PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BIULETYN

Nr 114 (2046), 29 maja 2020 © PISM

Inwigilacja w ChRL w trakcie epidemii COVID-19

Marcin Przychodniak

Inwigilacja społeczeństwa to jedno z głównych narzędzi władzy w ChRL. Epidemia COVID-19 dała rządzącym pretekst do nasilenia nadzoru, m.in. przez wykorzystanie na terytorium kraju rozwiązań używanych głównie wobec Ujgurów w Sinciangu. Efektywność inwigilacji jest dla chińskich władz istotna ze względu na możliwe niepokoje wywołane problemami gospodarczymi po epidemii. Znaczenie inwigilacji w walce z wirusem w ChRL spowodowało, że także w demokracjach pojawiają się postulaty wprowadzenia podobnych praktyk.

Praktyka inwigilacji w ChRL. Inwigilacja społeczeństwa jest ważnym narzędziem utrzymania monopolu władzy Komunistycznej Partii Chin (KPCh). Rządzący przedstawiają ją jako gwarancję stabilności i rozwoju ChRL. Dotyczy ona szczególnie osób i grup, które publicznie nie zgadzają się z polityką władz. Są to dysydenci (w 2019 r. ze względu na zbyt późne podjęcie leczenia zmarł uwięziony laureat Nagrody Nobla Liu Xiaobo), organizacje pozarządowe występujące przeciw dyskryminacji (np. Ujgurów, katolików, osób LGBT czy kobiet), a także reprezentujący ich niezależni prawnicy. Inwigilacja i wynikające z niej represje nie omijają także członków partii (nawet na najwyższych szczeblach). Stały się m.in. elementem walki Xi Jinpinga z konkurencją polityczną.

Poligonem doświadczalnym jest od 2017 r. specjalny region autonomiczny Sinciang, gdzie zastosowano inwigilację wielosystemową (m.in. kontrolę internetu, monitoring połączony z profilowaniem, lokalizację pobytu, gromadzenie baz DNA, budowę systemów *big data*) do rozpoznawania Ujgurów. Są oni oskarżani przez władze o działalność terrorystyczną i umieszczani w specjalnych obozach. Niektóre z rozwiązań identyfikujących uczestników protestów (np. logowania telefonów komórkowych) zastosowano w Hongkongu w 2019 r.

Organem nadzorującym proces inwigilacji jest komitet ds. politycznych i prawnych w KC KPCh. Sekretarzem generalnym komitetu jest obecnie Chen Yixin – do końca kwietnia br. specjalny wysłannik Xi ds. zarządzania kryzysowego w Wuhanie w związku z epidemią.

Zmiany podczas COVID-19. Epidemia COVID-19 posłużyła władzom ChRL jako pretekst do nasilenia inwigilacji, w tym zbierania danych wrażliwych (jak odciski palców, historie chorób, informacje o podróżach, próbki DNA) od większej liczby obywateli. Władze postrzegały epidemię jako zagrożenie polityczne związane z niewydolnością systemu ochrony zdrowia w Wuhanie i Hubei. Rosnąca liczba chorych i zgonów powodowała niezadowolenie społeczeństwa, wyrażane m.in. w mediach społecznościowych. Dlatego władze uznały, że konieczne było zwiększenie kontroli nad przepływem informacji i reakcjami społeczeństwa, nad czym m.in. miał czuwać Chen Yixin.

Epidemia COVID-19 stanowiła także pretekst, aby w kraju (przede wszystkim w Hubei) przetestować nowoczesne rozwiązania stosowane wobec Ujgurów. Oznaczało to m.in. instalację tysięcy nowych kamer (jest ich już w ChRL ok. 200 mln), wraz z oprogramowaniem do rozpoznawania twarzy czy profilowania. W bieżącym roku ma powstać zintegrowana ogólnokrajowa sieć monitoringu dla aparatu bezpieczeństwa, wykorzystująca m.in. systemy *big data*. Chińskie firmy (np. CloudWalk, SenseTime) rozwijają technologie

sztucznej inteligencji (AI) pozwalające zdalnie na badanie temperatury ciała czy nawet profilowanie rasowe. AI ma też zastosowanie w testowanych obecnie systemach wiarygodności społecznej (mających m.in. nawiązywać do już istniejących mechanizmów, które „nagradzają" obywateli punktami za zachowanie zgodne z przepisami), które w dłuższej perspektywie mają objąć cały kraj, dając władzy możliwość kształtowania korzystnych dla niej zachowań społecznych.

Wskutek epidemii COVID-19 rozwinęły się także aplikacje komórkowe (tworzone na zlecenie władz prowincji czy miast), obowiązkowe dla obywateli chcących np. podróżować czy korzystać z miejsc użyteczności publicznej. Często nie było to możliwe bez skanowania kodów QR. W przeciwieństwie do niedokładnych czasem danych z triangulacji komórkowej, precyzyjną lokalizację GPS obywateli władze uzyskują z powszechnych aplikacji jak Alipay czy WeChat. Najpopularniejszą z nich jest wprowadzona w Hangzhou (a potem rozszerzona na całe Chiny jako obowiązkowa) Alipay Global Health (ok. 700 mln użytkowników), która porządkuje subskrybentów na podstawie lokalizacji i informacji o przebytych chorobach i m.in. przekazuje dane do serwerów policyjnych.

COVID-19 ułatwił dostęp władz chińskich do informacji przesyłanych przez użytkowników. Wcześniej właściciele aplikacji (np. Tencent czy Alibaba) niechętnie udostępniali dane ze względu na obawy konsumentów i opinię inwestorów (są one m.in. notowane na giełdzie w Nowym Jorku). Działalność firm pozostaje jednak zależna od decyzji partyjnych, co zmusza je do podporządkowania się decyzjom władz, zwłaszcza w sprawach, które rządzący uznają za polityczne. Dzięki temu możliwa jest m.in. inwigilacja i ograniczanie działalności niezależnych dziennikarzy, blogerów czy lekarzy, którzy od grudnia 2019 r. dokumentowali przebieg epidemii w Wuhanie – np. serwis społecznościowy WeChat cenzuruje wpisy krytyczne wobec polityki Xi Jinpinga w odniesieniu do COVID-19. Chociaż władze, ulegając presji społecznej i chcąc uregulować rynek, w 2017 r. w ustawie o cyberbezpieczeństwie rozszerzyły regulacje chroniące użytkowników, to powszechnie używane podczas epidemii COVID-19 aplikacje komórkowe często tym regulacjom nie odpowiadały. W styczniu i lutym br. Chińczycy złożyli do Urzędu ds. Cyberprzestrzeni 2 tys. skarg, z czego ok. 15% dotyczyło właśnie luk bezpieczeństwa w oprogramowaniu.

Doświadczenia z inwigilacji Ujgurów i zwalczania COVID-19 pomogły w rozwoju chińskich firm z sektora technologii służących do inwigilacji (m.in. Huawei, Tencent, Hikvision czy Dahua). Przed epidemią wyeksportowały one oprogramowanie i sprzęt do ponad 60 krajów na świecie, m.in. Iranu, Wenezueli, Mjanmy czy Zimbabwe. Z sukcesem rywalizowały np. z japońskim NEC. Sprzyjało temu m.in. udzielanie państwom trzecim przez banki państwowe ChRL kredytów na zakup chińskiego sprzętu. COVID-19 ugruntował pozycję chińskich firm jako dostawców sprzętu w Rosji, ale i państwach demokratycznych. Już w trakcie epidemii kamery termiczne Dahua kupiły np. amerykańskie firmy takie jak Amazon, IBM czy Chrysler. Zarówno Hikvision, jak i Dahua współpracują też np. w Danii w ramach systemów smart cities. Kooperacji z tymi chińskimi firmami w 2019 r. zakazała instytucjom publicznym w USA administracja Donalda Trumpa, powołując się na ich udział w inwigilacji Ujgurów.

Wnioski i perspektywy. Inwigilacja jest immanentną cechą systemu politycznego ChRL. W optyce władz rozbudowa jej mechanizmów w oparciu o AI docelowo ma też zmniejszyć poziom jej odpowiedzialności za niewygodne decyzje. To system i zarządzający nim algorytm miałby bowiem przejąć odium związane z represjami wobec obywateli. Rozwiązania inwigilacyjne władze ChRL będą też chciały wykorzystać w kontekście możliwych niepokojów wynikających z problemów gospodarki chińskiej po COVID-19.

Monitoring, a przede wszystkim możliwe wdrożenie testowanych systemów wiarygodności społecznej, stanowi zagrożenie dla funkcjonowania firm europejskich (i ich pracowników) w ChRL. UE powinna traktować wyłączenie obcokrajowców z tych systemów jako warunek konieczny finalizacji porozumienia inwestycyjnego (EU–China Comprehensive Agreement on Investment).

Obecne w debacie europejskiej przekonanie o skuteczności inwigilacji ChRL w ramach COVID-19 powoduje, że propozycje wdrożenia podobnych mechanizmów mogą pojawić się w programach partii i ruchów politycznych w państwach UE (np. tych, w których polityka Chin jest ważnym elementem debaty politycznej, jak Włochy czy Węgry). Ewentualne wykorzystywanie praktyk i technologii chińskich zagrażałoby prawom obywatelskim w UE, jeśli zostałyby one wdrożone trwale i stosowane nieproporcjonalnie do celów. Konieczne jest np. wdrażanie opracowanych przez KE w 2019 r. etycznych wytycznych np. co do zastosowania AI do systemów oceny zachowania obywateli. Ponadto Unia powinna dążyć do wyłączenia chińskich firm biorących udział w inwigilacji obywateli ChRL z projektów finansowanych ze środków europejskich. Nacisk polityczny ze strony UE na anulowanie kontaktów z tymi podmiotami powinien również dotyczyć państw kandydujących do UE (np. Serbia) czy stowarzyszonych (np. Ukraina).