojarzą tych danych np. z adresem IP czy numerem telefonu użytkownika),

– nie śledzą lokalizacji.

Obie firmy zapowiadają, że uniemożliwią korzystanie ze swojego protokołu aplikacjom, które działają inaczej niż w modelu rozproszonym (lokalnie na urządzeniach) lub chcą sięgać po więcej danych (patrz – dokumentacja Apple i Google). Stawką jest to, by zachęcić jak najwięcej osób do skorzystania z tego rozwiązania, co wymaga wysokich standardów ochrony prywatności. W ostatnim ogłoszeniu Google i Apple zapowiadają, że aplikacje korzystające z ich API nie będą miały dostępu do danych o lokalizacji. To wydaje się wykluczać również model mieszany, czyli łączenie Exposure Notification z pomysłami takimi, jak skanowanie statycznych kodów QR przy wejściu do sklepu.

Czy ProteGO Safe jest zgodna z tymi zasadami? 11 kwietnia (dzień po komunikacie Google i Apple) Jakub Lipiński poinformował o wstrzymaniu prac nad własnym narzędziem do

contract tracingu: „Przygotowujemy ProteGO do integracji z API Google i Apple. ProteGO powinno znaleźć się w rękach użytkowników jak najszybciej, aby można było wykorzystać globalne rozwiązanie od pierwszego dni". Z dyskusji programistów wynika jednak, że ta zapowiedź – jak dotąd – nie została zrealizowana. Zdaniem Jarka Potiuka, który rozwijał ProteGO w jego pierwszej fazie, aplikacja przy obecnych założeniach nie przejdzie przeglądu ze strony Apple ani Google, nie będzie więc mogła korzystać z protokołu Exposure Notification.

Ministerstwo Cyfryzacji zapewnia jednak, że pracuje nad zmianą modelu działania aplikacji i jej pełną kompatybilnością z API, które w maju wypuszczą Google i Apple: „Kiedy rozpoczynaliśmy prace nad ProteGO (poprzednia nazwa projektu), Google i Apple nie zapowiedzieli jeszcze prac nad swoim rozwiązaniem, a Singapur nie opublikował kodu źródłowego swojej aplikacji TraceTogether. (…) Teraz mamy już singapurski kod. Wiemy też, że Google i Apple pracują nad swoim pomysłami. Od początku zapowiadamy, że na nie czekamy".

„Dziś Polska jest jednym z pierwszych krajów na świecie, które testują rozwiązanie Google i Apple. Dzięki tygodniom pracy, która do tego doprowadziła, ProteGO Safe może znaleźć się w gronie pierwszych aplikacji opartych o to uznane przez ekspertów narzędzie" – mówi Justyna Orłowska, Pełnomocnik Prezesa Rady Ministrów do spraw GovTech.

Co się stanie, jeśli w połowie maja okaże się, że aplikacja ProteGO Safe nie jest kompatybilna z protokołem Google/Apple?

Po pierwsze, nie będzie skuteczna, bo jako zwykła aplikacja działająca w tle będzie „usypiała" wraz z urządzeniem – czyli kiedy wyłączysz ekran, urządzenie przestanie nadawać sygnały

do innych urządzeń.

Po drugie – w sklepach Google Play i App Store nie ma żadnych mechanizmów gwarantujących spójność kolejnych wersji aplikacji. Nie wystarczy więc jednorazowy audyt kodu potwierdzający, że aplikacja spełnia oczekiwania w zakresie poufności i prywatności. Wydawca aplikacji będzie mógł każdej chwili będzie podmienić zaufaną apkę na nową wersją, wyglądającą tak samo, lecz działającą zupełnie inaczej (oraz mającą niewiele wspólnego z publicznie dostępnym kodem źródłowym). Taka wersja mogłaby na przykład nadawać przez Bluetooth już nie losowy identyfikator, lecz współrzędne domu użytkownika. Co gorsza, niezależni audytorzy będą mieli szansę wykryć to dopiero wtedy, gdy nowa wersja trafi do dystrybucji w sklepie z aplikacjami – a i to przy założeniu, że ktoś faktycznie przejrzy każdą kolejną wydaną wersję.

Od takiego ryzyka wolne będą aplikacje korzystające z protokołu Exposure Notification. Aplikacja aktywuje proces śledzenia kontaktów, lecz za nadawanie losowych identyfikatorów odpowiada kod Google/Apple. Dzięki temu rządzący nie będą mieli pokusy, by samodzielnie zaburzać równowagę między prywatnością użytkowników a skutecznością śledzenia infekcji.

Biorąc pod uwagę możliwe konsekwencje, wszystkim, którzy chcą polskiej aplikacji do śledzenia interakcji społecznych pozostaje trzymać kciuki za wdrożenie zmian, które już zapowiedziało Ministerstwo Cyfryzacji i zapewnienie pełnej kompatybilności z protokołem Exposure Notification.

Czy ProteGo Safe ma szansę pomóc w walce z epidemią?

To pytanie pada na końcu, ponieważ zajmujemy się ochroną danych, a nie epidemiologią, ale dla decydentów politycznych właśnie ono powinno być najważniejsze. Jeśli nie mamy na nie

dobrej odpowiedzi, cały projekt nie ma sensu. Ani Ministerstwo Cyfryzacji, ani Ministerstwo Zdrowia nie przedstawiły jeszcze własnych analiz na poparcie tezy, że aplikacja ProteGO Safe ma realną szansę pomóc w opanowaniu koronawirusa. Dlatego naszą argumentację opieramy na źródłach zagranicznych (m.in. raporcie opracowanym na zlecenie brytyjskiego NHS – polecamy jako przykład tworzenia polityki w oparciu o dowody, nie spekulacje).

Electronic Frontier Foundation uważa, że Bluetooth nie został stworzony do szacowania odległości między użytkownikami. „Takie wykorzystanie technologii Bluetooth nie było testowane i nie ma udowodnionej skuteczności. Opiera się na wykorzystaniu smartfonów, przez co nie obejmie wszystkich [nie każdy ma smartfona]. Aplikacje bazujące na rozwiązaniu oferowanym przez Apple i Google nie są magicznym techno-rozwiązaniem, które mogłoby zastąpić obecne zalecenia ograniczania kontaktów. Ich skuteczność zależy od licznych wyrzeczeń i zaufania, które sprawi, że będzie z niego korzystać maksymalnie dużo osób. Ale niedostateczna ochrona prywatności to zaufanie podważa, a tym samym ogranicza skuteczność aplikacji".

Wyniki eksperymentów przeprowadzonych przez twórców TraceTogether pokazują, że nawet w kontrolowanych warunkach siła wzorcowego sygnału Bluetooth odbieranego przez różne modele telefonów może różnić się stukrotnie (!).

Zagraniczni eksperci zgłaszają też wątpliwości odnośnie skuteczności narzędzi technologicznych, szczególnie, jeśli miałyby one działać w oderwaniu od innych – ważniejszych z perspektywy epidemiologicznej – środków, takich jak masowe testy na obecność wirusa.

Najczęściej pojawiające się wątpliwości:

– żeby aplikacja mogła spełnić swoją funkcję, musi zainstalować ją bardzo dużo osób – badacze spierają się, czy

wystarczy 60% społeczeństwa, czy potrzeba jeszcze więcej. Nawet w Singapurze, często podawanym za modelowy przykład wdrożenia tego rozwiązania, osiągnięto zaledwie 20%, co oznacza, że tylko w 4% losowych spotkań obie strony będą dysponować aplikacją (do tego jej skuteczność w rejestracji każdego kontaktu nie jest gwarantowana);

– skuteczność protokołu Exposure Notification nie jest znana – wciąż może więc okazać się, że jest to bardziej zagranie marketingowe niż realne rozwiązanie problemu śledzenia kontaktów;

– jest wysokie prawdopodobieństwo, że z aplikacji będą korzystać przede wszystkim osoby spoza grup ryzyka i ci, którzy aktywnie unikają zarażenia, przez co dane z niej pochodzące nie będą dawały miarodajnego obrazu rozprzestrzeniania się epidemii;

– liczne fałszywe alarmy (sygnał Bluetooth przechodzi przez ścianę – urządzenia mogą się komunikować, podczas gdy ich użytkownicy nie mają ze sobą styczności) mogą powodować ignorowanie ostrzeżeń;

– dając fałszywe poczucie bezpieczeństwa, aplikacja może usypiać czujność. Przestaniemy zachowywać dystans, zasady higieny, ograniczenie kontaktów;

– niedostateczna dostępność testów sprawi, że osoby ostrzeżone przez aplikację będą musiały się poddać kwarantannie niezależnie od tego, czy są nosicielami wirusa, czy też nie.

Najważniejszy wniosek? Sama aplikacja nic nie da. Może zadziałać tylko jako element planu, w którym podstawową rolę odgrywa polityka wczesnej identyfikacji osób zarażonych i masowe testy.

Wejście w taki społeczny eksperyment, bez mocnych naukowych dowodów na szanse powodzenia, wymaga naprawdę wysokiego poziomu zaufania między państwem i obywatelami. To zaufanie

podkopują takie pomysły, jak przywołany „znikający fragment” z wytycznych Ministerstwa Rozwoju, który warunkował dostęp do przestrzeni publicznej od posiadania aplikacji. W tym kontekście z pewną ulgą czytamy zapewnienie Ministerstwa Cyfryzacji: „Naszym celem jest, aby aplikacja była w pełni bezpieczna. Jest i będzie dobrowolna.(…) Jak pokazują brytyjskie badania (London School of Hygiene & Tropical Medicine) skuteczna izolacja zakażonych oraz wykorzystanie aplikacji typu exposure notification (tego typu aplikacją jest ProteGO Safe) o 44% mogą zredukować ryzyko rozprzestrzeniania się koronawirusa. Jest jednak jeden warunek – z aplikacji musi korzystać co najmniej 50% społeczeństwa. Nasz cel – to 40%. Dlatego tak ważne, by zdobyła zaufanie Polaków”.

Autorstwo: Katarzyna Szymielewicz, Anna Obem, Tomasz Zieliński
Współpraca: Wojciech Klicki
Źródło: Panoptykon.org