Rząd znów narzuca ludziom aplikacje. Po co?

21 września 2022

Resort spraw wewnętrznych chce wymusić na sprzedawcach smartfonów instalowanie na urządzeniach aplikacji RSO i Alarm 112. Pomysł od razu wzbudził kontrowersje. Szybko pojawiły się pytania o możliwość łatwiejszego inwigilowania obywateli oraz o bezpieczeństwo aplikacji. Nie jest też wcale oczywiste, czy rząd może wymusić instalowanie czegokolwiek w telefonach.

Aplikacje na pomoc

W opublikowanym 5 września 2022 r. projekcie ustawy o ochronie ludności oraz o stanie klęski żywiołowej znalazły się dwa przepisy, które postawiły bańkę cybertech na nogi: „Autoryzowany sprzedawca, o ile jest to techniczne możliwe, obowiązany jest do preinstalacji aplikacji mobilnej RSO na telekomunikacyjnych urządzeniach końcowych sprzedawanych użytkownikom" (art. 64) oraz „Autoryzowany sprzedawca, o ile jest to technicznie możliwe, obowiązany jest do preinstalacji aplikacji mobilnej Alarm112 na telekomunikacyjnych urządzeniach końcowych sprzedawanych użytkownikom" (art. 148).

W uzasadnieniu do projektu nie znajdziemy odpowiedzi na nurtujące nas pytania: czemu ma służyć nowy obowiązek ani dlaczego tego celu nie da się zrealizować przy pomocy innych środków, np. nieobowiązkowych aplikacji. O ile możemy przyjąć, że preinstalacja aplikacji RSO jest jednym z elementów unowocześniania form wczesnego powiadamiania społeczeństwa o zagrożeniach (s. 5 uzasadnienia), o tyle aplikacja Alarm112 w ogóle się w uzasadnieniu nie pojawia.

„RSO – Regionalny System Ostrzegania (RSO) to bezpłatna aplikacja mobilna powstała przy współpracy Ministerstwa Spraw Wewnętrznych i Administracji z Telewizją Polską S.A. Aplikacja

ta jest elementem szerszej usługi informowania społeczeństwa o zagrożeniach na terenie Polski za pośrednictwem różnych kanałów informacyjnych: strony internetowe wojewodów, paski informacyjne i telegazeta w telewizorach odbierających sygnał naziemny DVB oraz internetowa telewizja hybrydowa hbbtv" – czytamy w oficjalnej informacji w sklepie z aplikacjami. Aplikacja została pobrana 100 tys. razy, a jej ostatnia aktualizacja jest datowana na 17 lipca 2018 r.

Aplikacja Alarm112 ma jeszcze mniej pobrań (10 tys.), a ostatnia aktualizacja pochodzi z 7 grudnia 2020 r. „Celem aplikacji mobilnej jest zapewnienie możliwości przekazywanie zgłoszeń alarmowych na numer alarmowy 112 bez konieczności używania komunikacji głosowej, co powoduje, że rozwiązanie jest również przyjazne dla osób niepełnosprawnych. Przy pomocy aplikacji użytkownik ma możliwość wykonania zgłoszenia alarmowego z terenu Polski o zaistnieniu zagrożenia: życia, zdrowia, bezpieczeństwa, mienia, środowiska naturalnego do Centrum Powiadamiania Ratunkowego". Aplikacja została stworzona dla osób z niepełnosprawnościami. Dzięki niej np. osoby niesłyszące mogą wezwać pomoc.

Wszyscy mają apki? Mam i ja!

Od telekomunikacji przez rozrywkę i finanse po usługi publiczne – aplikacje służą już nie tylko do korzystania z podstawowych funkcji smartfona. Stają się nieodzownym interfejsem do usług bankowych, mediów, klubów sportowych, sieci handlowych. Polski rząd też ma na tym polu przynajmniej jeden sukces: superpopularną aplikację mObywatel (ponad 5 mln pobrań). Mieszkańcy miast często korzystają też np. z aplikacji do opłacania parkowania i kupna biletów czy wynajmowania jednośladów.

To ważne, że rząd wychodzi naprzeciw oczekiwaniom społecznym i proponuje aplikacje ułatwiające korzystanie z usług publicznych. Zwłaszcza jeśli rozwiązują one realne potrzeby

(jak aplikacja Alarm112, umożliwiająca wezwanie pomocy osobom niesłyszącym i wszystkim tym, którzy z różnych powodów nie będą w stanie wykręcić numeru alarmowego i porozumieć się z dyspozytorem). Problem pojawia się dopiero wtedy, gdy władze próbują ludziom narzucić swoje aplikacje, co do których społeczeństwo ma ograniczone zaufanie (m.in. dlatego, że kod aplikacji jest zamknięty i nie przeszedł niezależnego audytu).

Jak wdrożyć aplikację budzącą zaufanie

Na kanwie doświadczeń z aplikacjami Kwarantanna domowa i ProteGO Safe w 2020 r. przygotowaliśmy apel Technologia w walce z koronawirusem. 7 filarów zaufania – listę zasad, które powinny być respektowane, żeby powstające narzędzia były z jednej strony zgodne z wymogami ochrony danych, a z drugiej – budziły społeczne zaufanie. Pod apelem podpisało się ponad 200 osób, m.in. ekspertów i ekspertek z zakresu nowych technologii, prawa, bezpieczeństwa cyfrowego, prywatności, programistów.

W pierwszej kolejności rząd powinien przekonać nas, że obowiązkowa instalacja tych aplikacji jest naprawdę konieczna – bo nie ma innego sposobu rozwiązania danego problemu. Uzasadnienie nas w tej kwestii nie przekonuje. Mamy też wątpliwości, jak szybko udałoby się to rozwiązanie wdrożyć w praktyce: smartfonów nie wymieniamy co miesiąc ani nawet co roku (a obowiązek miałby dotyczyć nowych urządzeń). Słyszymy też wątpliwości speców od narzędzi (Niebezpiecznik, Informatyk Zakładowy), że 1) nie wszystkie systemy operacyjne (komercyjne i niezależne) pozwolą na wpuszczenie obcej aplikacji; 2) nie wiadomo, kim właściwie jest „autoryzowany sprzedawca” z projektowanych przepisów; 3) a w ogóle to apka zadziała dopiero, kiedy ją otworzymy i wyrazimy zgodę na powiadomienia.

Załóżmy jednak, że rząd ma mocne argumenty przemawiające za tym, że dana apka jest najlepszym rozwiązaniem zdiagnozowanego

problemu, a wyzwania techniczne uda się pokonać (rozważania na temat tego, czy i jak jest to możliwe, zostawiamy specjalistom). Wówczas na pierwszy plan wysuwają się pytania dotyczące ochrony prywatności. Czy aplikacja jest zaprojektowana tak, żeby nie gromadzić innych danych, niż to obiektywnie niezbędne dla powiadomienia ratowników? Kto pisze jej kod? Czy kod jest (będzie) otwarty i możliwe jest (będzie) poddanie go niezależnemu audytowi? Skąd mamy mieć pewność, że aplikacja działa dokładnie tak, jak zostało to opisane w jej regulaminie i polityce prywatności, i że (z czasem) nie posłuży rządowi do innych celów?

Politykę prywatności rządowych aplikacji znajdziesz na stronie TVP

Chcielibyśmy też wiedzieć więcej o tym, kto jest administratorem danych, gdzie trafiają dane, jak długo są przechowywane itd. (zwłaszcza w przypadku aplikacji Alarm112, która wymaga podania imienia, nazwiska czy numeru PESEL). Ani w sklepie z aplikacjami dla Androida, ani na stronach gov.pl dotyczących aplikacji nie znaleźliśmy polityki prywatności i regulaminu aplikacji Alarm 112. Z polityką prywatności Alarmu 112 można zapoznać się dopiero po zainstalowaniu aplikacji. Politykę prywatności aplikacji RSO znaleźliśmy… na stronie TVP.

Po pierwszej lekturze mamy więcej pytań niż odpowiedzi. Z jednej strony polityka prywatności RSO uspokaja, że „aplikacja nie zbiera żadnych danych osobowych” oraz że „aplikacja nie śledzi ani nie zapamiętuje (i nie przekazuje na żadne serwery) położenia Użytkownika w czasie korzystania z aplikacji”. Niżej pojawia się jednak ważne doprecyzowanie: „Dane o położeniu pobierane są tylko wtedy, gdy wymaga tego skorzystanie z powiązanej z nimi funkcji przesłania komunikatu”. Czyli jednak przetwarza dane!

Z kolei po zainstalowaniu Alarmu 112 niezbędna jest

rejestracja (łącznie z PESEL-em), traktowana jako „wyrażenie zgody” na przetwarzanie danych. Na tym etapie pojawia się możliwość zapoznania z polityką prywatności. Napisane jest w niej, że dane o położeniu pobierane są tylko wtedy, gdy wymaga tego skorzystanie z powiązanej z nimi funkcji – przesłania zgłoszenia alarmowego do Centrum Powiadamiania Ratunkowego.

Jeśli rząd chce uspokoić opinię publiczną, powinien – już na etapie prac legislacyjnych – zasięgnąć opinii UODO i przygotować dla obu aplikacji rzetelną ocenę wpływu na ochronę danych osobowych. To nie tylko dobra praktyka, ale i obowiązek wynikający z RODO, jeśli to rozwiązanie faktycznie miałoby stać się obligatoryjne i – co za tym idzie – oznaczałoby przetwarzanie danych na masową skalę.

Polski rząd idzie pod prąd europejskich regulacji

Akt o rynkach cyfrowych (DMA, Digital Markets Act) przewiduje, że użytkownicy urządzeń mobilnych powinni mieć możliwość odinstalowania dowolnej aplikacji na smartfonie. DMA wprawdzie dotyczy największych platform z sektora prywatnego – po to, żebyśmy mogli odinstalować z naszych smartfonów aplikacje monopolistów, np. Facebooka czy Google TV. Tymczasem polski rząd idzie na przekór trendom i każe instalować na smartfonach dwie swoje aplikacje. Czy to naprawdę konieczne? I czy ma szansę zadziałać tak, jak rząd sobie to wyobraża?

Czy rządowe aplikacje będą nas inwigilować?

Od dnia opublikowania projektu przepisów wprowadzających obowiązek preinstalacji aplikacji, trafiają do nas liczne pytania o inwigilację. Zacznijmy od tego, że polskie przepisy nie chronią nas przed inwigilacją. Krajowa Administracja Skarbowa, Policja, CBA, ABW i inne służby mogą sprawdzać

każdego i każdą z nas bez szczególnych ograniczeń. Założenie podsłuchu wymaga wprawdzie zgody sądu, a sprawdzanie lokalizacji telefonów powinno być raportowane – ale to za mało, żeby można było mówić o kontroli. Szerokie uprawnienia do kontrolowania nas ma też np. ZUS.

Polskie władze nadużywają naszego zaufania na co dzień (zwiększając uprawnienia służb i pozostawiając je poza kontrolą) i od święta (używając Pegasusa wobec osób publicznych). Preinstalowana rządowa aplikacja to prosty kanał ataku – wystarczy, że ktoś wpadnie na pomysł, żeby z niego skorzystać. Jak komentuje dla nas Michał „rysiek" Woźniak:

„Pierwszym krokiem przy włamywaniu się na jakiekolwiek urządzenie jest uzyskanie możliwości uruchomienia złośliwego kodu w kontekście jakiejkolwiek aplikacji. To jeszcze nie wystarcza do przejęcia kontroli nad urządzeniem, ale jest koniecznym pierwszym krokiem. Pegasus na przykład wykorzystywał do tego luki w iMessage.

Czy te potencjalnie obowiązkowe aplikacje będą wystarczająco dobrze zabezpieczone, by nie dało się ich wykorzystać w takim pierwszym kroku? Czy rząd (który już pokazał, że chętnie wykorzystuje Pegasusa do szpiegowania opozycji) nie skusi się na uproszczenie sobie przyszłych włamań, poprzez umieszczenie w tych aplikacjach funkcji pozwalających taki pierwszy krok we włamaniu wykonać bez konieczności przełamywania zabezpieczeń innej aplikacji? Nie musi przy tym umieszczać tych funkcji dziś, może je dodać przed aktualizacją, kiedy będą »potrzebne«".

Mając to wszystko na uwadze, wracamy do powtarzanej przez nas od ponad dekady mantry: narzędzia mogące służyć do nadzoru państwo powinny być stosowane z rozwagą i pod kontrolą.

Autorstwo: Anna Obem, Wojciech Klicki, Katarzyna Szymielewicz
Współpraca: Dominika Chachuła
Źródło: Panoptykon.org

Źródłografia

1. https://legislacja.rcl.gov.pl/docs/2/12363754/12909374/12909375/dokument573203.DOCX

2. https://legislacja.rcl.gov.pl/docs/2/12363754/12909374/12909375/dokument573205.DOCX

3. https://panoptykon.org/7-filarow-zaufania

4. https://niebezpiecznik.pl/post/rzad-chce-aby-sprzedawcy-domyslnie-instalowali-2-apki-od-mswia-na-smartfonach-polakow/

5. https://informatykzakladowy.pl/dlaczego-mswia-nie-zainstaluje-wszystkim-swojej-aplikacji/

6. https://komunikaty.tvp.pl/aplikacja_mobilna