Wolność, prywatność i nadzór po COVID-19

20 stycznia 2023

Od Rosji po Stany Zjednoczone, przez Polskę, Filipiny i RPA – jak świat długi i szeroki pandemia koronawirusa okazała się doskonałą pożywką dla zwiększonego nadzoru nad społeczeństwem. Prawne i technologiczne rozwiązania wykorzystywano do tego, by zbierać dane o zdrowiu ludzi, monitorować osoby poddane kwarantannie, ale też uciszać protestujących. To główne wnioski z raportu o (nad)używaniu technologii w czasie COVID-19, przygotowanego przez European Center for Not-for-Profit Law, International Network of Civil Liberties Organizations i Privacy International.

Rządy monitorujące

Próbując ograniczyć zasięg pandemii, rządy wprowadziły rozwiązania prawne i technologiczne, które pozwalały śledzić rozprzestrzenianie się wirusa. Powstały ogromne bazy z danymi wrażliwymi (wyniki testów na COVID). Te rozwiązania wprowadzano w pośpiechu, bez konsultacji publicznych, bez podstawy prawnej (Francja) albo z wadliwą podstawą prawną (Polska). Pośpiech, w jakim je tworzono, brak informacji i szeroki dostęp do baz, brak możliwości składania skarg zwiększyły natomiast obawy o inwigilację i manipulację. A także o to, że dane zostaną wykorzystane do celów komercyjnych. W krajach, w których prawa człowieka nie są przestrzegane, zebrane dane mogą też zostać wykorzystane przeciwko środowiskom opozycyjnym i aktywistycznym.

W Polsce nie ma realnej kontroli nad działaniami służb, które przecież mają dostęp także do baz danych o osobach poddanych kwarantannie. Jak wykorzystywały te informacje? I jak wykorzystają je w przyszłości? Nikt tego nie wie.

Wiemy natomiast, jak silną negatywną reakcję wzbudziła obowiązkowa aplikacja Kwarantanna domowa (osoby na kwarantannie o różnych porach dnia miały przesyłać selfie opatrzone danymi o lokalizacji, tak by można było sprawdzić, czy przestrzegają zakazu wychodzenia z domu). Część krytyki wprawdzie dotyczyła tego, że aplikacja się zawiesza, a żądania selfie nieraz wyrywają ze snu ciężko chorych ludzi, ale inwigilacyjny aspekt tego narzędzia również był szeroko komentowany. Za niedociągnięcia Kwarantanny domowej „zapłaciła" kolejna aplikacja, już dobrowolna, ProteGO Safe, która – mimo sporych nakładów na promocję – nie przyjęła się.

Koronawirus jak terroryzm

W raporcie zebrane zostały też przykłady tego, jak do ograniczenia transmisji wirusa rządy niektórych państw wykorzystały narzędzia, którymi dysponują policja i służby specjalne. W ruch poszły więc m.in. mechanizm śledzenia urządzeń mobilnych (Izrael), geolokalizacja (Pakistan) czy drony (Francja).

Władze na całym świecie skorzystały z pandemii jako z dogodnej wymówki, żeby uciszać krytyków – także w Polsce, gdzie pod pretekstem pandemii zakazywano protestów ulicznych po wydanym w październiku 2020 r. wyroku ograniczającym możliwość aborcji praktycznie do zera.

Autorzy raportu przytaczają opinię Fionnuali Ní Aolái, specjalnej sprawozdawczyni ONZ ds. promocji oraz ochrony praw człowieka podczas zwalczania terroryzmu: „Mechanizmy antyterrorystyczne są notorycznie wykorzystywane do łamania prawa człowieka, m.in. poprzez niezgodne z prawem targetowanie środowisk aktywistycznych czy mniejszości. Są wykorzystywane w sposób nieprzejrzysty i poza realną kontrolą. Te same obawy pojawiają się, kiedy przepisy i technologie antyterrorystyczne są wykorzystywane do nowych celów".

Korporacje na pomoc państwu

W czasie pandemii rządy na całym świecie współpracowały z prywatnymi podmiotami z branży cyfrowej. Firmy IT przygotowywały aplikacje mobilne, a Google i Apple współpracowały nad udostępnieniem protokołu do śledzenia kontaktów między ludźmi (dlatego Niemcy i Wielka Brytania zrezygnowały z rozwijania własnych aplikacji, mimo że dałyby im one większą kontrolę nad przetwarzaniem danych).

Czy to jeszcze współpraca, czy już zdanie się na łaskę korporacji? Aktywiści z RPA uważali na przykład, że przekazywanie oficjalnych wiadomości na temat koronawirusa za pomocą należącego do firmy Meta komunikatora WhatsApp to już przekroczenie tej granicy. Inni aktywiści doprowadzili do ujawnienia umów dotyczących przekazywania danych między rządami Kolumbii i Wielkiej Brytanii a prywatnymi podmiotami (np. brytyjski start-up Faculty, współpracujący z amerykańskim Palantirem, pomagał rządowi Wielkiej Brytanii łączyć bazy danych o chorych i na tej podstawie przygotowywać zalecenia do walki z pandemią).

Ilu podobnych przypadków nie znamy i jakie jeszcze skandale się pod nimi kryją?

Koniec pandemii – nadzór zostaje

Chociaż nasze głowy zajęte są już kolejnymi kryzysami – od wojny po galopującą inflację – to pandemia zostawiła po sobie trwały inwigilacyjny spadek. Bazy danych o zdrowiu, które powstały podczas pandemii, zostaną wykorzystane do nowych celów (np. w Kolumbii, Indiach i RPA powstaną narodowe platformy ochrony zdrowia).

Rolę big techów w reagowaniu na kryzysy publiczne ujawnili – chyba niechcący – premierzy państw z grupy wyszehradzkiej, którzy po inwazji Rosji na Ukrainę w lutym 2022 r. zwrócili

się do cyfrowych korporacji po pomoc.

Polska pojawia się w raporcie tylko dwa razy: w kontekście śledzących aplikacji mobilnych i uciszania protestów ulicznych. Czy to znaczy, że jest aż tak dobrze, czy tylko nie wiemy, jak bardzo jest źle?

Autorstwo: Anna Obem
Współpraca: Rozalia Bielińska
Źródło: Panoptykon.org

Źródłografia

1. https://ecnl.org/sites/default/files/2022-12/Executive%20Summary%20Under%20Surveillance%20-%20%28Mis%29use%20of%20Technologies%20in%20Emergency%20Responses.pdf

2. https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response