Odpowiadamy na pytania o aplikację „Kwarantanna domowa”

2 kwietnia 2020

Państwo od lat nie potrafi przenieść części swoich działań na platformy online. Wymaga jednak wysokich kompetencji cyfrowych od swoich obywateli i obywatelek: zgodnie z uchwalonymi właśnie przepisami, aplikacja „Kwarantanna domowa” ma być obowiązkowa.

Ustawa o zmianie niektórych ustaw w zakresie systemu ochrony zdrowia związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 przewiduje, że obywatele i obywatelki przebywający na kwarantannie będą musieli zainstalować aplikację mobilną, żeby ułatwić służbom kontrolę nad przestrzeganiem jej zasad. Z tego obowiązku mają być wyłączone tylko „osoby z dysfunkcją wzroku (niewidzące lub niedowidzące)” i „osoby, które złożyły oświadczenie, że w ogóle nie mają telefonu lub ich telefon uniemożliwia instalację tego oprogramowania”. Każdy, kto chciałby się powołać na te szczególne okoliczności, będzie musiał złożyć oświadczenie pod rygorem odpowiedzialności karnej.

Warto w tym miejscu przypomnieć, że aplikacja „Kwarantanna domowa” została wprowadzona przez Ministerstwo Cyfryzacji jako narzędzie dobrowolne i do tej pory osoby przebywające na kwarantannie nie były ani zmuszane, ani nawet namawiane do jej instalowania. W odpowiedzi na nasze pytanie o cel wprowadzenia tego narzędzia jeszcze w ubiegłym tygodniu Ministerstwo zapewniało: „Nasza aplikacja nie jest odpowiedzią na łamanie kwarantanny, ale narzędziem ułatwiającym jej odbycie”. Najwyraźniej w przeciągu kilku dni intencje władzy

diametralnie się zmieniły.

Narzucenie obywatelom i obywatelkom podlegającym kwarantannie obowiązku instalowania aplikacji, która monitoruje ich lokalizację i zbiera dane biometryczne, uważamy za problematyczne z następujących powodów.

Jakie dane o użytkowniku zbiera aplikacja? Czy nie zbiera ich za dużo?

Według regulaminu aplikacja zbiera: ID obywatela – techniczny identyfikator, imię, nazwisko, numer telefonu, deklarowany adres pobytu, zdjęcie, lokalizację obywatela, datę końca kwarantanny. Jednak po kliknięciu opcji Uprawnienia w sklepie Google Play okazuje się, że aplikacja ma szersze uprawnienia, np.:

– widzi, z jaką siecią Wi-Fi się łączysz;

– odczytuje zawartość pamięci Twojego urządzenia i może modyfikować lub kasować jego zawartość;

– odczytuje identyfikator urządzenia i informacje o połączeniu;

– ma dostęp do aparatu i mikrofonu, może więc nagrywać dźwięk i wideo;

– odczytuje lokalizację na bazie danych z sieci komórkowej i GPS;

– ma też kontrolę nad latarką.

Po zainstalowaniu aplikacji okazuje się, że sprawdza też, jakie inne aplikacje są zainstalowane na telefonie i czy nie ma wśród nich takiej, która oszukuje lokalizację.

O tych funkcjach nie ma informacji w regulaminie aplikacji. Zapytaliśmy o nie Ministerstwo Cyfryzacji. Oto odpowiedź: „Aplikacja korzysta z dostępu do lokalizacji na podstawie GPS, sieci komórkowej i Wi-Fi. Nie rejestruje (nie odnotowuje), z jakiej sieci korzysta Obywatel. Zgodę na dostęp do lokalizacji Obywatel wyraża, akceptując systemowe powiadomienie. Powiadomienie pojawia się w momencie pierwszego uruchomienia aplikacji. (…) Podczas wykonywania pierwszego zadania widoczne jest pytanie o zgodę na dostęp do zdjęć, multimediów i plików na urządzeniu. Wykorzystywany jest on do zapisania wykonanego zdjęcia i odczytania tego zdjęcia w celu przesłania do automatycznej weryfikacji.”

Ministerstwo poinformowało nas, że aplikacja nie korzysta z pozostałych funkcji (latarki czy nagrywania dźwięku). Gdyby np. chciała uruchomić mikrofon, osoba korzystająca z aktualnego systemu Android albo iOS otrzymałaby analogiczne powiadomienie jak w przypadku dostępu do zdjęć, multimediów i plików na urządzeniu. Nic takiego się nie dzieje, nie mamy zatem powodów, by wątpić w zapewnienia Ministerstwa.

Udało nam się potwierdzić, że aplikacja nie sprawdza lokalizacji użytkowników przez cały czas, a jedynie podczas uruchamiania i wykonywania przez użytkownika zadania. Ministerstwo zapewnia też, że aplikacja korzysta z aparatu wyłącznie po to, by robić zdjęcia. Nie nagrywa krótkich filmików, czego obawiali się eksperci komentujący zabezpieczenia aplikacji przed typowymi próbami oszustw ze strony użytkowników.

Co o tym wszystkim sądzimy? Uważamy, że zakres zbieranych przez aplikację danych jest adekwatny do jej celu, a więc zweryfikowania, czy użytkownik nie narusza zasad kwarantanny domowej. Z jednym zastrzeżeniem: przesyłanie zdjęć twarzy na serwery Ministerstwa Cyfryzacji nie jest niezbędne, ponieważ analiza zgodności twarzy i weryfikacja metadanych zdjęcia (czasu wykonania i geolokacji) mogłaby się też odbywać lokalnie, na urządzeniu użytkownika.

Rozwiązanie zastosowane w aplikacji „Kwarantanna domowa” oznacza, że (mniej lub bardziej twarzowe) zdjęcia osób wraz ze szczegółami widocznymi w tle, które niekoniecznie chciałyby pokazywać, trafiają na serwery, skąd mogą trafiać dalej w bliżej nieokreślonym celu i być przetwarzane na różne sposoby. Zamiast wysyłać zdjęcia na serwery Ministerstwa lepiej z punktu widzenia prywatności byłoby wykonywać analizę zgodności twarzy na urządzeniu. Taki algorytm (np. FisherFace) mógłby tworzyć lokalny model cech biometrycznych. Suma kontrolna takiego wzoru mogłaby być przechowywana na serwerze, by weryfikować, czy wzór się nie zmienił w czasie. W przypadku nadejścia żądania weryfikacji lokacji oraz twarzy sprawdzane byłoby tylko to, czy lokalny wzorzec się nie zmienił, a następnie – również lokalnie – następowałoby porównanie twarzy z wzorcem. Dodatkowym zabezpieczeniem byłoby wzbogacenie algorytmu o mechanizm atestacji zdalny pomiar stanu zdrowia urządzenia i tego, czy użytkownik czegoś nie kombinuje – komentuje Mateusz Chrobok, entuzjasta biometrii behawioralnej, wiceprezes do spraw biometrii behawioralnej w Buguroo.

Ministerstwo Cyfryzacji wybrało jednak rozwiązanie scentralizowane. Uzasadnia swój wybór w następujący sposób: „Zdjęcia weryfikowane są po stronie serwera. O wiele łatwiej oszukać pojedyncze urządzenie (czyli telefon) niż zabezpieczony serwer. Tym samym weryfikacja po stronie serwera jest bezpieczniejsza dla Obywatela. Należy pamiętać, że nie każdy Obywatel ma zabezpieczony telefon, choćby w podstawowym stopniu”. Zgoda, bezpieczeństwo danych jest w tej dyskusji istotnym argumentem.

Jak długo mają być przechowywane dane i czy jest to uzasadnione?

Zgodnie z par. 14 regulaminu Minister Cyfryzacji będzie przechowywać dane osobowe użytkowników aplikacji przez 6 lat, czyli okres przedawnienia roszczeń według Kodeksu cywilnego,

liczony od momentu dezaktywacji aplikacji. Przechowywanie danych przez czas przedawnienia roszczeń to rutynowa praktyka, która sprawdza się w relacjach komercyjnych i przy przetwarzaniu zwykłych danych. Jednak aplikacja „Kwarantanna domowa” nie jest zwykłą usługą. To administracyjne narzędzie kontroli, zbierające wrażliwe dane na dużą skalę.

Z jednej strony (w punkcie 10 regulaminu) Ministerstwo Cyfryzacji zastrzega, że cała odpowiedzialność za poprawne działanie aplikacji (m.in. jej aktualizowanie) i utrzymanie dostępu do sieci telekomunikacyjnej spoczywa na użytkownikach. Z drugiej strony uspokaja na swojej stronie, że jeśli raport nie dotrze na czas, jest to tylko sygnał dla policji, że powinna wybrać się na miejsce odbywania kwarantanny i sprawdzić, czy osoba jest w domu. A więc o nałożeniu ewentualnej kary finansowej zdecyduje nie brak raportu z aplikacji, ale niezależne ustalenia dokonane przez policję.

Naszym zdaniem Ministerstwo Cyfryzacji na swoich serwerach powinno przechowywać raporty (zdjęcia) tylko tak długo, jak to konieczne do sprawdzenia, czy konkretna osoba przestrzegała zasad kwarantanny. Argument „z dochodzenia roszczeń” zupełnie nas w tym kontekście nie przekonuje. Przesłane przez obywateli zdjęcia i dane o lokalizacji powinny być usuwane natychmiast po ich prawidłowym zweryfikowaniu (tzn. ustaleniu, że objęta kwarantanną osoba przebywa pod swoim adresem).

W odpowiedzi na nasze wątpliwości Ministerstwo Cyfryzacji doprecyzowało: „Nie tworzymy bazy zdjęć jako ustrukturyzowanego zbioru do przeszukiwania po identyfikatorze obywatela, np. PESEL. Składujemy je w celach określonych w regulaminie. Zdjęcia będą usuwane zaraz po odbyciu kwarantanny”.

Z tej odpowiedzi wnioskujemy, że przez okres 6 lat będą przechowywane jedynie podstawowe dane, podawane przez użytkowników i użytkowniczki przy instalowaniu aplikacji, ale już nie raporty przez nich przesyłane. Do takiego zakresu nie

mamy zastrzeżeń.

Czy dane o lokalizacji i zdjęcia tysięcy ludzi mogą zostać wykorzystane do innego celu, np. trenowania algorytmów rozpoznawania twarzy?

Z regulaminu aplikacji (par. 9) dowiadujemy się, że dostęp do danych mają następujące podmioty:

– Komenda Główna Policji,

– Wojewódzkie Komendy Policji,

– wojewodowie,

– Centralny Ośrodek Informatyki,

– Take Task SA,

– Centrum Systemów Informacyjnych Ochrony Zdrowia.

Zgodnie z par. 9 ust. 9 regulaminu dane obywateli przez te wszystkie podmioty mogą być przetwarzane tylko ze względu na ważny interes publiczny, tj. zaistniałą sytuacją kryzysową związaną z rozprzestrzenianiem się wirusa SARS-CoV-2. A konkretnie w celu wsparcia Służb w monitoringu realizacji kwarantanny osób, co do których istnieje podejrzenie, że mogą być roznosicielami choroby zakaźnej COVID-19. To dość jasno określony cel, niepozostawiający wiele miejsca na interpretację. Dodatkowo Ministerstwo Cyfryzacji zastrzega sobie prawo do retencji danych użytkowników aplikacji przez okres 6 lat, żeby zabezpieczyć interes prawny Skarbu Państwa związany z potencjalnymi roszczeniami użytkowników.

Czy to nas uspokaja? Nie do końca. O ile takie podmioty jak

Centralny Ośrodek Informatyki czy Take Task SA rzeczywiście będą związane wspomnianym wyżej celem epidemiologicznym, o tyle ze służbami specjalnymi (o których w ogóle nie ma mowy w regulaminie aplikacji) może być inaczej. W Polsce, gdy tylko wchodzi w grę bezpieczeństwo państwa, kończy się zasięg regulaminów, ustaw i rozporządzeń chroniących prawa obywateli. Służby specjalne (ABW, AW, CBA, SKW i SWW) nie są objęte żadnymi przepisami dotyczącymi ochrony danych osobowych. W praktyce oznacza to, że mogą pozyskiwać od innych organów państwa wszystkie informacje, jakie uznają za przydatne do realizacji swoich zadań.

Być może dmuchamy na zimne, ale staranność watchdoga każe nam to zastrzeżenie opisać. Jeśli okazałoby się, że dane o lokalizacji i zdjęcia przesyłane przez osoby odbywające kwarantannę domową są przechowywane dłużej przez którąkolwiek z uprawnionych instytucji, nie będzie można wykluczyć, że zostaną przechwycone przez służby do innych celów. Na przykład do trenowania algorytmów służących do rozpoznawania twarzy. Ten niepokój jest uzasadniony: trenowanie algorytmów twarzami użytkowników bez ich wiedzy i zgody ma długą i udokumentowaną historię – od Captchy przez FaceApp.

Czy aplikacja jest dobrowolna?

Od 1 kwietnia 2020 r. instalowanie aplikacji jest obowiązkowe dla osób odbywających kwarantannę domową. Podstawa prawna: art. 7e ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. poz. 374, z późn. zm.).

Dlaczego policja nadal odwiedza osoby korzystające z aplikacji?

Aplikacja jest przedstawiana jako narzędzie alternatywne do

policyjnych kontroli. Tak długo, jak długo raporty z aplikacji potwierdzają, że zasady kwarantanny nie zostały naruszone, policja nie powinna niepokoić jej użytkowników. Doświadczenia osób, do których udało nam się dotrzeć, tej zależności jednak nie potwierdzają. Mimo tego, że kilka razy dziennie wysyłają swoje zdjęcia i nie ruszają się z mieszkania, policja nadal ich odwiedza. Zdarzyło się też, że zadzwonił sanepid. Dlaczego? W naszej ocenie takie nakładające się środki nadzorcze są nieproporcjonalne.

Siostra, u której mieszkam, jest przedszkolanką i ona rzeczywiście przeżywa te codzienne odwiedziny policji. I jeszcze się boi, że jak się sąsiedzi zorientują, że ma lokatora w kwarantannie, to jej nawet do sklepu nie wpuszczą – obawia się Karolina, która odbywa kwarantannę w małej miejscowości pod Poznaniem. Zainstalowałam aplikację, bo byłam ciekawa, jak działa produkt zaproponowany przez Ministerstwo. Myślałam też, że odciążę policjantów z obowiązku przyjeżdżania do mnie. Już sprawdziłam, jak działa, policjanci mówią, że i tak muszą przyjeżdżać, to nie będę narażać prywatności i ryzykować, że ktoś je wykorzysta.

Wreszcie pojawia się wątpliwość: co z osobami, które nie mają smartfona albo których sprzęt nie spełnia wymogów technicznych (iOS w wersji min. 13.2, Android min. 6.0, usługi Google Play – niedostępne w smartfonach Huawei)? One muszą liczyć się z wizytami funkcjonariuszy.

Ministerstwo Cyfryzacji, skonfrontowane z tymi pytaniami, uspokaja, że potrzebna jest jeszcze chwila na to, by system zaczął w pełni działać. Rząd podtrzymuje, że jego celem jest odciążenie funkcjonariuszy, a jednocześnie zaoszczędzenie obywatelom, którzy wolą korzystać z aplikacji, policyjnych wizyt.

Komendy sukcesywnie otrzymują informacje o korzystających z aplikacji. Tym samym policja przestaje odwiedzać pierwszych Obywateli korzystających z aplikacji. Policjanci będą również

przekazywali Obywatelom informację o aplikacji. Szacujemy, że to kwestia kilku dni, by informacja skutecznie dotarła do wszystkich zainteresowanych.
Na marginesie: czy obywatele powinni mieć prawo samodzielnie weryfikować, jak działa aplikacja „Kwarantanna domowa”?

Naszym zdaniem tak – powinni mieć takie prawo. Koalicja European Digital Rights, do której należy Fundacja Panoptykon, wydała w ubiegłym tygodniu oświadczenie, w którym podkreśla, że kontrola społeczna wszystkich środków technicznych wykorzystywanych w walce z koronawirusem jest bardzo potrzebna. Na niej buduje się zaufanie do państwa: do tego, że naprawdę działa ono w naszym najlepszym interesie i niczego nie ukrywa.

W przypadku aplikacji taka społeczna kontrola jest możliwa pod warunkiem wykorzystania otwartego oprogramowania. Tymczasem wygląda na to, że „Kwarantanna domowa” jest przepisaną na szybko (co w tych okolicznościach jest zrozumiałe) aplikacją Taketask, w cywilu służącą do zarządzania sklepami (np. kontrolowania ekspozycji towaru). Czy możemy oczekiwać od firmy, że udostępni swój kod, na którym na co dzień zarabia, dla dobra publicznego? W tej sytuacji to oczekiwanie jest jak najbardziej zasadne.

Konstytucyjny test niezbędności. Czy dobrowolna aplikacja nie wystarczy do odciążenia policji?

Zgodnie z konstytucją państwo nie może zbierać innych informacji o obywatelach niż te, które są niezbędne do realizacji jego zadań. W każdym przypadku to państwo powinno ową niezbędność zbierania danych uzasadnić. Odnosząc tę zasadę do walki z epidemią: państwo nie może zmuszać obywateli do korzystania z nadzorczej technologii i przekazywania danych osobowych, o ile nie jest to niezbędne do osiągnięcia celu – w

tym przypadku doprowadzenia do tego, by jak najwięcej osób przestrzegało nałożonej na nie kwarantanny.

Czy rzeczywiście służby nie są w stanie zapewnić przestrzegania zasad kwarantanny w inny sposób niż poprzez zbieranie danych biometrycznych i danych o lokalizacji wszystkich obywateli objętych kwarantanną? Czy – w kontekście potrzeby odciążenia policji – nie wystarczy, by duża część (zapewne większość) osób objętych kwarantanną dobrowolnie zdecydowała się udostępnić swoje dane po to, by uniknąć codziennych kontaktów z funkcjonariuszami? Patrząc na dotychczasową praktykę, policja nie będzie w stanie sprawnie reagować na każdy przypadek błędnego lub brakującego raportu. Po narzuceniu aplikacji wszystkim osobom poddanym kwarantannie liczba raportowanych błędów z pewnością się zwiększy – i to nie dlatego, że ludzie masowo zaczną naruszać zasady kwarantanny, ale ze względu na problemy z jej obsłużeniem (por. kolejny punkt). Wreszcie: ważnym argumentem przemawiającym przeciwko nałożeniu obowiązku technologicznego nadzoru na wszystkie osoby objęte kwarantanną są podawane przez policję dane (+ kolejne źródło). Wynika z nich, że tylko niewielki procent Polaków narusza zasady kwarantanny.

Jeśli celem państwa jest nakłonienie ludzi do tego, żeby przestrzegali reguł społecznej izolacji (a nie zbieranie ich danych osobowych), oraz odciążenie służb, wydaje się, że da się to osiągnąć kombinacją już istniejących środków – takich jak kampania informacyjna, wsparcie dla osób objętych kwarantanną w ich życiowych potrzebach, przesiewowe kontrole, wysokie kary finansowe za naruszenie kwarantanny i dobrowolna aplikacja, która ułatwia odbywanie kwarantanny.

W uzasadnieniu ustawy nie znaleźliśmy wyjaśnienia, dlaczego zaostrzenie jednego z tych środków (tj. narzucenie obowiązku instalowania aplikacji wszystkim objętym kwarantanną) po kilku tygodniach doświadczeń okazało się konieczne. W obliczu epidemii należy działać szybko, ale też rozważnie. W tym kontekście ograniczenie ograniczanie prywatności setek tysięcy

obywateli – bo tym jest zmuszanie ich do regularnego przesyłania swoich zdjęć – uważamy za zwykłe pójście na skróty.

O ile sam pośpiech można zrozumieć w kontekście epidemii, o tyle ograniczanie prywatności setek tysięcy obywateli – bo tym jest zmuszanie ich do regularnego przesyłania swoich zdjęć – już nie.

Jest obowiązek, ale brakuje wsparcia dla obywateli o niskich kompetencjach cyfrowych

Aby aplikacja mogła poprawnie zadziałać obywatele i obywatelki podlegające kwarantannie muszą zadbać o aktualizowanie aplikacji, stały dostęp do sieci telekomunikacyjnej, a w końcu o to, żeby smartfon był stale pod ręką. Muszą też samodzielnie rozstrzygnąć (przecież środki dystansowania społecznego nadal obowiązują), czy ich urządzenie pozwala zainstalować aplikację, jak to zrobić, jak ustrzec się przed błędami, jak zadbać o regularne aktualizacje oprogramowania.

Wbrew temu, co założyć ustawodawca, odpowiedzi na te pytania nie zawsze są proste. Bo co to znaczy „urządzenie mobilne umożliwiające zainstalowanie oprogramowania”? Czy chodzi o teoretyczną możliwość (a więc każdy smartfon z systemem operacyjnym iOS w wersji min. 13.2 lub Android min. 6.0), czy realną możliwość instalacji na konkretnym urządzeniu, które może mieć np. zajętą pamięć? Jak ocenić sytuację kogoś, kto w ramach umowy z operatorem dostał nowy telefon (spełniający wymogi), ale nie zaczął go używać, bo jest przyzwyczajony do swojego starego modelu (niespełniającego wymogów)?

Ustawodawca najwyraźniej zakłada, że Polacy o niskich kompetencjach cyfrowych czy mieszkający poza obszarem miast – gdzie ze stabilnością sieci bywa różnie – poradzą sobie z

narzuconymi obowiązkami. Zakłada również, że osoba w kwarantannie (która sama przecież może mieć oznaki choroby takie jak wysoka gorączka) będzie pilnie śledzić powiadomienia z aplikacji i reagować na każde wezwanie do przesłania zdjęcia. Jest jednak możliwy scenariusz, w którym wiele osób nie sprosta postawionym wymaganiom, co spowoduje gwałtowny wzrost liczby błędnych raportów, na które będzie musiała reagować policja.

Nietrudno odgórnie nałożyć na obywateli obowiązek stosowania narzędzi technologicznych. Znacznie ciężej zadbać o to, by mieli możliwość go przestrzegać. Starsze osoby, będące w grupach podwyższonego ryzyka, które zostały objęte obowiązkową kwarantanną, i tak są narażone na ogromny stres. Ten stres pogłębi się wraz z nowym, być może zupełnie dla nich niezrozumiałym, obowiązkiem technologicznego samonadzoru. Będą musiały samodzielnie zdecydować, czy ich telefon umożliwia zainstalowanie i obsługę aplikacji. A jeśli dojdą do wniosku, że nie – czeka je oświadczenie pod rygorem odpowiedzialności karnej.

Zamknięty kod – brak przejrzystości, która jest filarem zaufania obywateli do państwa

W tych trudnych okolicznościach państwo potrzebuje wsparcia i współpracy ze strony obywateli. A taką gotowość po ich stronie najlepiej budować na zaufaniu, które wzrasta dzięki przejrzystości. Nie czekając na pytania, państwo powinno wykazać, że rzeczywiście działa w naszym najlepszym interesie i niczego przed nami nie ukrywa.

W przypadku aplikacji „Kwarantanna domowa” i innych technologicznych narzędzi warunkiem społecznej kontroli jest wykorzystanie otwartego oprogramowania. Otwarty kod umożliwia kontrolę nad systemem. Dzięki temu można na bieżąco, a nie

dopiero po latach stwierdzić, czy doszło do wycieku danych, jakie błędy są w aplikacji, które powodują trudności w używaniu. Można też, niskim kosztem, rozwijać aplikację po to, by lepiej zabezpieczyć jej użytkowników przed zagrożeniami związanymi z naruszeniem ich prawa do prywatności.

Tymczasem wygląda na to, że „Kwarantanna domowa" jest przepisaną na szybko aplikacją Taketask, na co dzień służącą do zarządzania sklepami (np. kontrolowania ekspozycji towaru). Jak wynika z analiz, które niezależni eksperci przeprowadzili bez dostępu do kodu źródłowego, aplikacja jest m.in. wyposażona w bibliotekę Facebooka, mimo że w praktyce nie komunikuje się z tym portalem.

Ze względu na mnożące się pytania oczekujemy, że państwo udostępni kod źródłowy aplikacji i w ten sposób oszczędzi niezależnym ekspertom dalszego zgadywania, czy jeszcze jakieś funkcje (w tym śledzące) są zaszyte w tym narzędziu.

Niebezpieczny precedens

Nałożenie obowiązku korzystania z aplikacji wprowadza również niebezpieczny precedens: uzależnia możliwość realizacji usług publicznych od wykorzystania konkretnego rozwiązania technologicznego. Uważamy, że w odniesieniu do osób fizycznych państwo powinno zaoferować analogowy ekwiwalent usługi publicznej. Po pierwsze, z przyczyn, które opisaliśmy powyżej, nie każdy jest w stanie korzystać z technologii. Po drugie, obywatele i obywatelki po prostu powinni mieć wybór, jak są gotowi kontaktować się z administracją (czy przy użyciu technologii, czy analogowo).

Art. 32 konstytucji przesądza, że państwo musi stać na straży gwarancji równego traktowania, również w zakresie dostępu do usług i nakładania obowiązków. W wypadku technologii cyfrowych brak równości wynika z przyczyn obiektywnych. Ludzie mają różne kompetencje, różne obiektywne możliwości (np. zasięg sieci) oraz różne nastawienie do korzystania z technologii w

kontakcie z władzą publiczną. Stąd w całej administracji nie istnieją – w przypadku osób fizycznych – procedury, które przewidują obowiązek stosowania wyłącznie narzędzi technologicznych.

Ogromne znaczenie ma fakt, że osobom, które nie zdecydują się na używanie aplikacji, może grozić odpowiedzialność karna. W związku z problemami z instalacją ktoś może błędnie uznać, że jego telefon nie spełnia wymagań sprzętowych, i złożyć oświadczenie o nieposiadaniu sprzętu kompatybilnego z aplikacją. Wobec takiej konstrukcji przepisów i ryzyka tego, że niektóre osoby mogą nie być w stanie wypełnić narzuconego im obowiązku, jest to sankcja zdecydowanie zbyt surowa, która potencjalnie godzi w prawa osób już wykluczonych.

Czego oczekujemy

1. Aplikacja powinna być dobrowolna. Wzywamy więc do usunięcia przepisu nakładającego obowiązek jej instalowania. Zamiast tego władze powinny wytłumaczyć, jakie korzyści – zarówno całemu społeczeństwu, jak i jednostce – daje dobrze zaprojektowana i wprowadzona aplikacja.

2. Aplikacja powinna zostać udostępniona z otwartym kodem. Pomoże to w ocenie jej bezpieczeństwa dla użytkowników i ustrzeże przed ukrywaniem problemów związanych z ochroną danych.

3. Władze powinny wzmocnić kampanię informacyjną dotyczącą zasad i warunków przebywania na kwarantannie oraz zapewnić objętym nią obywatelom i obywatelkom odpowiednie wsparcie (np. pomoc w zrobieniu zakupów i wyprowadzeniu psa, opiekę nad małoletnimi).

4. Aby zapewnić możliwie najwyższy poziom ochrony danych osobowych przetwarzanych w aplikacji ich administrator (Minister Cyfryzacji), a w szczególności wyznaczony przez niego Inspektor Ochrony Danych powinien ściśle współpracować z

Urzędem Ochrony Danych Osobowych, m.in. w zakresie przygotowania i prowadzenia obowiązkowej w tym wypadku analizy oceny skutków dla ochrony danych osobowych.

5. Władze powinny wzmocnić działania wspierające osoby, które dobrowolnie chcą zainstalować i używać aplikację. Dotychczasowa propozycja (pomoc w formie infolinii) może być niewystarczająca szczególnie dla osób, które mają w domu tylko jedno urządzenie mobilne, na którym będą miały jednocześnie instalować aplikację i odbywać rozmowę telefoniczną.

Autorstwo: Katarzyna Szymielewicz, Anna Obem, Fundacja Panoptykon i Fundacja ePaństwo
Źródło: Panoptykon.org [1] [2]
Kompilacja 2 artykułów: WolneMedia.net