

Technologia w walce z koronawirusem - 7 filarów zaufania

Technologia może pomóc nam w walce z pandemią koronawirusa, ale wdrażanie w trybie przyspieszonym nowych rozwiązań technologicznych nie może stać się furtką do naruszeń praw i wolności obywateli. Monitorowanie społecznych kontaktów przy pomocy narzędzi technologicznych zadziała tylko przy dużym poparciu i dobrowolnej współpracy ze strony ludzi. Taka postawa wymaga wysokiego poziomu zaufania obywateli do narzędzia, które zostanie im zaproponowane przez państwo.

Wychodząc naprzeciw potrzebie chwili, przypominamy najważniejsze zasady projektowania narzędzi w sposób zgodny z RODO i budzący społeczne zaufanie:

1. Minimalizacja i poprawność danych

W celu przeciwdziałania pandemii można przetwarzać tylko te dane, które są **niezbędne** do realizacji celu założonego w ramach konkretnego narzędzia (np. jeśli celem jest zarejestrowanie społecznej interakcji, która stwarza ryzyko zarażenia, wystarczy zapisanie pary urządzeń, które się „spotkały”, bez ich rzeczywistej lokalizacji). Co więcej, dostęp do danych powinny mieć tylko osoby i instytucje, które ten cel realizują (np. nie ma potrzeby, by obywatel korzystający z aplikacji do śledzenia społecznych kontaktów wiedział, kto naraził go na zakażenie; taką informację powinny otrzymać tylko służby sanitarne).

Wykorzystywane powinny być tylko możliwie najbardziej prawidłowe dane o ludziach. Jest to szczególnie ważne w rozwiązaniach sprawdzających prawdopodobieństwo zarażenia na podstawie danych o lokalizacji: przetwarzanie niepotwierdzonych danych potęgowałoby chaos, bo użytkownicy otrzymywaliby fałszywe powiadomienia o możliwym zarażeniu.

2 Ograniczenie czasu przechowywania danych

Dane osobowe nie powinny być przechowywane dłużej, niż jest to konieczne do zrealizowania konkretnego celu, jakiemu mają służyć. Na przykład zapis kontaktów społecznych przemieszczającej się osoby jest potrzebny tylko przez okres, w jakim standardowo pojawiają się objawy zakażenia (do 14 dni), a dane biometryczne osoby objętej kwarantanną, przesłane w raporcie z aplikacji, tylko do momentu zweryfikowania, że raport był poprawny. W ustalaniu maksymalnych terminów powinni brać udział lekarze, epidemiolodzy i eksperci techniczni.

3 Dane przechowywane na urządzeniu obywatela

Narzędzia służące do zwalczania koronawirusa nie powinny prowadzić do tworzenia nowych baz danych, przechowywanych na serwerach administracji publicznej. Zasadą powinno być gromadzenie i przetwarzanie danych osobowych na urządzeniu osoby, której te dane dotyczą. Przekazanie danych na zewnętrzny serwer (np. zarządzany przez służby sanitarne) powinno następować tylko w ściśle określonych i uzasadnionych przypadkach (np. stwierdzonego incydentu zarażenia), a obywatel powinien być o tej konieczności uprzednio poinformowany.

4 Bezpieczeństwo, szyfrowanie i anonimizacja danych

Dane osobowe powinny być szyfrowane, anonimizowane (tam, gdzie to niemożliwe - pseudonimizowane), a korzystające z nich aplikacje powinny zachowywać najwyższe standardy bezpieczeństwa i być poddawane odpowiednim audytom. W ramach walki z epidemią grozi nam przetwarzanie danych milionów obywateli przez systemy, które powstają pod presją czasu. To sytuacja podwyższonego ryzyka również w kwestii cyberbezpieczeństwa: jakikolwiek wyciek będzie miał katastrofalne skutki dla społecznego zaufania do technologii wdrażanych przez państwo.

5 Czytelna informacja dla obywateli

Podstawą społecznego zaufania do narzędzi technologicznych służących walce z pandemią jest czytelna i zrozumiała informacja dla osób, których dane będą wykorzystywane. Obywatele powinni rozumieć zasady działania proponowanych im narzędzi, zakres zbieranych o nich danych oraz to, kto i w jaki sposób z tych danych skorzysta.

6. Otwartość kodu i przejrzystość algorytmów

Standardem dla narzędzi służących do walki z pandemią powinna być pełna otwartość kodu oraz algorytmów stosowanych do analizy danych (np. parametry brane pod uwagę przy określaniu ryzyka zakażenia w kontakcie społecznym muszą być jawne). Tylko taki standard umożliwi publiczną kontrolę nad narzędziami technologicznymi, a zarazem przełoży się na ich bezpieczeństwo. Otwartość kodu daje bowiem możliwość szybszego zidentyfikowania błędów i możliwych zagrożeń dla prywatności, co dodatkowo wzmacnia zaufanie do danej aplikacji.

7 Publiczna kontrola nad narzędziami

Każde narzędzie, z którego państwo zamierza skorzystać w walce z pandemią, powinno zostać wcześniej zweryfikowane pod kątem cyberbezpieczeństwa i standardów ochrony danych osobowych. W przypadku rozwiązań, których kod jest niedostępny do publicznej analizy, to państwo musi wykazać, że standardy bezpieczeństwa danych i ochrony prywatności są spełnione. W sytuacji, gdy takie rozwiązanie ma być wykorzystywane do zbierania danych osobowych obywateli, organ administracji musi mieć też pełną kontrolę nad systemem.