DMZ KANCELARIA

Aplikacje do contact tracingu. Czy odzyskamy prywatność po czasach zarazy?

W związku z pandemią COVID-19 państwa na całym świecie rozpoczęły pozyskiwanie danych na niespotykaną dotąd skalę przy wykorzystaniu aplikacji między innymi do śledzenia kontaktów, czyli kontroli osób przebywających na kwarantannie. Niestety w wielu przypadkach aplikacje stosowane przez poszczególne państwa bezzasadnie mogą ingerować w nasze prawo do prywatności. Niestety, nie wszystkie państwa informują przejrzyście swoich obywateli jak wykorzystywane są narzędzia, które umożliwiają ich śledzenie.

Należy pamiętać, że wszelkie wprowadzone środki nadzoru muszą być przede wszystkim oparte o odpowiednią podstawę prawną, proporcjonalne i uzasadnione. I co najważniejsze powinny być ograniczone w czasie – trwać tylko tak długo, jak to konieczne, aby walczyć z pandemią. Pozyskiwanie danych w celu śledzenia osób będących na kwarantannie, przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19 czy w celu śledzenia kontaktów wydaje się zasadne, ale nie możemy zapominać o prywatności. Wydaje się, że nie tak łatwo w przyszłości będzie zrezygnować z przetwarzanych w tych celach danych. Jak wskazują wirusolodzy, po COVID-19 pojawią się kolejne niebezpieczne wirusy. Dlatego przedstawicielom władzy należy patrzeć na ręce i żądać szczegółowych informacji dotyczących wykorzystania danych, żeby szczytny cel pozyskiwania danych nie zmienił się w inwigilację obywateli. W XXI wieku rozwiązania teleinformatyczne oczywiście mogą pomóc w walce z zagrożeniem

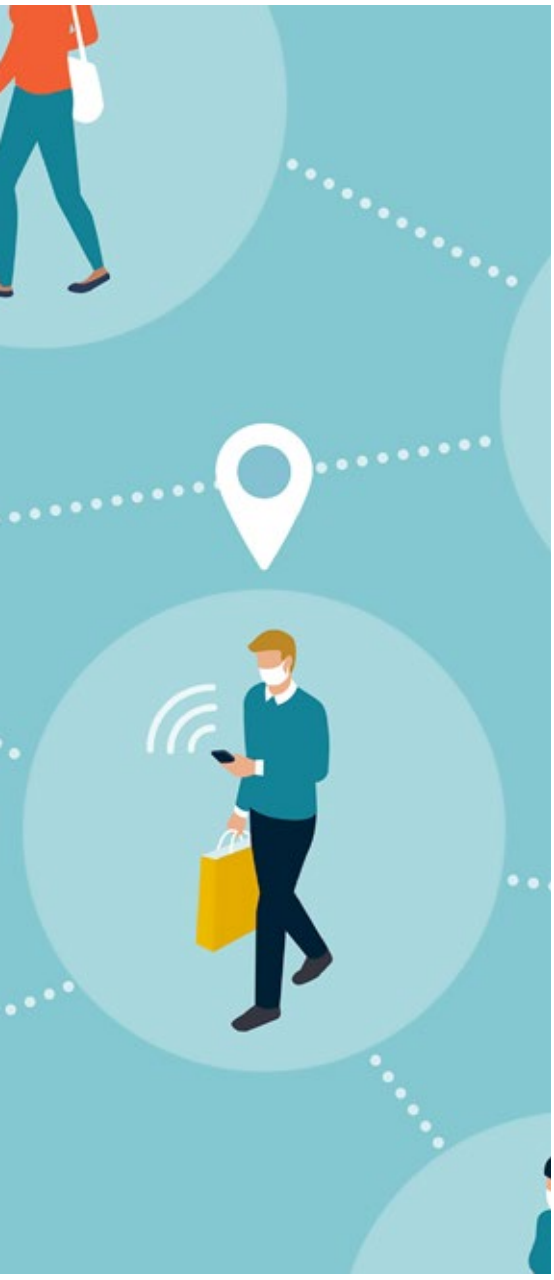
Marcin Zadrożny
Adwokat, posiada wieloletnie doświadczenie w zakresie obsługi prawnej klienta korporacyjnego oraz reprezentacji klientów przed sadami. Ekspert do spraw gospodarczych, z zakresu ochrony danych osobowych i cyberbezpieczeństwa. Audytor wiodący zarządzania bezpieczeństwem informacji (ISO/IEC 27001) i audytor wewnętrzny zarządzania informacjami o prywatności (ISO/IEC 27701).

epidemiologicznym, ale nie pokonają wirus, a mogą być niebezpieczne dla podstawowych praw człowieka.

Contact tracing, czyli śledzenie kontaktów

W „kieszeni" praktycznie każdy z nas ma mały komputer, który umożliwia naszą geolokalizację między innymi poprzez moduł GPS. Contact tracing to rozwiązanie, które pozwala zweryfikować, czy spotkaliśmy osobę zakażoną i jeśli tak, to umożliwia poinformowanie nas o tym. Ale skąd smartfon może wiedzieć, że spotkaliśmy taką osobę? W tym przypadku dzięki modułowi Bluetooth, który każdy ma w swoim smartfonie. Google i Apple w kwietniu tego roku rozpoczęły współprace w związku z wybuchem pandemii, czego efektem było udostępnienie specjalnego interfejs programistycznego (API) w systemach operacyjnych Android i iOS, z którego mogą korzystać dedykowane aplikacje.

Polska w końcu z tego rozwiązania również skorzystała i na początku czerwca udostępniono nową wersję polskiej aplikacji – ProteGO Safe, która wykorzystuje śledzenie kontaktów. Polska aplikacja składa się z dwóch modułów. W pierwszym użytkownik analizuje swój stan zdrowia poprzez aktualizowanie infor-



macji na temat swojego samopoczucia i ewentualnych objawów infekcji. Drugi moduł jest zdecydowanie ciekawszy, ponieważ analizuje nasze kontakty, wykorzystując w tym celu właśnie moduł Bluetooth.

Jak dokładnie działa drugi moduł? Każdy z telefonów z zainstalowaną aplikacją ProteGO Safe przez cały czas skanuje otoczenie w poszukiwaniu innych urządzeń z zainstalowaną aplikacją i jeżeli takie urządzanie znajdzie, to zapisuje tak zwany ślad kontaktu, czyli ciąg znaków, które identyfikują urządzenie. Losowe identyfikatory gromadzone są w telefonie i przechowywane przez 14 dni. Następnie dziennik zawierający losowe identyfikatory jest sprawdzany przez aplikację ProteGO Safe. W ten sposób powstaje baza „kontaktów", z którymi spotkaliśmy się w ostatnim czasie. Nawet jeżeli było to przypadkowe spotkanie, np. w sklepie, na chodniku, w windzie czy w autobusie. Gdy u osoby zostanie potwierdzone zakażenie i osoba ta korzysta z aplikacji otrzyma od służb sanitarnych dedykowany klucz/ PIN, który powinna wprowadzić w aplikacji ProteGO Safe na smartfonie. Gdy to zrobi, każda z osób, która wcześniej miała kontakt z zakażoną osobą, dostanie stosowne powiadomienie w swojej aplikacji. W sytuacji, gdy takie powiadomienie otrzymamy powinniśmy skontaktować się niezwłocznie ze służbami sanitarnymi i postępować wedle ich zaleceń. Jeżeli okazałoby się, że i my jesteśmy chorzy, dostaniemy również dedykowany klucz, który powinniśmy wprowadzić w aplikacji i tym samym osoby, które miały z nami kontakt nawet przypadkowy i mają zainstalowaną aplikację, otrzymają stosowne powiadomienie. Aplikacja obecnie w Polsce jest dobrowolna, może ją pobrać każdy. Jednakże jej skuteczność zależy od powszechności jej stosowania.

Wszystko wydaje się piękne, ale co z naszą prywatnością? Jakie dane pozyskuje polska aplikacja?

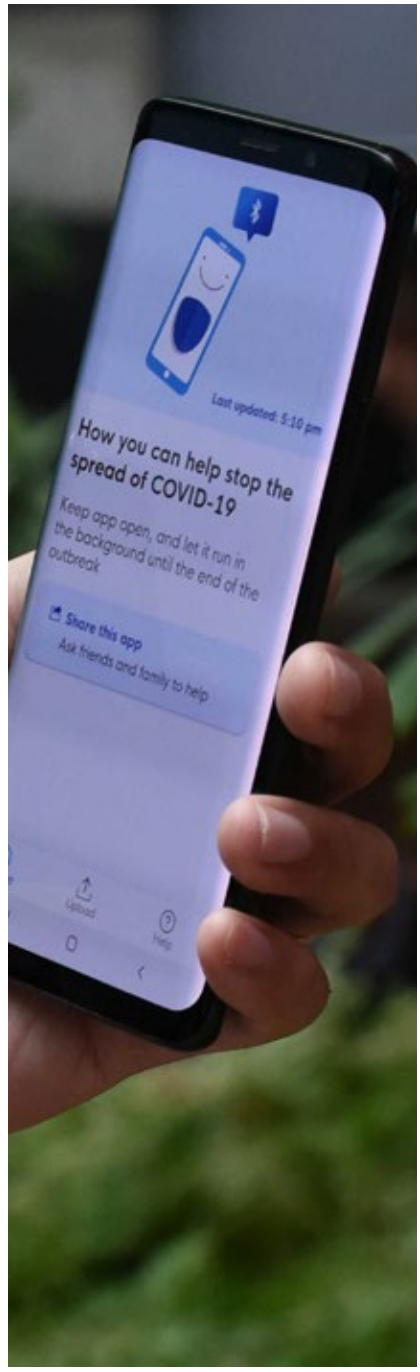
Z komunikatu z systemu Apple, tj. iOS wynika, że: „aby lepiej zrozumieć rozprzestrzenianie się choroby, każdy kontakt z osobą z potwierdzonym zakażeniem spowoduje udostępnienie autoryzowanej aplikacji czasu jego trwania, daty oraz mocy sygnału Bluetooth. Żadne identyfikujące Ciebie dane nie są udostępnianie." Ministerstwo Cyfryzacji, które zleciło przygotowanie aplikacji ProteGO Safe zapewnia, że użytkownicy ProteGO Safe są zupełnie anonimowi. Ministerstwo Cyfryzacji podkreśla, że smartfony wymieniają się jedynie identyfikatorami, których nie można powiązać z konkretną osobą, a sama aplikacja nie wysyła żadnych danych pozwalających na identyfikację konkretnego użytkownika na serwery. Tak w teorii.

Tymczasem pod koniec kwietnia programiści współpracujący przy tworzeniu ProteGO Safe, informowali, że korzystanie z aplikacji wcale nie jest anonimowe, ponieważ Ministerstwo Cyfryzacji może i tak łatwo uzyskać informację o tożsamości użytkowników aplikacji. W polskiej aplikacji został zaimplementowany gwarantujący prywatność protokoł contact tracingu od Google i Apple o czym była mowa powyżej, ale niestety sama aplikacja zbudowana została w oparciu o WebView (PWA). Ma to swoje negatywne konsekwencje polegające w uproszczeniu na tym, że kod aplikacji ładowany jest z serwera. W związku z czym, o każdym otwarciu aplikacji dowie się serwer ministerstwa i pozyska określone dane o urządzeniu użytkownika aplikacji. Krytyka takiego rozwiązania spowodowała, że Minister Cyfryzacji zapowiedział zmiany w aplikacji dotyczące wykorzystania WebView.

Niestety ryzyko śledzenia nas poprzez tego typu aplikacje zawsze istnieje i dlatego budzi to w dalszym ciągu kontrowersje. W czerwcu norweski organ nadzorczy odpowiedzialny za ochronę danych osobowych zakazał tymczasowo stosowania podobnej aplikacji do ProteGO Safe. W ocenie norweskiego organu nadzorczego aplikacja Smittestopp zbierała zbyt duże danych osobowych o jej użytkownikach, w tym pozyskiwała dane o lokalizacji i informacje

o kontakcie użytkowników z innymi osobami. Aplikacja wykorzystywała zarówno GPS, jak i Bluetooth, do śledzenia ruchów ludzi praktycznie w czasie rzeczywistym oraz pozyskiwała informacje z kim użytkownicy aplikacji mają kontakt. Informacje następnie miały być przechowywane przez okres 30 dni. Ostatecznie rząd Norwegii wycofał się z planów wdrożenia aplikacji do śledzenia kontaktów z uwagi na spór wokół prywatności użytkowników toczący się pomiędzy Norweskim Instytutem Zdrowia Publicznego, a krajowym organem nadzorczym odpowiedzialnym za ochronę danych osobowych. Rząd Norwegii ostatecznie zgodził się z argumentami, że niski wskaźnik rozprzestrzeniania się wirusa w kraju sprawia, że gromadzenie danych osobowych mieszkańców kraju przez aplikację śledzącą nie znajduje uzasadnienia.

Z podobnych systemów korzysta coraz więcej krajów na całym świecie. Na pewno aplikacje śledzące mogą pomóc zrozumieć sytuację epidemiologiczną, jak również ograniczyć rozprzestrzenianie się wirusa, jednakże muszą chronić naszą prywatność, nie mogą być inwazyjne i powinny gwarantować bezpieczeństwo przetwarzania danych osobowych. Stan pandemii pokazał, że przepisy RODO są potrzebne i obywatele krajów spoza UE dopiero teraz się o tym przekonują. Tytułem przykładu, w USA trwa dyskusja o informatycznych sposobach śledzenia ludzi, przy braku w większości stanów USA przepisów o ochronie prywatności. Rosyjska aplikacja do monitorowania przestrzegania przez zarażonych obywateli zaleconego reżimu sanitarnego ma dostęp między innymi do połączeń, lokalizacji, aparatu, pamięci urządzenia. Wiele rządów azjatyckich z tego samego powodu, śledzi ludzi przez smartfony, bez ich uprzedniej zgody. W Indiach natomiast władze wprowadziły obowiązkową aplikację pod nazwa Aarogya Setu, która



to ocenia ryzyko infekcji użytkowników na podstawie między innymi ich lokalizacji, odbywanych podróży i informacji medycznych.

EROD o aplikacjach do walki z pandemią

W Unii Europejskiej, Europejska Rada Ochrony Danych (EROD) dynamicznie zareagowała na kryzys spowodowany COVID-19 i sposobem wykorzystania aplikacji wspierających walkę z pandemią. Już w kwietniu podczas posiedzenia plenarnego, EROD przyjęła pismo dotyczące projektu wskazówek Komisji Europejskiej w sprawie aplikacji wspierających walkę z pandemią COVID-19[1]. W ocenie Europejskiej Rady Ochrony Danych podczas tworzenia aplikacji powinny być wykorzystywane mechanizmy wynikające z RODO, w tym ochrona danych w fazie projektowania i domyślna ochrona danych. W ocenie EROD istotnym jest również udostępnienie publiczne kodu źródłowego aplikacji w celu jak najszerszej jej kontroli.

EROD nie zwalnia tempa, ponieważ podczas posiedzenia plenarnego, które miało miejsce 16 czerwca 2020 Europejska Rada Ochrony Danych przyjęła kolejne oświadczenie[2] tym razem w sprawie interoperacyjności aplikacji służących ustalaniu kontaktów zakaźnych, opierając się na Wytycznych EROD 4/2020 w sprawie wykorzystywania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych w kontekście pandemii COVID-19.

To co z naszą prywatnością po czasach zarazy?

Tego niestety nikt nie jest wstanie przewidzieć. Nie wiadomo, kiedy czas zarazy się skończy. Obecnie myślimy o kolejnej fali zakażeń. Jednakże tu i teraz powinniśmy patrzeć na ręce władzy demokratycznej. Państwo potrzebuje narzędzi cyfrowych do walki z kryzysem wywołanym stanem epidemii, ale zbyt daleko posunięte pozyskiwanie danych i inwazyjna ingerencja w prywatność może być niebezpieczna dla obywateli, w tym prowadzić do ich profilowania.

[1] https://uodo.gov.pl/pl/file/2839
[2] https://uodo.gov.pl/pl/file/2951