

Polska Orwellowska?

1 marca 2023

Rośnie sceptycyzm społeczeństwa względem rozwiązań cyfrowych, po które sięgają władze. Coraz więcej osób zdaje sobie sprawę, że nowe technologie otwierają drogę do kontrolowania obywateli. Czy grozi nam „autorytaryzm cyfrowy”?

Sejm pracuje nad Prawem Komunikacji Elektronicznej (PKE) – regulacją potocznie nazywaną „lex pilot”, która chociaż ma na celu m.in. wdrożenie Europejskiego Kodeksu Łączności Elektronicznej, w rzeczywistości jest sprzeczna z prawem unijnym i zasadami państwa prawnego, a jej wdrożenie może doprowadzić do kolejnych napięć z Brukselą.

W początkowym kształcie ustawy można było znaleźć uzasadnienie, że obowiązki w zakresie zbierania i przechowywania nowych kategorii danych mają na celu ochronę państwa oraz zapewnienie bezpieczeństwa publicznego. To jednak nie pierwszy przypadek, w którym rządzący pod hasłem „dobra obywateli” forsują rozwiązania korzystne dla władzy i sięgają po dane użytkowników. Choć pod naciskiem opinii publicznej złożono niedawno poprawki do kontrowersyjnego projektu oraz odroczone jego procedowanie, można spodziewać się, że pomysł pozyskiwania danych Polaków może wrócić po tegorocznych wyborach – jeśli ich wynik okaże się korzystny dla PiS.

Autorytaryzm cyfrowy?

Rażąca dysproporcja pomiędzy poszanowaniem międzynarodowych standardów praw człowieka a działaniami polskich władz przesuwającymi granice ingerencji w swobody obywatelskie, budzi coraz większy niepokój. Biorąc pod uwagę projekty regulacji poszerzających dostęp służb do danych, ich niekontrolowaną inwigilację oraz tło polityczne, wielu badaczy i działaczy społecznych zadaje pytania o to, czy Polska zbliża się do systemu politycznego, który można nazwać

„autorytaryzmem cyfrowym”.

Zgodnie z badaniami Access Now, organizacji non-profit, której misją jest obrona i rozszerzenie świadomości w zakresie cyfrowych praw człowieka, istnieją cztery podstawowe cechy, którymi charakteryzują się cyfrowe dyktatury: niemalże nieograniczony nadzór i inwigilacja obywateli; propagowanie mowy nienawiści i szerzenie dezinformacji; odcinanie dostępu do Internetu, a także wprowadzanie cenzury bądź blokowanie niezależnych mediów. Poszczególne mechanizmy, regulacje czy konkretne rozwiązania technologiczne można ocenić pod kątem tego, w jakim stopniu przybliżają władzę do wywierania presji i sprawowania wszechobecnej kontroli nad życiem obywateli.

Nadzór i inwigilacja

Masowy i ukierunkowany nadzór znany w reżimach autorytarnych dokonuje się przede wszystkim za pomocą oprogramowania szpiegowskiego. Jego ofiarami zwykle są krytycy rządu lub działacze polityczni, którzy z różnych przyczyn stali się niewygodni dla władzy. Najlepszym przykładem nadużywania nowych technologii do realizacji celów politycznych jest sprawa Pegasus, oprogramowania szpiegowskiego wykorzystywanego przez polski rząd do nieproporcjonalnej inwigilacji przeciwników politycznych. Jej skali oraz katalogu osób będących na podsłuchu do tej pory nie ustalono. Jak wskazano w raporcie komisji śledczej Parlamentu Europejskiego, jego stosowanie nie było transparentne i znajdowało się poza jakąkolwiek kontrolą, skala ingerencji w prawa jednostki była niewspółmierna do celu (rzekomo bezpieczeństwa narodowego i porządku publicznego), a nadzór wymiaru sprawiedliwości nad praktykami w zakresie inwigilacji pozostawał iluzoryczny. Jak podkreślił PE, w Polsce zgoda sądu na kontrolę operacyjną służy nie jako mechanizm zabezpieczający przed nadużyciami, ale stanowi środek legalizacji inwigilacji dla celów politycznych.

Ofiary inwigilacji mogą nigdy nie dowiedzieć się o podsłuchach, co sprawia, że teoretyczne istnienie możliwości wniesienia sprawy sądowej, tak naprawdę nie jest egzekwowane. Jak podaje Fundacja Panoptikon, już dwa lata temu polska policja chętnie korzystała ze swoich uprawnień, przetwarzając dane telekomunikacyjne obywateli prawie 2 mln razy. W obliczu zakupionego niedawno narzędzia, które umożliwi policji odzyskanie i pobranie danych nawet z zablokowanych czy zaszyfrowanych urządzeń (również GPS czy dronów), wszyscy obywatele mają uzasadnione powody do tego, by czuć się jak podejrzeni.

Mowa nienawiści i dezinformacja

Sponsorowane przez państwo kampanie propagandowe i dezinformacyjne, brak reakcji na hejt w Internecie czy aktywny udział w podżeganiu do nienawiści np. wobec konkretnych społeczności – to również wyznaczniki istnienia napędzanego cyfrowo reżimu autorytarnego. Pomimo deklarowanej przez partię rządzącą walki z dezinformacją, nietrudno przypomnieć sobie przykłady, w których media propagowały nieprawdziwe treści wymierzone w opozycjonistów, czy wykorzystywały dane z mediów społecznościowych dla osiągnięcia własnych celów. Próby algorytmicznej manipulacji wyborcami wystąpiły chociażby w 2020 roku podczas kampanii Andrzeja Dudy, w następstwie której doszło do reelekcji prezydenta. Jedną z największych akcji dezinformacyjnych polskiego rządu dotyczyła natomiast strajków kobiet – w rzeczywistości wzięło w nich udział około 430 tys. osób, ale media prorządowe sukcesywnie zaniżały te statystyki, podając informacje o zaledwie kilku tysiącach i „chmurze covidowej” unoszącej się nad strajkującymi. Słynne paski informacyjne TVP nierzadko zawierały obraźliwe zwroty i fałszywe treści. Jak stwierdziła Rada Języka Polskiego w sprawozdaniu skierowanym do Sejmu, używany przez Wiadomości TVP język polski to „instrument w walce politycznej [...] w celu kreacji własnej wizji świata i narzucania jej obywatelom”.

Niepokojące są również doniesienia o możliwym powiązaniu twitterowego konta „Visegrad24” (jednego z największych i bardziej dezinformacyjnych serwisów w Polsce) z politykami partii rządzącej.

Cenzura i blokowanie niezależnych mediów

W reżimach autorytarnych, utrzymanie władzy wiąże się zwykle z koniecznością wprowadzenia ograniczeń wolności wypowiedzi czy blokowania mediów, które w przestrzeni cyfrowej prezentują treści niezależne od dyskursu politycznego rządu. W tym kontekście znamieną wydaje się niechęć Krajowej Rady Radiofonii i Telewizji (KRRiT) wobec przedłużenia koncesji dla TVN. Krajowa Rada określała stację mianem „jakby piątej kolumny wobec państwa polskiego”, wysuwając jednocześnie tezę, że działania przez nią prowadzone zmierzają do obalenia rządu. Co więcej, jednymi z pierwszych kontrowersji wokół lex pilot były przepisy uprzywilejowujące telewizję publiczną poprzez umieszczenie na pierwszych kanałach TVP1, TVP2, TVP3, TVP Kultura i TVP Info. Przyjęcie PKE w takim kształcie prowadziłoby więc do jawnej dyskryminacji stacji komercyjnych, naruszenia uczciwej konkurencji na rynku oraz pogwałcenia zasady pluralizmu mediów. Wszystko to celem ściślejszego nadzoru przepływu informacji i kształtowania charakteru ich przekazu medialnego.

W kontekście kontrolowania treści udostępnianych w sieci, niepokojące wydają się również oficjalne informacje o powrocie Ministerstwa Sprawiedliwości do procedowania ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych. Choć pomysłodawcy tego projektu podkreślają konieczność ochrony „zagrożonej demokracji”, wolności obywatelskich i zapewnienia swobody debaty publicznej, w rzeczywistości ustawa doprowadzi do przekazania Krajowej Radzie Usług Cyfrowych (kontrolowanej przez KRRiT) kompetencji do decydowania, co

wolno, a czego nie należy mówić w Internecie.

Rzeczpospolita autorytarna?

Przypadki wykorzystywania nowych technologii do realizacji celów politycznych spowodowały spadek zaufania obywateli do państwa oraz proponowanych przez rząd innowacji opartych o dane. Świadczą o tym chociażby kontrowersje wokół Systemu Informacji Medycznej (nazwanego niechlubnie rejestrem ciąży), którego wdrożenie, choć wynikało z przepisów unijnych, wywołało ogólne oburzenie i obawy o to, że strata dziecka będzie weryfikowana przez organy ścigania.

Z takich powodów, wraz z powstawaniem coraz to bardziej zaawansowanych narzędzi technologicznych demokracje powinny opracować nowe, szyte na miarę XXI wieku sposoby kontroli władzy po to, by zapewnić, że nowe technologie działają z korzyścią, nie zaś szkodą dla społeczeństwa.

Blanka Wawrzyniak – kierowniczka programu badawczego gospodarki cyfrowej w Fundacji InStrat. Prawniczka i badaczka zajmująca się prawem konkurencji oraz społeczno-ekonomicznymi aspektami nowych technologii: etyką sztucznej inteligencji, prawami człowieka w sieci, przyszłością pracy i sektorem gig-economy, zarządzaniem danych w interesie publicznym.

Autorstwo: Marta Musidłowska

Źródła: Trybuna.info, Visegrad Institute

0 autorce

Marta Musidłowska –

**stypendystka
programu Marcina
Króla w Visegrad
Insight. Analityczka
polskich, unijnych i
amerykańskich
regulacji związanych
z nowymi
technologiami,
przede wszystkim
dotyczących ochrony
i zarządzania**

**danymi. Wspierała
również prawnie
polsko-amerykański
startup rozwijający
aplikację służącą
świadomym wyborom
konsumenckim.**