Analiza KBN

COVID-19

Seria C Nr 10 (72) / 2020 3 sierpnia 2020 r.

Niniejsza analiza powstała w wyniku realizacji projektu *Bezpieczeństwo narodowe Polski w obliczu pandemii koronawirusa: implikacje wewnętrzne i międzynarodowe* finansowanego ze środków konkursu SocietyNow!#1 w ramach programu Inicjatywa Doskonałości w Uniwersytecie Jagiellońskim.

Paweł Frankowski

Nadzór i elektroniczne instrumenty zarządzania/rządzenia w sytuacjach kryzysowych i postkryzysowych

Wraz z tym, jak elektroniczne środki nadzoru zaczęły dominować w relacjach między producentem i pracownikiem oraz producentem i konsumentem, pojawiła się silna obawa co do tego, czy istniejące struktury regulacyjne i zasady dotyczące ochrony praw człowieka zapewniają odpowiednią ochronę jednostek. Nieskończenie wielka liczba danych pozwala nie tylko na dopasowanie produktu do obecnych potrzeb konsumenta, ale także skuteczne prognozowanie przyszłego zachowania. Chociaż wykorzystanie tych danych na potrzeby marketingu, w tym marketingu politycznego, jest faktem, to warto zastanowić się, jakie efekty na społeczeństwo, w skali globalnej i regionalnej, wywiera wprowadzenie elektronicznych środków nadzoru jako proponowanego instrumentu szybkiej reakcji na globalny kryzys związany z rozwojem epidemii COVID-19.

Środki nadzoru elektronicznego w czasie pandemii

Chociaż doniesienia na temat możliwości zastosowania elektronicznych środków nadzoru, takich jak aplikacje wymuszające przebywanie w miejscu kwarantanny bądź też śledzące potencjalnych zainfekowanych, dotyczą wielu państw, to podjęte środki różnią się pod wieloma względami. W części przypadków rządy wprowadzają aplikacje wspierające tzw. *social distancing*, dzięki czemu można kształtować świadomość obywateli w zakresie wzrostu możliwości transmisji zakażenia. Drugie podejście promuje śledzenie kontaktów (*contact tracing*), co pozwala na precyzyjne określenie sieci potencjalnych powiązań osób zakażonych oraz dróg transmisji wirusa. Jednocześnie podejście to stwarza zagrożenie powstania potężnego narzędzia inwigilacji i nadzoru, gdzie w imię bezpieczeństwa i zdrowia publicznego możliwe stanie się przechowywanie danych dotyczących dokładnej lokalizacji i wykorzystanie ich nie tylko do działań na rzecz ochrony zdrowia, ale także na potrzeby bliżej niesprecyzowanego bezpieczeństwa. Pozwala to na przyjęcie ustaw nadzwyczajnych, w których prawo do prywatności jest skonfrontowane z potrzebą skutecznego działania rządu przy wykorzystaniu nowoczesnych technologii. Powoływanie się na „nadzwyczajne okoliczności" w celu uzasadnienia wzmożonej inwigilacji i nadzoru rodzi głębokie obawy co do intencji podmiotów publicznych promujących elektroniczne instrumenty nadzoru, jak i podmiotów prywatnych dostrzegających istotną niszę rynkową.

Zastosowanie aplikacji śledzących wymaga bowiem posiadania sprzętu, który jest w stanie sprostać wymaganiom programu, jak również narzuca konieczność częstszego ładowania telefonu w przypadku wykorzystywania technologii Bluetooth, dzięki której implementowane są rozwiązania pozwalające na określenie, jak blisko użytkownik aplikacji znajdował się od potencjalnego nosiciela. Jedną z charakterystycznych cech reakcji na zjawisko pandemii COVID-19 jest zwiększona świadomość tego, w jakim stopniu zachowanie jednostki może mieć wpływ na innych. Wiążą się z tym przyjęte zalecenia i nakazy zachowania odpowiedniej odległości w środkach transportu publicznego, ale także obowiązek dezynfekcji i inne działania na rzecz utrzymania wyższego standardu higieny. Aby jednak zmienić i warunkować zachowania obywateli oraz monitorować potencjalne zagrożenia, rządy na całym świecie przyjmują szereg „nadzwyczajnych" środków w ramach istniejących ram prawnych, ale powodowane potrzebą chwili podejmują też działania sytuujące się poza przyjętymi normami prawnymi.

Śledzenie kontaktów za pośrednictwem smartfonów, jako najpopularniejszego narzędzia kontaktu, jest jednym z przykładów zastosowania technologii nadzoru w celu zmiany lub warunkowania zachowania. Obowiązek używania aplikacji śledzących, często zaadaptowanych

z istniejących już rozwiązań programistycznych, pokazuje, jak wiele problemów pojawia się na styku technologii nadzoru, bezpieczeństwa, zarządzania kryzysowego i praw człowieka.

Problematyczny charakter elektronicznych środków nadzoru

Problemy, jakie mogą się pojawić wraz z zastosowaniem technologii nadzoru elektronicznego w próbach opanowania epidemii COVID-19, można sprowadzić do trzech grup wyzwań.

Pierwszą grupę będą stanowić sekurytyzacja pandemii i utrwalenie środków nadzoru elektronicznego jako normalnych i akceptowalnych instrumentów kontroli, monitorowania oraz wymuszania zgodności. Zazwyczaj środki nadzoru elektronicznego są przedstawiane jako tymczasowe, jednak przykład reakcji rządów na zamachy terrorystyczne z pierwszej dekady XXI wieku pokazuje, że niektóre odpowiedzi rządów na poprzednie kryzysy zostały znormalizowane i utrwalone. Taka sama obawa pojawia się przy okazji reakcji rządów na pandemię COVID-19. Przyjmując, że elektroniczne środki nadzoru staną się trwałym elementem działania rządów, także w Polsce, należy zwrócić szczególną uwagę na podmioty prywatne świadczące usługi na rzecz podmiotów publicznych w tym zakresie, jak i lobbujące za określonymi rozwiązaniami prawnymi. W raporcie ONZ *Nadzór i prawa człowieka*[1] wskazano, że przy opracowywaniu i stosowaniu narzędzi nadzoru elektronicznego sektory publiczny i prywatny są „bliskimi współpracownikami". Wynika to z faktu, że rząd i agencje rządowe nie dysponują wystarczającymi środkami i zasobami ludzkimi, by wdrożyć instrumenty pozwalające na szybkie reagowanie i stworzenie stosownej aplikacji w momencie zagrożenia kryzysowego. Stawia to jednak pod znakiem zapytania efektywność i przygotowanie zespołów zarządzania kryzysowego, które nie były w stanie przewidzieć konieczności rozwoju niezbędnego oprogramowania, nawet w fazie testowej. Tym samym bliska współpraca podmiotów prywatnych i publicznych w momencie zagrożenia kryzysowego rodzi pytania o transparentność wydatkowania środków publicznych, jak i przyjęty model rozwoju aplikacji nadzoru elektronicznego.

Współczesny przemysł, zwłaszcza działający w obszarze usług na rzecz bezpieczeństwa, jest nierozłącznie związany z polityką, gdyż z tej strony pojawia się zapotrzebowanie na usługi świadczone przez ów sektor. Jednocześnie warto zauważyć, że aktywność Unii Europejskiej w zakresie kreowania polityk przemysłowych dotyczy także sektora bezpieczeństwa, a projekty badawcze takie jak iBorderCtrl, zmierzające do stworzenia systemu rozpoznawania twarzy, ukierunkowane są na problemy, z którymi boryka się UE, czyli na przykład nielegalna migracja.

[1] UN Human Rights Council, *Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/41/35, 28.05.2019, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement.

Rozwój pandemii COVID-19 oraz elektronicznych środków nadzoru pozwoli na przeniesienie przyjętych nadzwyczajnych rozwiązań na obszary, gdzie wcześniej działania takie nie były podejmowane lub też prowadzono badania nad możliwością wykorzystania instrumentów nadzoru elektronicznego. Należy zaznaczyć, że na poziomie UE brak jest ustandaryzowanych procedur regulujących nadzór elektroniczny, co pośrednio wynika z braku woli państw członkowskich. To również problem nadzoru ze strony instytucji takich jak parlamenty i podmioty procesów politycznych gwarantujące bezstronność w wykorzystaniu danych gromadzonych podczas funkcjonowania aplikacji nadzoru elektronicznego. Powstaje zatem konieczność powołania instytucji, która w sposób bezstronny i możliwie odpolityczniony sprawowałaby nadzór nad całością procesu funkcjonowania instrumentów nadzoru elektronicznego wykorzystywanych w zwalczaniu i zapobiegania epidemiom.

Druga grupa problemów dotyczy sposobów uzasadniania i akceptacji środków nadzoru w społeczeństwach, gdzie należy podkreślić nierówny dostęp obywateli do technologii pozwalających zarówno na warunkowanie zachowania (dystansowanie społeczne), jak i wymuszanie przestrzegania zaleceń. W czasie kryzysu pojawia się konieczność zaproponowania rozwiązań, które nie tylko szybko przyniosą rezultaty, ale także sprawią wrażenie skutecznych i efektywnych działań. Jednocześnie w pośpiesznym i często nieskoordynowanym postępowaniu umyka problem przestrzegania praw człowieka, na co wskazują raporty instytucji międzynarodowych przyjęte na kilka lat przed rozwojem epidemii COVID-19. Raport Komisji Zagadnień Prawnych i Praw Człowieka Zgromadzenia Parlamentarnego Rady Europy odnotowuje, że praktyki nadzoru elektronicznego zagrażają prawom człowieka, takim jak prawo do prywatności (art. 8 Europejskiej konwencji praw człowieka (ETS nr 5)), wolności informacji i wypowiedzi (art. 10) oraz prawom do rzetelnego procesu sądowego (art. 6) i wolność wyznania (art. 9). Komisja uznała również, iż wyżej wymienione prawa są nieodzowną podstawą funkcjonowania demokracji, a ich naruszenie bez odpowiedniej kontroli sądowej zagraża praworządności. Tym samym wszelkie działania uzasadnione wolą zwalczania lub kontroli pandemii przy wykorzystaniu elektronicznych środków nadzoru są potencjalnie naruszeniem podstawowych zasad społeczeństw demokratycznych. Wskazany powyżej pośpiech we wprowadzaniu rozwiązań *ad hoc* może prowadzić do wielu niedociągnięć w standardach bezpieczeństwa, które mogą być łatwo wykorzystane także przez terrorystów, cyberterrorystów, a przede wszystkim przestępców posługujących się nowoczesnymi technologiami. Wdrażane rozwiązania, takie jak systemy rozpoznawania twarzy, systemy dokładnej lokalizacji czy systemy określające potencjalne drogi kontaktu osób zarażonych, ograniczają możliwości wolności i wypowiedzi, ponieważ społeczeństwa są nieustannie poddane nadzorowi, a potencjalnie

nieszkodliwe zachowania mogą być zinterpretowane jako zagrożenie dla bezpieczeństwa. Przykład systemów rozpoznawania twarzy pokazuje, że odsetek fałszywie pozytywnych lub fałszywie negatywnych rekordów oscyluje na poziomie 0,1 procenta, co pozornie wydaje się akceptowalnym marginesem błędu. Gdy jednak przyjąć, że systemy te zainstalowane są w miejscach o dużym natężeniu ruchu, jak place miast lub lotniska, skala błędnych rozpoznań jest potencjalnie wysoka. Dla przykładu, miasto Kraków w 2019 roku odwiedziło 14 milionów turystów, co daje przeciętnie 38 tysięcy osób dziennie (przy uproszczeniu, że natężenie ruchu turystycznego rozkłada się równomiernie w ciągu roku). Przyjmując, iż większość odwiedzających pojawi się na krakowskim Rynku, 38 osób dziennie może być wskazanych przez system jako potencjalne zagrożenie dla bezpieczeństwa. Zakładając, że ruch turystyczny zajmuje tylko 12 godzin, w ciągu godziny trzy błędnie zidentyfikowane osoby będą celem zainteresowania systemów nadzoru i kontroli. Podobnie problematyczne jest zastosowanie aplikacji pozwalających na określenie, jak blisko znajdujemy się od osoby potencjalnie zakażonej COVID-19. Systemy lokalizacji oparte na wymianie pakietów danych między telefonami nie rozróżniają sytuacji, gdy dwie osoby są oddzielone ścianą lub gdy jedna z nich znajduje się na przykład w tramwaju, a druga na przystanku. Uzasadnienie dla zastosowania i skuteczności wyżej wymienionej aplikacji staje się dyskusyjne.

Trzecia grupa problemów dotyczy niesprecyzowanych konsekwencji przeniesienia instrumentów nadzoru elektronicznego na środki mobilności, a w konsekwencji kontrolowania przemieszczania się osób zarówno w obrębie państwa, jak i przekraczających granice. Wpływ technologii nadzoru na struktury społeczne w dużej skali, przy jednoczesnym prognozowaniu możliwego wystąpienia zachowań potencjalnie karalnych, analizować można, opierając się na modelu Christophera Pollitta, który wskazał na trzy typy mobilności charakteryzujące współczesne społeczeństwa. W pierwszym typie, jakim jest *mobilność lokalizacyjna*, czyli fizyczne przemieszczanie się w określonej przestrzeni, środki nadzoru pozwalają nie tylko na określenie lokalizacji, ale również związanie miejsca z danymi wymienianymi przez kanały łączności, takie jak rozmowa telefoniczna czy Internet. Połączenie informacji odnośnie do miejsca, charakteru danych, płatności dokonywanych kartą płatniczą, danych pasażera (w przypadku pobrania danych od przewoźników lotniczych czy kolejowych) umożliwia generowanie alertów dla wyznaczonych służb odpowiedzialnych za bezpieczeństwo pandemiczne. Pojawiają się jednak wątpliwość co do tego, kto jeszcze ma dostęp do tych danych, jak długo będą one przechowywane i jaki będzie okres retencji danych uzasadniany bliżej nieokreślonym interesem publicznym, kto i na jakich zasadach może mieć do nich wgląd i czy na przykład jednostki badawcze mogą wykorzystywać gromadzone dane do celów naukowych. Drugi typ mobilności czyli *mobilność operacyjna*, jest

ściśle powiązany z wykorzystaniem aplikacji śledzących osoby potencjalnie. Wiąże się to z trzecim typem mobilności wskazanej przez Pollitta, czyli *mobilnością interakcyjną*, pozwalającą na utrzymanie stałych interakcji między ludźmi i źródłami danych. Mając na względzie fakt, że elektroniczne instrumenty nadzoru pozwalają na precyzyjne kontrolowanie dostępu do *przestrzeni*, w której znajduje się podmiot poddany nadzorowi (lub w której nie może lub nie powinien się znajdować albo znajduje się warunkowo), i *czasu* niezbędnego do osiągnięcia *miejsca*, pandemia staje się znakomitym źródłem uzasadnień dla działań zmierzających do pełniejszej kontroli nad *przestrzenią* i *czasem*. Jest to jedno z podstawowych źródeł władzy politycznej; powinno być zatem poddane nadzorowi publicznemu. Wiąże się to tym samym z realizacją następujących postulatów: (1) stworzenie przejrzystych regulacji określających możliwości zastosowania elektronicznych środków nadzoru; (2) zmiana uprawnień Urzędu Ochrony Danych Osobowych zmierzająca do odpolitycznienia poprzez między innymi wydłużenie kadencji prezesa do sześciu lat; (3) poszerzenie struktury wyżej wymienionego urzędu o radę, w której skład wchodziłyby osoby reprezentujące podmioty prywatne, ośrodki badawcze, organizacje pozarządowe oraz przedstawicieli Parlamentu; (4) podjęcie działań na rzecz stworzenia paneuropejskiego systemu regulacji nadzoru elektronicznego z uwagi na funkcjonowanie wspólnego rynku.

Przyszłość systemów nadzoru elektronicznego w czasie pandemii

Większość państw Unii Europejskiej rozwinęła środki elektronicznego śledzenia osób zakażonych lub mogących mieć styczność z takimi osobami. Ponieważ instrumenty te powstały w stosunkowo krótkim czasie, jak również bez koordynacji na poziomie UE, doszło do sytuacji, w której systemy te nie tylko nie są kompatybilne i niemożliwe jest przekazywanie informacji w wymiarze transgranicznym, ale także różne są procedury retencji danych. Jednocześnie dostawcy aplikacji korzystają z różnych sposobów geolokacji, co pozwala na odtworzenie sieci kontaktów między osobami potencjalnie zakażonymi. Pojawia się zatem wątpliwość co do zgodności tych instrumentów z regulacjami unijnymi. Odpowiedzią na to jest podjęta 16 czerwca 2020 roku decyzja państw członkowskich o przygotowaniu rozwiązań zapewniających interoperacyjność mobilnych aplikacji, tak by stworzyć skoordynowane podejście pozwalające na znoszenie ograniczeń zarówno w granicach wewnętrznych, jak i zewnętrznych Unii. Ponieważ nadal nie powstała wspólna aplikacja lub platforma łącząca systemy stworzone w państwach UE, trudno prognozować, jaka będzie przyszłość proponowanego rozwiązania.

Należy przyjąć, że systemy nadzoru elektronicznego osób zakażonych lub mających potencjalnie styczność z takimi osobami będą rozwijane i stopniowo staną się jednym z akceptowalnych narzędzi nadzoru, tak jak było z systemami monitoringu wizyjnego. Warto też podkreślić, że pandemia COVID-19 jest pierwszym tego typu wydarzeniem w historii, gdy możliwe stało się zastosowanie instrumentów nadzoru na tak szeroką skalę. Gdyby podobne wydarzenie nastąpiło 10 lat temu, brak byłoby jakiejkolwiek możliwości uruchomienia aplikacji śledzących, gdyż liczba użytkowników smartfonów była wówczas relatywnie niewielka. W kontekście rosnącej akceptacji dla wykorzystania smartfonów i aplikacji mobilnych przez użytkowników tychże urządzeń można postawić tezę, że zastosowanie wyżej wymienionych środków nadzoru stanie się koniecznością.