Grzegorz Rydlewski

RZĄDZENIE W EPOCE INFORMACJI, CYFRYZACJI I SZTUCZNEJ INTELIGENCJI

DOM WYDAWNICZY ELIPSA

Rządzenie w epoce informacji, cyfryzacji i sztucznej inteligencji

Wydział Nauk Politycznych i Studiów Międzynarodowych
Uniwersytet Warszawski

Grzegorz Rydlewski

Rządzenie w epoce informacji, cyfryzacji i sztucznej inteligencji

DOM WYDAWNICZY
ELIPSA

Warszawa 2021

Publikacja dofinansowana przez Wydział Nauk Politycznych
i Studiów Międzynarodowych Uniwersytetu Warszawskiego

Recenzenci
prof. dr hab. Andrzej Antoszewski (Uniwersytet Wrocławski)
prof. dr hab. Jan Garlicki (Uniwersytet Warszawski)

Redakcja
Ewa Rydlewska

Projekt okładki
Agnieszka Miłaszewicz

Korekta
Zespół

ISBN 978-83-8017-369-9
DOI 10.33896/978-83-8017-369-9

DOM WYDAWNICZY ELIPSA

Opracowanie komputerowe, druk i oprawa:
Dom Wydawniczy ELIPSA
ul. Inflancka 15/198, 00-189 Warszawa
tel. 22 635 03 01
e-mail: elipsa@elipsa.pl, www.elipsa.pl

Spis treści

Professor Grzegorz Rydlewski, PhD
University of Warsaw
Faculty of Political Science and International Studies

Governance in the Age of Information, Digitalisation and Artificial Intelligence

Table of Contents

Tytułem wstępu

Na początku trzeciej dekady XXI wieku nie można już mieć wątpliwości co do tego, że pod wpływem ekspansji władzy informacji, komunikacji społecznej i technologii elektronicznej dochodzi w świecie do zmian o strategicznym charakterze. Internet i związane z nim narzędzia są już dominującymi instrumentami społecznej komunikacji. Nasza rzeczywistość zaczyna się upodabniać do dystopijnej wizji: kontakty społeczne w dużej mierze przenoszą się do internetu, a jego użytkowników można sprowadzić do roli podmiotów nieustannie kogoś obserwujących i zarazem przez kogoś obserwowanych w przestrzeni internetowej. Pozycję młodych ludzi w środowisku społecznym zaczyna wyznaczać liczba polubień pod zamieszczanymi przez nich w internecie zdjęciami i tekstami, na ogół bardzo lakonicznymi. W epoce „wiedzy na żądanie" kształtują się nowe sposoby uzyskiwania odpowiedzi na nurtujące ludzi pytania. W tej dziedzinie coraz mniej miejsca pozostaje na własną refleksję na podstawie lektur i kontaktów z reprezentantami starszego pokolenia. Potrzeby poznawcze są w dużym stopniu zaspokajane *ad hoc*, bez większego wysiłku, za pomocą internetowych wyszukiwarek. Ludzie sięgający po te narzędzia pragną otrzymywać jednoznaczne komunikaty, gotowe materiały wolne od skomplikowanych rozważań, napisane przystępnym językiem. Należy to wiązać z szerszym zjawiskiem, jakim jest upadek autorytetów. Poza środowiskiem akademickim nie budzi zainteresowania – trzeba przyznać, w wielu wypadkach bardzo wąska – wiedza specjalistyczna, w obiegu społecznym tracą też na znaczeniu elity nauki. Od dogłębnych i krytycznych analiz, wymagających odpowiedniego przygotowania ze strony czytelnika, ważniejsze są już popularne ujęcia i kompilacje, niekiedy pozbawione większej (lub wszelkiej) wartości merytorycznej. Zmiany polegają jednak nie tylko na powszechnym czerpaniu wiedzy z nowych źródeł; kształtują się też nowe wzorce postępowania. Graczami modelującymi rzeczywistość materialną stają się instytucjonalni i personalni administratorzy rzeczywistości wirtualnej, w tym przede wszystkim potężne firmy będące właścicielami mediów społecznościowych. Swoją wielką siłę pokazują algorytmy wykorzystywane przez pośredników aktywnych w komunikacji internetowej. Tradycyjne przekazy medialne przegrywają ze słuchaniem podcastów.

Przybywa nowych sposobów załatwiania codziennych spraw przy użyciu narzędzi internetowych. Znikają liczne bariery przestrzenne i czasowe. To, co wydawało się niemożliwe i nieosiągalne, dziś jest już dostępne w czasie rzeczywistym. To, co miało być zarezerwowane dla nielicznych, staje się codziennością milionów ludzi. W związku z blokadami bezpośrednich kontaktów na skutek pandemii, która zaatakowała świat w 2020 r., wiele działań ludzi, państw i instytucji zostało przeniesionych do sfery online. Sieć zaczyna znaczyć więcej niż hierarchia. Na świecie kształtuje się nowy układ sił i konkurencji, rysują się nowe linie podziałów i konfliktów, których zasadniczą przesłanką jest dominacja w zakresie technologii cyfrowych. Zjawiska i procesy ze sfery online i offline mieszają się ze sobą i przenikają do wszystkich dziedzin życia. Pojawia się e-rzeczywistość publiczna, a w niej rozwijają się takie formy, jak e-państwo, e-administracja, e-procedury i e-obywatele. Doskonalone, coraz szybsze i bardziej zintegrowane mechanizmy komunikacji elektronicznej oraz rozwiązania w postaci inteligentnych domów (*smart home*) i inteligentnych miast (*smart city*) przynoszą ludziom nowe ułatwienia i możliwości. Wraz ze zmianami w sferze technologii cyfrowej i sztucznej inteligencji (*artificial intelligence*, AI) pojawiają się jednak zupełnie nowe problemy i zagrożenia, których istota i zakres oddziaływania nie są jeszcze do końca rozpoznane. Technologia i polityka mocno się już zazębiają, zaś ich związek okazuje się często groźny dla wartości, standardów i mechanizmów świata demokratycznego. Nie trzeba chyba nikogo przekonywać, jak niebezpieczne dla funkcjonowania państw i ludzi są dezinformacja i manipulacja internetowa, fake newsy, internetowe trolle, hakerzy. Narzędzia technologii informacyjnej są już obecnie wykorzystywane do zwalczania wrogich podmiotów politycznych i struktur instytucjonalnych.

Przybywa relacji na linii człowiek–maszyna, które wypierają, a przynajmniej znacznie modyfikują, bezpośrednie relacje na linii człowiek–człowiek. Wytworzone przez ludzi produkty technologiczne szybko nabywają nowych umiejętności dzięki wykorzystaniu informacji pozyskanych z internetowych zasobów. Dane gromadzone w przestrzeni elektronicznej stają się surowcem do budowania narzędzi sztucznej inteligencji. Dziś całość zmian zachodzących w przestrzeni cyfrowej znajduje się jeszcze w rękach człowieka. Mnożą się jednak wątpliwości, czy tak będzie zawsze, czy inteligentne twory ludzkiej myśli naukowej i technicznej oraz zaawansowane technologie nie wymkną się spod władzy swoich twórców. Z różnych stron są kierowane do rządzących wezwania, by rozwój nowych technologii poddać niezbędnym regulacjom.

Zadziwia fakt, że koncentrując się na przeszłości i czasie bieżącym, w zbyt małym stopniu w badaniach dotyczących polityki zajmujemy się przyszłością, a przecież w ciągu kilkudziesięciu najbliższych lat diametralnie zmienią się warunki i sposób funkcjonowania ludzi, społeczeństw i instytucji. Wyraźnie

odczuwalny jest niedosyt refleksji o wyzwaniach – społecznych i politycznych – wiążących się z tym skokiem w nieznane czekającym ludzkość. Książka ta jest pomyślana jako próba spojrzenia pod tym kątem na najbliższą i bardziej odległą przyszłość polityki. Decyzję o jej napisaniu podjąłem także dlatego, że uznałem, iż – zajmując się od lat w swych publikacjach rządzeniem i decydowaniem politycznym – zbyt mało uwagi poświęciłem zdefiniowaniu i analizie pojawiających się w tym obszarze strategicznych wyzwań przyszłości i nieuniknionych zmian, które się z nimi wiążą.

U podstaw tej publikacji leży przekonanie, że wśród uwarunkowań decydowania politycznego i rządzenia w ostatnich latach, które muszą być uwzględnione przy każdej próbie ustalania kierunków, metod i sposobów dalszego prowadzenia działań w obu tych dziedzinach aktywności, zasadnicze znaczenie mają postępujący wzrost władzy komunikacji oraz ekspansja nowych technologii informacyjnych i rozwiązań w zakresie cywilizacji cyfrowej. Procesy te są dotychczas ujmowane najczęściej w kategoriach nowych mechanizmów i narzędzi optymalizowania działania w sferze funkcjonowania państw, instytucji władzy publicznej oraz podmiotów artykulacji i agregacji interesów politycznych. Wielu widzi w nich swego rodzaju nowe otwarcie w dziejach cywilizacji, źródło nadziei na postęp. Równocześnie zewsząd rozlegają się głosy wskazujące, że procesy te stanowią poważne zagrożenie – i jako takie mogą być dla ludzi źródłem lęku. Nie brakuje więc opinii nacechowanych wartościująco – zarówno ostrzeżeń, jak i wypowiedzi utrzymanych w optymistycznej tonacji – brakuje natomiast szerszej refleksji teoretycznej i spojrzenia strategicznego. Trzy okoliczności wydają mi się w tym kontekście na tyle ważne, że uzasadniają, jak sądzę, zamysł napisania tej książki.

Po pierwsze, w myśleniu o przyszłości politycy zostali znacznie wyprzedzeni przez inżynierów, biologów i badaczy innych specjalności, a także przez działających poza strukturami państwowymi wizjonerów i twórców sieciowej komunikacji społecznej. Przez długi czas rządzący włączali do swojej agendy i wpisywali do budżetów państwowych prace nad maszynami elektronicznymi i algorytmami – głównie z myślą o stworzeniu nowego rodzaju broni, która może zostać wykorzystana w konfrontacji militarnej. W mniejszym stopniu zastanawiano się nad zmianami zasad i mechanizmów rządzenia. W świecie polityki dominowało wąskie i instrumentalne podejście do rewolucji informatycznej – nawet wówczas, gdy upowszechniały się w społeczeństwie coraz bardziej innowacyjne narzędzia elektroniczne i wyraźnie już dawały o sobie znać wykraczające daleko poza obszar technologii skutki tej rewolucji. W istocie poszukiwano możliwości wykorzystania tych narzędzi w dotychczasowym modelu rządzenia i decydowania politycznego. Bardzo długo do świata polityki docierała prawda, że komunikacja społeczna, algorytmy, narzędzia cyfrowe i sztuczna inteligencja mają moc kreowania zmian modelu aktywności grup

ludzi i całych społeczeństw, a co za tym idzie – że stanowią one przesłankę rewizji rozwiązań modelowych w sferze organizacji i funkcjonowania domeny publicznej. Obserwując współczesne linie sporów między politykami i punkty ciężkości pojawiających się programów politycznych, można mieć uzasadnione podejrzenie, że wielu graczy na arenie politycznej nie do końca rozumie, jak ogromną zmianę niesie ze sobą tworzący się w szybkim tempie nowy porządek świata w postaci cywilizacji informacyjnej i technologicznej, o której pisał Alvin Toffler w swoich inspirujących – chciałoby się rzec: proroczych – rozważaniach o etapach ewolucji życia społecznego[1]. U zdecydowanej większości polityków horyzont zainteresowania światem i jego problemami kończy się niestety na najbliższych wyborach organów władzy publicznej w poszczególnych państwach oraz w strukturach ponadpaństwowych i międzypaństwowych.

Po drugie, politycy w niedostatecznym stopniu wyciągają wnioski z fundamentalnych zmian w społeczeństwie, które kształtują w nowy sposób bezpośrednie środowisko ich aktywności. Następstwem tej sytuacji są próby kontynowania rządzenia i decydowania politycznego w sposób w dużej mierze anachroniczny, oparty na modelu społeczeństwa, który odchodzi do historii. Mechanizmy rządzenia w licznych swoich elementach nie odpowiadają już wymaganiom zaawansowanego społeczeństwa sieciowego, którego członkowie permanentnie korzystają z systemów teleinformatycznych oraz elektronicznych technologii informacyjnych i znajdują się pod wpływem działających w ukryciu algorytmów. W efekcie powiększa się niebezpieczny rozziew między modelem artykulacji i agregacji interesów politycznych oraz legitymizacji i funkcjonowania władz publicznych a modelem społeczeństwa.

Wreszcie, po trzecie (to motyw przewodni niniejszych rozważań), w naukach o polityce potrzebne jest bardziej gruntowne przemyślenie strategicznych scenariuszy, kreślących racjonalną wizję przyszłości rządzenia i decydowania politycznego. Nauki o polityce nie mogą być zwrócone jedynie ku przeszłości i teraźniejszości. Konieczność spojrzenia w przyszłość wręcz się narzuca, bo przecież w ostatnim okresie w życiu społecznym i politycznym coraz częściej są podejmowane działania związane z kształtowaniem się nowego technocybernetycznego świata. Na gruncie prawa próbuje się usunąć deficyty regulacyjne w zakresie komunikacji społecznej, sieci komputerowych i telekomunikacyjnych oraz narzędzi sztucznej inteligencji. Obrońcy praw człowieka wskazują na konieczność ograniczenia negatywnych skutków rozbieżności między wolnością a bezpieczeństwem, które nasilają się pod wpływem rozwoju cyfrowych technologii inwigilacji i nadzoru społecznego. Wychodzą na jaw patologie cywilizacji cyfrowej, które niejednokrotnie wywierają bezpośredni wpływ na sferę polityczną lub wręcz wchodzą w skład instrumentarium polityki. Stawiane

[1] A. Toffler, *Trzecia fala*, Poznań 2006, s. 179 i nast.

są pytania o standardy etyczne w odniesieniu do postępu technologicznego i o granice badań naukowych. W reakcji na zachodzące zmiany przeważają jednak nadal działania niemające wymiaru strategicznego. Brak w niej zwykle znamion całościowej refleksji nad nowym modelem rządzenia.

Uważam, że reprezentanci nauk o polityce w większym niż dotychczas stopniu powinni wynikami swojej pracy wspierać refleksję na temat zachodzących zmian. W środowisku politologów nadal dominuje, moim zdaniem błędne, przekonanie, że prognozowanie w sprawach polityki jest na tyle niepewne, iż nie ma sensu podejmować wysiłków w tym kierunku, ponieważ nie mogą one prowadzić do rezultatów wartościowych pod względem naukowym. Z zadowoleniem trzeba jednak odnotować, że zaczynają w tej dziedzinie zachodzić w Polsce pozytywne zmiany. Wśród wartościowych publikacji z ostatnich lat, w których są podejmowane rozważania o istocie oraz społecznym i politycznym znaczeniu ekspansji władzy informacji, komunikacji społecznej, technologii cyfrowej i sztucznej inteligencji, znajdują się również – całkiem liczne – prace autorów polskich. Do wielu z tych publikacji odwołuję się w tej książce w przypisach i końcowym zestawieniu literatury.

Rządzenie, podobnie jak inne sfery aktywności publicznej, podlega ciągłym zmianom. Można wręcz uznać, że zmienność stanowi niezbywalną cechę rządzenia. Nieustannie pojawiają się w tej dziedzinie innowacje, wypierając znane dotąd zjawiska i mechanizmy. Na dynamikę tego procesu w zasadniczy sposób rzutują przeobrażenia zachodzące w środowisku rządzenia, w tym przede wszystkim dotyczące kształtu społeczeństwa, zasobów rządzenia oraz dominujących relacji w przestrzeni publicznej[2]. Rozległość i natężenie tych przeobrażeń każą sądzić, że proces zmian w rządzeniu ulegnie przyspieszeniu. Zmiany te będą się odnosić do strony podmiotowej, przedmiotowej i funkcjonalnej rządzenia. Rewolucja cyfrowa w sposób nieunikniony przełoży się na transformację ustrojową w sferze wykonywania władzy publicznej i organizacji działalności politycznej.

Prognozowanie przyszłości rządzenia w przestrzeni publicznej jest przydatne dla praktyki. W naukach o polityce stanowi ono istotne wyzwanie badawcze. Intensywność i rozległość zmian rzeczywistości społecznej w epoce technologii cyfrowych sprawia, że teraźniejszość staje się teraz bardzo szybko przeszłością, zaś przyszłość – teraźniejszością. Tworzenie projekcji przyszłości może służyć uwolnieniu refleksji na temat rządzenia od spojrzenia z doraźnej perspektywy, czyli zamknięcia w kręgu spraw bieżących, a tym samym może się przyczyniać do lepszego przygotowania tej dziedziny aktywności do sprostania wyzwaniom przyszłości.

---

[2] Szerzej na ten temat: G. Rydlewski, *Rządzenie w świecie megazmian. Studium politologiczne*, Warszawa 2009.

Można wskazywać liczne przykłady reagowania w rządzeniu na projekcje przyszłości, które pojawiają się w przestrzeni publicznej. O wartości prognoz w tej dziedzinie decyduje więc nie tylko ich domniemana trafność (ostatecznie weryfikowana po pewnym czasie rzeczywistym rozwojem wydarzeń), lecz także to, w jakim stopniu są one już obecnie narzędziem kreowania rzeczywistości. Takie projekcje wpływają na dzisiejsze zachowania polityków, a przy tym stanowią swego rodzaju inwestycję w przyszłość. Niedobór systemowej refleksji nad przyszłością niesie za sobą ryzyko podejmowania w rządzeniu przypadkowych, nieprzemyślanych decyzji i działań, co oznacza, że gra o przyszłość mieć będzie w dużej mierze charakter loteryjny, stając się domeną partykularnych i doraźnych interesów. Natura nie znosi próżni, mówi znana sentencja; parafrazując ją, można powiedzieć, że w polityce nie ma miejsca na niezagospodarowane przestrzenie. Świadomość tego faktu nakazuje wprowadzić wymiar przyszłości do debaty o rządzeniu.

Publikacja ta składa się z jedenastu rozdziałów. W pierwszym z nich w sposób syntetyczny prezentuję rządzenie jako zjawisko podlegające procesowi stałych zmian i pozostające w silnych wzajemnych powiązaniach ze swoim otoczeniem. W rozdziale drugim przedstawiam ekspansję władzy komunikacji, technologii cyfrowych i sztucznej inteligencji jako strategiczną przesłankę zmian w rządzeniu. W rozdziale trzecim ukazuję, jakie znaczenie dla rządzenia ma kształtowanie się pod wpływem rozwoju cywilizacji technologiczno-informacyjnej nowego modelu społeczeństwa. W rozdziale czwartym rozpatruję w kontekście politycznym możliwości i zagrożenia wiążące się z funkcjonowaniem mediów społecznościowych i rozwojem cywilizacji cyfrowej. W rozdziale piątym zwracam uwagę na unikatową wartość danych zgromadzonych w zasobach cyfrowych oraz wskazuję problemy związane z wykorzystywaniem tych danych, w tym nowy wymiar napięć między wolnością, prywatnością i bezpieczeństwem, który wiąże się ze zjawiskiem inwigilacji elektronicznej. Rozdział szósty poświęcam zagadnieniu wejścia nowych technologii komunikacyjnych i cyfrowych w zakres konkurencji i konfrontacji między państwami oraz zajmuję się prognozami mówiącymi o nasilaniu się nierówności społecznych w kształtującym się cybernetycznym porządku świata. W rozdziale siódmym próbuję spojrzeć na cyberprzestrzeń jako na miejsce spotkania technologii i polityki przez pryzmat ich patologicznych związków. Analizując zjawisko rozpowszechnienia w internecie politycznej dezinformacji i manipulacji, szczególną uwagę poświęcam kwestii zagrożeń procesów wyborczych oraz wielopodmiotowym działaniom systemowym mającym na celu ograniczenie patologii cyfrowych. W rozdziale ósmym przedstawiam wyzwania regulacyjne dla rządzenia, w tym w sferze etyki i prawa, które niesie za sobą ekspansja cywilizacji cyfrowej, oraz dokonuję przeglądu działań na rzecz uregulowania zasad i standardów rozwoju inteligentnych technologii. W rozdziale dziewiątym

wskazuję na jakościowe wyzwania dla rządzenia w dziedzinie bezpieczeństwa związane z wzrastającym uzależnieniem od niezakłóconego funkcjonowania narzędzi cyfrowych, ewolucją charakteru potencjalnych konfliktów, cyberprzestępczością oraz podejmowaniem przez niektóre państwa wrogich działań polegających na hakowaniu świadomości społecznej, urządzeń elektronicznych i oprogramowania komputerowego. W rozdziale dziesiątym prezentuję strategiczne usytuowanie sztucznej inteligencji wśród narzędzi zrównoważonego i odpowiedzialnego rozwoju oraz stan wykorzystania rozwiązań cywilizacji cyfrowej w sferze polityki, rządzenia i administracji w Polsce. W ostatnim, jedenastym rozdziale zestawiam strategiczne dylematy pojawiające się w ramach polityki i rządzenia, które są związane z dalszą ekspansją cywilizacji cyfrowej, w tym dotyczące przyszłości demokracji elektronicznej, decydowania i administrowania publicznego oraz polityk publicznych. Na tym tle stawiam pytania o miejsce człowieka i obywatela w cyfrowym świecie, sytuację państwa w tej nowej rzeczywistości, a także przyszłość modelu klasycznej demokracji przedstawicielskiej.

Podejmując próbę nakreślenia obrazu czekających nas zmian w rządzeniu, już na początku muszę uczynić dwa zastrzeżenia. Po pierwsze – w tych rozważaniach mowa jest o decydowaniu, rządzeniu i władzy w przestrzeni publicznej, podczas gdy w różnych ujęciach, zwłaszcza filozoficznych, socjologicznych i psychologicznych, można odnaleźć inne konteksty i zastosowania pojęcia rządzenia. Wspomnieć tu można, tytułem przykładu, stanowisko Michela Foucaulta[3], zgodnie z którym rządzenie „polega na wpływaniu na postępowanie innych ludzi, a dokładniej mówiąc: na oddziaływaniu na ich zdolność do regulacji własnego zachowania”[4]. Po drugie – nie jest celem tej książki szczegółowe analizowanie technicznego wymiaru zmian, które wiążą się z ekspansją cywilizacji cyfrowej i sztucznej inteligencji. Te kwestie zostawiam specjalistom, z których merytorycznych ustaleń korzystam w tej publikacji. Zastanawiam się natomiast przede wszystkim nad prawdopodobnymi korelacjami między tymi zmianami a rewizją mechanizmów i rozwiązań modelowych występujących w świecie polityki, decydowania politycznego i rządzenia.

Prognozowanie w sprawach społecznych nie jest łatwe. Mamy w tej materii do czynienia z wieloma niewiadomymi, dlatego przewidywanie przyszłości zawsze będzie obciążone arbitralnością. Pozostaje więc tylko wskazywać na możliwe współwystępowanie rozpatrywanych zjawisk i procesów oraz prawdopodobne współzależności i korelacje między nimi. W istocie nie ma tu miejsca

---

[3] M. Foucault, *Nadzorować i karać. Narodziny więzienia*, Warszawa 1998; tegoż, *Filozofia, historia, polityka. Wybór pism*, Warszawa 2004; tegoż, *Bezpieczeństwo, terytorium, populacja*, Warszawa 2010.

[4] M. Juza, *Między wolnością a nadzorem. Internet w zmieniającym się społeczeństwie*, Warszawa 2019, s. 144.

na formułowanie apodyktycznych sądów czy kategorycznych twierdzeń. Jest natomiast zapotrzebowanie na przemyślane hipotezy i wnioski powiązane z rekonstrukcją ich przesłanek[5]. Jak słusznie zauważa Yuval N. Harari: „Historia uczy, że rozwój wydarzeń, który wydaje się najbardziej prawdopodobny, może nigdy nie nastąpić z powodu nieprzewidzianych przeszkód, i że materializują się inne, nieprzewidziane scenariusze"[6]. Równocześnie – idąc tokiem myślenia Harariego – „powinniśmy poważnie traktować tezę, że następny etap dziejów będzie stał pod znakiem nie tylko transformacji natury technicznej i organizacyjnej, ale także fundamentalnych przemian ludzkiej świadomości i tożsamości"[7].

Wypada jeszcze podkreślić, że nie rozważam w tej książce prawdopodobieństwa pojawienia się w przyszłości zupełnie nowej tożsamości podmiotów decydujących o biegu spraw w układzie światowym[8]. Jako politologa interesuje mnie przyszłość rządzenia, w ramach której kreowanie rzeczywistości politycznej będzie nadal pozostawało w rękach ludzi i będzie ukierunkowane na to, by nowe rozwiązania technologiczne służyły efektywnej realizacji wartości i spełnianiu potrzeb ludzi, zgodnie z ideą godności ludzkiej, prawami i wolnościami człowieka i z przestrzeganiem zasady różnorodności kulturowej.

Kilkanaście lat temu Edmund Wnuk-Lipiński, pisząc o ówczesnych zmianach w przestrzeni społecznej i politycznej, stwierdził, że żyjemy w „międzyepoce" (określenie zapożyczone od Melchiora Wańkowicza), czyli w czasach przejściowych, zaś „najgłębsze zmiany jakościowe są prawdopodobnie jeszcze przed nami"[9]. Znakomity socjolog miał rację. Już dziś widać wyraźnie, że w dużej mierze za sprawą inteligentnych technologii zintegrowanych sieciowo z ludźmi nasza przyszłość zmieni się tak dalece, iż „to, co nieprawdopodobne, stanie się nową normalnością"[10]. Warto o tym dyskutować – i przygotowywać się do nadejścia takich czasów.

Już kilkadziesiąt lat temu Zbigniew Brzeziński pisał na temat niebezpieczeństw związanych z rewolucją technologiczną połączoną z umocnieniem się podejścia technokratycznego. Przewidywał, że „Społeczeństwo będzie kontrolowane przez elity pozbawione wszelkich etycznych ograniczeń. Takie elity nie zawahają się przed wykorzystaniem najnowszych technologii dla własnych

---

5 Zob. J. Zych, *Teleinformatyka dla bezpieczeństwa 2.0*, Poznań 2019, s. 32 i nast.

6 Y.N. Harari, *Sapiens. Od zwierząt do bogów*, Kraków 2018, s. 506.

7 Tamże.

8 Zainteresowanych taką perspektywą odsyłam do pracy Maxa Tegmarka, kreślącej wizję przemian życia od etapu biologicznego do etapu technologicznego, w którym poszczególne podmioty będą zdolne projektować „swoje organy i oprogramowanie". Zob. M. Tegmark, *Życie 3.0. Człowiek w erze sztucznej inteligencji*, Warszawa 2019 (tam też obszerna literatura na ten temat).

9 E. Wnuk-Lipiński, *Świat międzyepoki*, Kraków 2004, s. 7.

10 K. Kelly, *Nieuniknione. Jak inteligentne technologie zmienią naszą przyszłość*, Warszawa 2017; P. Levinson, *Miękkie ostrze, czyli historia i przyszłość rewolucji informacyjnej*, Warszawa 2006.

celów, aby wpływać na opinie ludzi i utrzymywać społeczeństwo pod ciągłą kontrolą. (…) Wkrótce będzie możliwe prowadzenie niemal ciągłego nadzoru nad każdym obywatelem i utrzymanie stale uaktualnianych akt zawierających nawet najbardziej osobiste dane obywateli. Akta będą podlegały szybkiemu wglądowi przez władze”[11].

Podzielam pogląd, który wyraził w swej książce Kai-Fu Lee, jeden ze światowych liderów badań i wdrożeń w zakresie sztucznej inteligencji, pisząc, że we wszystkich dziedzinach życia i pracy ludzi oraz funkcjonowania struktur społecznych, politycznych i gospodarczych znajdujemy się w zupełnie wyjątkowym momencie[12]. Sztuczna inteligencja, którą wspomniany badacz i praktyk zalicza (w ślad za ujęciem, które zaproponowali Erik Brynjolfsson i Andrew McAfee[13]) do technologii ogólnego przeznaczenia, wychodzi z fazy eksperymentów badawczych i w wielkim tempie wkracza w fazę zastosowań. Tak jak w przeszłości silniki parowe i elektryczność, a w naszych czasach technologie informacyjne i komunikacyjne, sztuczna inteligencja wymyka się dotychczasowym schematom i doświadczeniom składającym się na proces zmian, tworząc zupełnie nowe możliwości i zagrożenia. Technologia internetowa ma już za sobą etap budowy narzędzi interaktywnej komunikacji elektronicznej, tworzenia inteligentnych wyszukiwarek oraz kształtowania mechanizmów bazujących na algorytmach. Opanowano już zdolności ustalania w ramach rozbudowywanych z każdym dniem zbiorów cyfrowych danych, relacji przyczynowo-skutkowych między różnymi – pozornie odległymi od siebie – faktami. Obecnie sztuczna inteligencja znajduje się w swym rozwoju w fazie, w której może nie tylko porządkować dane, ale i je „rozumieć” oraz analizować w sposób zacierający granice między światem online i offline. Coraz więcej przykładów przemawia za tym, że wspomniana technologia ogólnego przeznaczenia wchodzi w fazę rozwoju zdolności autonomicznych, które pozwolą tworom sztucznej inteligencji włączyć się w tworzenie rzeczywistości[14]. To musi zmieniać reguły gry także w rządzeniu.

---

11 Z. Brzeziński, *Between Two Ages. America's Role in the Technetronic Era*, New York 1970.

12 Kai-Fu Lee, *Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata*, Poznań 2019.

13 E. Brynjolfsson, A. McAfee, *Drugi wiek maszyny. Praca, postęp i dobrobyt w czasach genialnych technologii*, Warszawa 2015.

14 Kai-Fu Lee, *Inteligencja sztuczna…*, s. 130 i nast.

Rozdział pierwszy

Zmiany i spory jako trwały element w historii rządzenia

1.1. Interaktywne powiązania między polityką i jej otoczeniem

Silny wpływ otoczenia społecznego, politycznego i międzynarodowego na rządzenie • Zmiana jako trwały element historii rządzenia • Załamywanie się monopolu państw i rządów na rządzenie • Umacnianie się wielocentrycznego, wielopoziomowego i wielopasmowego modelu rządzenia

Dla relacji między rządzeniem a współczesną ekspansją władzy informacji, cywilizacji cyfrowej i sztucznej inteligencji podstawowe znaczenie ma fakt, że polityka zawsze pozostaje w interaktywnych związkach ze swoim otoczeniem zewnętrznym, w tym zwłaszcza z otoczeniem społecznym, politycznym i międzynarodowym. To właśnie kształt tego otoczenia wyznacza w dużym stopniu treść i zasady decydowania politycznego rozumianego jako dokonywanie nielosowych wyborów ukierunkowanych na zdobycie i utrzymanie władzy w strukturach publicznych, uzyskanie wpływu na zagospodarowanie zasobów społecznych oraz alokację dóbr, określanie celów i standardów sprawowania władzy publicznej i prowadzenia polityk publicznych.

Z otoczenia rządzenia pochodzą impulsy do decydowania politycznego, jego zasoby i czynniki ograniczające. Zjawiska i procesy zachodzące w szeroko rozumianej sferze społecznej oraz publicznej są zarazem uwarunkowaniem decydowania politycznego i wyzwaniem dla niego, zarazem wyznaczają jego ramy i znajdują się pod jego wpływem.

Zmiany o charakterze aksjologicznym, podmiotowym, przedmiotowym, systemowym i funkcjonalnym stanowią trwały element rządzenia. W ich wyniku nie można już obecnie sprowadzać rządzenia wyłącznie do działania gabinetów ministrów. Mimo że nadal, szczególnie na gruncie nauk prawnych, aktualne jest badanie rządzenia na tle trójpodziału władzy i wpisywanie do jego

treści przede wszystkim działań z obszaru władzy wykonawczej, w naukach o polityce wydaje się przydatne szersze ujęcie pojęcia „rządzenie". W takim ujęciu uwzględnić trzeba sfery aktywności państw, struktur ponadpaństwowych i międzypaństwowych oraz ich organów władzy i administracji. W takim pojmowaniu rządzenia chodzi głównie o wykonywanie władzy publicznej i realizację polityk publicznych. Tak też rządzenie jest rozumiane w tej publikacji.

Od końca XX wieku załamuje się monopol państw i rządów na rządzenie. Utrwala się pluralistyczny model rządzenia. Coraz większe znaczenie zyskuje rządzenie ponadnarodowe. Jak zauważają w podsumowaniu badań na ten temat Agnieszka Rothert i Anna Wierzchowska, stanowi ono „złożony system, w którym nie istnieje jedna, suwerenna władza, lecz funkcjonuje sieć interakcji i relacji pomiędzy organami lokalnymi, regionalnymi, państwowymi i ponadpaństwowymi, sektorem publicznym i prywatnym"[1]. Jak już sygnalizowałem przed ponad dekadą, następuje „różnicowanie się strony podmiotowej i przedmiotowej rządzenia, połączone z załamywaniem się monopolu państw i rządów oraz kształtowaniem się wielopoziomowego, wielopasmowego i wielocentrycznego modelu rządzenia, w którym aktywnymi podmiotami (niepaństwowymi aktorami określanymi nieraz terminem *non-state actors*) stają się również podmioty zlokalizowane poniżej i powyżej poziomu państwowego (w tym przede wszystkim niepaństwowe organizacje społeczeństwa obywatelskiego, organizacje ponadnarodowe oraz globalne korporacje finansowe i gospodarcze)"[2]. Z perspektywy czasu, który upłynął od napisania powyższych słów, widać, że zawarta w nich charakterystyka zachowała aktualność. Wymaga jednak istotnego uzupełnienia o bardziej szczegółowe ujęcie przesłanek erozji tradycyjnego modelu rządzenia: mam tu na myśli zjawiska i procesy związane z ekspansją nowych form i narzędzi komunikacji społecznej oraz umacnianiem się cywilizacji cyfrowej.

Tezy o kształtowaniu się nowych mechanizmów rządzenia nie można utożsamiać z opinią, że misja państw i rządów uległa w tej dziedzinie wyczerpaniu. Doświadczenie historyczne podpowiada, że państwa i rządy będą odnajdywać nowe narzędzia służące zachowaniu swojej władczej pozycji. Pogląd Ulricha Becka, że państwa w zmieniających się warunkach nie są już w stanie realnie kontrolować kluczowych procesów ekonomicznych, społecznych i politycznych, wydaje się dyskusyjny. Nie budzi natomiast wątpliwości teza, że „polityka nie jest już jedynym i centralnym miejscem, w którym decyduje się o kształtowaniu społecznej przyszłości"[3], bowiem dziś służą temu celowi działania podejmowane w różnorodnych polach subpolityki, w tym w ramach gospodarki, nauki

---

1 *Wprowadzenie* w tomie monograficznym „Studiów Politologicznych" pod wspólnym tytułem *Rządzenie w przestrzeni ponadnarodowej*, 2013, t. 27, s. 9.

2 G. Rydlewski, *Rządzenie w świecie megazmian…*, s. 67.

3 U. Beck, *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Warszawa 2002, s. 341.

i techniki. Jednak nawet jeśli w zakresie ekspansji nowych, inteligentnych technologii komunikacyjnych i cyfrowych państwa zostały wyprzedzone przez innych aktorów, a dziedzina ta uzyskała znaczny zakres autonomizacji, to dziś już widać, że podmioty państwowe przystąpiły do zdecydowanej kontrofensywy. Państwa i rządy walczą o odzyskanie swojej pozycji na płaszczyźnie kształtowania i kontroli rzeczywistości społecznej poprzez mocniejsze wykorzystywanie narzędzi cyfrowych i sztucznej inteligencji do realnego, a nie tylko nominalnego, pełnienia swojej misji władczej.

1.2. Związki między rządzeniem i władztwem politycznym

Trwałe usytuowanie rządzenia w kręgu wykonywania władzy publicznej • Zróżnicowane mechanizmy zmian w rządzeniu • Rządzenie wyzwaniem intelektualnym, organizacyjno-logistycznym, politycznym, finansowym, świadomościowym i komunikacyjnym • Powiązania między optymalizowaniem rządzenia a synergicznym zespoleniem potencjału ludzi, mechanizmów i procedur

Rządzenie – podlegając nieustannym zmianom aksjologicznym, podmiotowym, przedmiotowym, systemowym i funkcjonalnym, powiązanym z dynamiką swojego otoczenia – obejmuje zawsze instytucje i działania oraz stosunki związane z wykonywaniem władzy publicznej, w tym przede wszystkim władzy politycznej.

W historii rządzenia proces jakościowych zmian nie miał charakteru linearnego. Co pewien czas następował w nim powrót do tych samych (lub analogicznych) problemów i odbywała się rewizja poszczególnych rozwiązań. Należy też podkreślić, że rządzenie zawsze pozostawało we wzajemnych relacjach ze swoim otoczeniem zewnętrznym, w tym zwłaszcza z otoczeniem społecznym, politycznym i międzynarodowym. W bilansie tych relacji wpływ otoczenia na rządzenie był zwykle większy niż wpływ rządzenia na otoczenie. Dotychczasowe doświadczenia w dziedzinie rządzenia pokazują, że jest ono równocześnie wyzwaniem intelektualnym, organizacyjno-logistycznym, politycznym, finansowym, świadomościowym i komunikacyjnym. Z pewnością nie zmieni się to w przyszłości, co oznacza, że projekty optymalizowania rządzenia w zmieniających się warunkach muszą uwzględniać wyzwania związane z synergicznym łączeniem potencjału ludzi (w tym polityków i urzędników), instytucji (decyzyjnych, sztabowych i koordynacyjnych, analitycznych i wspomagających, wykonawczych) oraz mechanizmów i procedur (programowania, realizacyjnych i ewaluacyjnych). Coraz wyraźniej widać, że optymalizacja rządzenia będzie wymagać roztropnego współdziałania ośrodków władzy i wiedzy oraz otwartości na zachodzące zmiany cywilizacyjne.

1.3. Rządzenie jako aktywność służąca realizacji zmieniających się wyzwań

Rządzenie jako układ funkcjonalny • Rządzenie jako układ decyzyjny • Rządzenie jako system zarządzania

Rządzenie jest układem funkcjonalnym wartości, interesów, norm, celów i zadań oraz instytucji, procedur, rozwiązań kadrowych. Musi sprostać zmieniającym się wyzwaniom. Bez względu na przyjęte rozumienie tego zakresu aktywności, rządzenie jest systemem celowych działań, w ramach których w przestrzeni publicznej następuje identyfikowanie, zagospodarowanie, wykorzystanie i ukierunkowywanie zasobów materialnych, ludzkich, instytucjonalnych oraz sytuacyjnych. Jest obszarem, w którym wpływ uwarunkowań zewnętrznych, działania wewnątrzsystemowe oraz treść i charakter następstw tych działań tworzą interaktywną całość[4].

Rządzenie stanowi swoisty układ decyzyjny, w którym równolegle, w warunkach znacznej zmienności i ryzyka oraz niepewności, realizowane są przez liczne podmioty konkurencyjne cele i zadania. W procesie rządzenia dokonuje się w sposób nielosowy, w sytuacji istnienia merytorycznej alternatywy, wyboru kierunków i sposobów działania w sprawach publicznych. Mówiąc najkrócej: rządzenie jest miejscem określania i wykonywania polityki.

Rządzenie stanowi współcześnie także multicentryczny, wielopoziomowy i wielopasmowy system zarządzania. W jego ramach – w warunkach przenikania się układów hierarchicznych i sieciowych – programowana, legitymizowana i organizowana jest aktywność ludzi, grup społecznych oraz instytucji publicznych. W systemie tym wyznacza się przestrzeń działania podmiotów pozarządowych, nadaje się kształt strukturom instytucjonalnym, wybiera kierunki i ścieżki rozwoju.

1.4. Wzrost znaczenia w rządzeniu mechanizmów funkcjonalnych i relacyjnych

Rządzenie jako rozwiązanie systemowe • Wzrost znaczenia w rządzeniu mechanizmów funkcjonalnych i relacyjnych • Zmieniająca się pozycja rządu w tworzeniu polityki

[4] Szerzej na ten temat: G. Rydlewski, *Rządy i rządzenie w Polsce 1918–2018. Ciągłość i zmiany*, Warszawa 2018, s. 15 i nast.

W ujęciu strukturalnym rządzenie stanowi określoną konstrukcję systemową. W ujęciu funkcjonalnym rządzenie jest zbiorem działań, w którym – mając na uwadze konkurujące cele i programy, sprzeczne oczekiwania, konflikty interesów (potencjalne lub zaistniałe) oraz ogrom społecznych potrzeb i ograniczone możliwości ich zaspokojenia – dokonuje się nielosowych wyborów prowadzących do rozdziału dóbr, zarządzania zasobami i zagospodarowania kanałów przepływów. W ramach rządzenia nieustannie odbywa się decydowanie o sprawach ogólnych, branżowych i jednostkowych, strategicznych i szczegółowych.

Dzisiaj już wyraźnie widać, że – między innymi za sprawą ekspansji masowej komunikacji zindywidualizowanej oraz technologii cyfrowych – w rządzeniu instytucje ustępują w coraz większym stopniu mechanizmom funkcjonalnym i relacyjnym. Te mechanizmy z kolei nie są już tylko odpersonalizowanymi narzędziami, ulegają znacznemu upodmiotowieniu. Rośnie znaczenie relacji związanych między innymi z dominującym w przestrzeni publicznej sposobem kształtowania, reprezentowania, uzasadniania, konfrontowania i uzgadniania zróżnicowanych interesów oraz z nowymi technikami wyrażania poglądów i interaktywnego komunikowania się, w tym debatowania i toczenia sporów bez konieczności fizycznego spotkania, czy też z rządzącym się nowymi prawami językiem używanym w sprawach publicznych. Zyskują na znaczeniu i mocniej zaczynają oddziaływać zjawiska ze sfery wartości i świadomości, szczególnie model aksjologiczny przestrzeni publicznej, stan opinii publicznej oraz dominujące cechy kultury politycznej i prawnej społeczeństwa. Zjawiska i procesy zachodzące w sferze publicznej są zarazem uwarunkowaniem decydowania politycznego i wyzwaniem dla niego oraz wyznaczają jego ramy[5].

Fakt, że rządowe organy władzy wykonawczej, bez względu na to, jak silnie są osadzone w porządku konstytucyjnym i normatywnym, stanowią tylko jeden z podmiotów rządzenia, znajduje też pełne potwierdzenie w analizie stu ostatnich lat działania rządów i przebiegu rządzenia w Polsce. Widać to zwłaszcza w obszarze tworzenia polityki. Wśród uwarunkowań wyznaczających praktyczne granice udziału rządu w rządzeniu można wskazać m.in.: silną pozycję niektórych polityków (np. Józefa Piłsudskiego, charyzmatycznego przywódcy II RP); rozwiązania sytuujące systemowo ośrodki władzy poza rządem, w PRL – w kierownictwie partii rządzącej, a w dużej mierze wręcz poza granicami państwa polskiego; sytuacyjne układy wynikające z rozdrobnienia sceny politycznej, które uzależnia rządzenie od doraźnie kształtowanych koalicji parlamentarnych, co miało miejsce w pierwszych latach po zmianie ustrojowej 1989 r.; patologiczne w swej istocie przeniesienie ośrodka

[5] Szerzej zob.: G. Rydlewski, *Polska polityczna 2012/2013. Sfera publiczna jako środowisko decydowania politycznego*, Warszawa 2014; J. Garlicki, A. Noga-Bogomilski, *Kultura polityczna w społeczeństwie demokratycznym*, Warszawa 2004.

dyspozycji politycznej do nieponoszącego odpowiedzialności konstytucyjnej kierownictwa struktury politycznej dominującej w parlamencie, co ma miejsce po 2015 r.; systemowe następstwa takich procesów, jak globalizacja, integracja ponadnarodowa, informatyzacja i cyfryzacja, decentralizacja i dekoncentracja wewnątrzpaństwowa.

1.5. Rządzenie jako rzeczywistość wyobrażona

Wielokryterialność wartościowania rządzenia • Kluczowe znaczenie w ocenie rządzenia przyjętego systemu wartości i interesów • Rola w wartościowaniu rządzenia narracji ideowych i doktrynalnych • Uniwersalny i ponadczasowy charakter sporu w sprawie modelu rządzenia • Przenikanie mechanizmów transakcji handlowych do polityki i rządzenia

Rządzenie zawsze podlega wielokryterialnemu ocenianiu. Jest analizowane w kontekście aksjologicznym, prawnym, społecznym, politycznym, ekonomicznym, prakseologicznym. Sytuuje się je na tle przyjętych w trybie umownym zobowiązań oraz zasad komunikacji społecznej. Obok wymiaru użyteczności ma zawsze swój wymiar psychologiczny[6], a także socjologiczny – wyznaczony przez prawidłowości działania ludzi w grupie społecznej.

Rządzenie w swojej istocie jest porządkiem wyobrażonym i tym samym jest oceniane przy uwzględnieniu przyjętego systemu wartości i interesów[7]. Jak już wskazywałem, rządzenie zawsze stanowi wyzwanie intelektualne, legislacyjno-organizacyjne, polityczne, finansowe, świadomościowe i komunikacyjne. Ma określoną tożsamość ustrojową, normatywną, społeczną, polityczną, administracyjną i prakseologiczną. Jest złożonym procesem pozyskiwania informacji i zarządzania nią, budowania i realizowania programów, planów i harmonogramów. W ramach rządzenia trwa walka o zachowanie integralności polityki w sytuacji napięć oraz osiągnięcie synergii systemowej i są podejmowane działania zmierzające do optymalnej implementacji decyzji, skutecznej ewaluacji i korekty oraz efektywnej komunikacji społecznej.

---

6 Zob. szerzej: D. Sears, R. Jervis, L. Huddy (red.), *Psychologia polityczna*, Kraków 2014; K. Skarżyńska, *Człowiek a polityka. Zarys psychologii politycznej*, Warszawa 2005.

7 Jak zauważa Yuval Noah Harari, w przypadku „porządku wyobrażonego" wierzymy w jakiś porządek „nie dlatego, że jest obiektywnie prawdziwy, ale dlatego, że wierzenie weń umożliwia nam owocną współpracę i budowanie lepszego społeczeństwa", on sam zaś jest zakorzeniony w świecie materialnym, kształtuje nasze pragnienia i jest intersubiektywny – „istnieje w obrębie sieci komunikacji łączącej subiektywną świadomość wielu jednostek", zob. *Sapiens. Od zwierząt…*, s. 137.

Na opinie o rządzeniu wpływają nie tylko związane z nim fakty. Zasadnicze znaczenie mają stosowane w procesie wartościowania przesłanki ideowe i doktrynalne, które określają standardy działania oraz oczekiwania na ich skutki. Te oczekiwania zaś podlegają istotnym zmianom. W efekcie takie pojęcia, jak dobre rządzenie czy model optymalny rządzenia są ściśle powiązane z dynamiką tych zmian. W perspektywie historycznej nie można więc mówić o jednym idealnym modelu rządzenia. Model ten inaczej kształtuje się na różnym podłożu ideowym, a więc przyjmuje odmienną postać w przypadku autorytaryzmu, faszyzmu, komunizmu czy liberalizmu.

Nasze doświadczenia historyczne i polityczne z ostatniego stulecia wyraźnie pokazują, że także w Polsce proces zmian w rządzeniu oraz modele dobrego rządzenia były powiązane ze zmieniającymi się dominującymi koncepcjami ideowo-doktrynalnymi. Na rządzenie w Polsce kolejno wpływały w tym stuleciu następujące koncepcje: silnego parlamentu, silnego państwa, silnej władzy wykonawczej, jedności narodowej (wobec wyzwań, przed jakimi stanął naród w obliczu okupacji i wojny), walki klasowej (w tym – zgodnie z tezą Stalina – zaostrzającej się walki klasowej), rozwiniętego społeczeństwa socjalistycznego, państwa liberalnego, solidarności społecznej. Można tu wskazać kilka opozycyjnych wobec siebie modeli doktrynalnych: koncepcji głoszącej wszechobecność państwa konkurującej z koncepcją pomocniczości i subsydiarności państwa; projektu zakładającego istnienie silnego państwa narodowego przeciwstawnego wizji państwa powoli „rozpływającego się" we wspólnej przestrzeni europejskiej; doktryny państwa inspirowanego religijnie (w skrajnej postaci – państwa wyznaniowego) zderzającej się z koncepcją państwa świeckiego (czy wręcz ateistycznego). Warto też zauważyć, że w toku kształtowania się ideowego zaplecza władzy powtarza się pewien schemat. Otóż po okresie umacniania się jakiejś koncepcji doktrynalnej, gdy jej zwolennicy są już przekonani, że należy do nich nie tylko teraźniejszość, ale i przyszłość, następuje najczęściej ofensywa przeciwników tej koncepcji i dochodzi do politycznej „zmiany warty". Można to zdroworozsądkowo podsumować stwierdzeniem, że nic nie trwa wiecznie, nawet najbardziej butna władza przemija…

Spór o model rządzenia ma charakter uniwersalny i ponadczasowy. Model rządzenia był zawsze i będzie także w przyszłości przedmiotem polemik i kontrowersji (a także konfliktów) stymulowanych przez dominujące narracje ideologiczne i doktrynalne oraz silnie związanych z aktualnym stanem społeczeństwa. W ujęciu historycznym spór o model rządzenia był, prędzej czy później, rozstrzygany przez wzrost siły określonej narracji ideologicznej i doktrynalnej wyznaczającej środowisko rządzenia. Jak wyżej wspomniałem, kres, a przynajmniej zauważalny regres danej narracji, najbardziej w pewnym okresie wpływowej, zwykle nadchodził wówczas, gdy jej zwolennicy byli już całkowicie przekonani, że ich projekt jest bezalternatywny, że – krótko

mówiąc – nie mają z kim przegrać. W tej sytuacji pojawiała się w przestrzeni politycznej narracja konkurencyjna, wypracowywana i „dojrzewająca" od dłuższego czasu, a jeszcze przed publiczną inauguracją poddawana próbie wdrożenia, instalowania w świadomości społecznej. Projekt ten uzyskiwał wsparcie ze strony ludzi, którzy nie byli, a przynajmniej nie czuli się beneficjentami dotychczasowego modelu rządzenia.

Współcześnie widać wyraźnie – także w Polsce – przejawy kryzysu narracji liberalnej, a w istocie neoliberalnej. Zasady pomocniczości i subsydiarności są wypierane przez założenia doktryny wszechobecności i omnipotencji państwa. Nadaktywność państwa w różnych sferach (administracyjnej, gospodarczej, polityki kulturalnej etc.) świadczy o tym, że centralizacja jest z punktu widzenia rządzących bardziej atrakcyjna niż decentralizacja i dekoncentracja terytorialna. Kształtuje się system wartości, w którym sprawiedliwość okazuje się ważniejsza od praworządności, a koncepcji wzmacniania wspólnotowości ponadnarodowej i ponadpaństwowej przeciwstawiane są projekty eksponujące konieczność pielęgnowania tożsamości narodowej i państwowej.

Obecnie w Polsce nasila się chaos prawny, społeczeństwo jest głęboko i – jak się zdaje – trwale podzielone, wykazuje cechy anomii. Trzeba jednak pamiętać, że tego rodzaju zjawiska występują także poza naszym krajem. Mimo że wielu ludzi zdaje sobie sprawę z powagi sytuacji, nikt na razie nie wskazał skutecznego remedium. Nie widać na horyzoncie nowej całościowej narracji ideologicznej czy doktrynalnej, która byłaby ukierunkowana na integrowanie potrzeb teraźniejszości i przyszłości, a przy tym pozwalała ludziom i społecznościom zachować poczucie bezpieczeństwa w szybko zmieniającym się świecie. Indywidualną i zbiorową reakcją na niepewność, rozchwianie rzeczywistości, załamanie się ładu aksjonormatywnego są negacja, protest, gniew. Można już mówić o gniewie jako zjawisku globalnym[8]. Agresja wypiera deliberację. W tej sytuacji inicjatywę przejmują w niektórych państwach populiści, zwolennicy różnych koncepcji zachowawczo-zaściankowych żywiących się sentymentami narodowymi o zabarwieniu nacjonalistycznym. Lansowane są tezy o nieuchronności utrzymywania się w świecie różnic cywilizacyjnych, głoszące konieczność bezwarunkowej obrony narodowej i religijnej tożsamości danego państwa. Nie wydaje się, aby to właśnie do koncepcji zachowawczo-zaściankowych miała należeć przyszłość. W dłuższej perspektywie nie da się ich bowiem pogodzić z nieodwracalnymi następstwami globalizacji oraz integracji ponadpaństwowej i ponadnarodowej. A jednak to właśnie hasła obrony przed innymi mogą w połączeniu z populistycznym ukierunkowaniem polityki wyznaczać bieg zdarzeń w krótko- czy nawet średnioterminowej perspekty-

[8] Zob. P. Sloterdijk, *Czas i gniew*, Warszawa 2011. Niemiecki filozof posługuje się określeniem „banki gniewu".

wie. Bezbłędnie trafiają one bowiem do ludzi zawiedzionych, znajdujących się w kłopotach, niezadowolonych ze swojej sytuacji, przekonanych, że świat jest dla nich niesprawiedliwy. Tacy ludzie zdecydowanie przeważają liczebnie, co w systemach demokratycznych może skutkować, a w istocie już skutkuje, sukcesami wyborczymi ugrupowań populistycznych[9].

Współczesny model demokracji sprawia, że do polityki przenikają mechanizmy transakcji handlowych. Rządzenie zaczyna być oceniane w sposób właściwy wartościowaniu produktów i usług. W staraniach o uzyskanie większościowego poparcia dla określonych wyborów dokonywanych w rządzeniu wykorzystywane są techniki marketingu. Raz jeszcze potwierdza się teza Tocqueville'a, że większość stanowi w równej mierze siłę i problem demokracji[10].

Proces zmian modelowych w rządzeniu będzie trwał. Jak postaram się wykazać w tej książce, w jego dalszym biegu istotne znaczenie będą miały następstwa trwającej już ekspansji władzy komunikacji, cywilizacji cyfrowej i sztucznej inteligencji.

[9] Szerzej na ten temat: G. Rydlewski, *Coś więcej niż spór o model rządzenia. Kilka kwestii do przemyślenia nie tylko przez politologów*, Warszawa 2017.

[10] A. de Tocqueville, *O demokracji w Ameryce*, Warszawa 1976, s. 181 i nast.

Rozdział drugi

Perspektywa jakościowych zmian w rządzeniu u progu trzeciej dekady XXI wieku

2.1. Długi katalog strategicznych przesłanek nieuchronnych zmian w rządzeniu

Wielość strategicznych uwarunkowań zmian jakościowych w rządzeniu • Wzajemne przenikanie się istotnych uwarunkowań rządzenia

Jeśli chodzi o sprawy rządzenia, znajdujemy się obecnie w niestabilnej sytuacji, zawieszeni między coraz bardziej doskwierającą nam teraźniejszością (jej charakter dobrze oddaje określenie „skrzecząca rzeczywistość") i niosącą nieuchronnie jakościowe zmiany przyszłością. W tej dziedzinie kluczowego znaczenia nabiera zdolność dostrzeżenia pojawiających się wyzwań – oznaczających nowe możliwości działania i zarazem kreujących systemowe zagrożenia. Jest to ważne właśnie teraz, kiedy w otoczeniu polityki i decydowania politycznego zachodzą szybkie i wielopłaszczyznowe zmiany. Czynniki, które składają się na te zmiany, mogą odgrywać rolę zasadniczych, wręcz strategicznych, uwarunkowań zmian w rządzeniu. Pozostają one ze sobą w stosunkach współzależności, mają zróżnicowaną dynamikę i są obarczone licznymi niewiadomymi.

U progu trzeciej dekady XXI wieku można wskazywać wiele strategicznych uwarunkowań zmian jakościowych w rządzeniu. Od dłuższego czasu najważniejszymi z nich są: demokratyzacja, globalizacja, integracja ponadpaństwowa, informatyzacja i sieciowość oraz ekspansja algorytmów i sztucznej inteligencji, mediatyzacja i tabloidyzacja sfery polityki, nasilanie się globalnych zagrożeń oraz postępująca profesjonalizacja działań i wymagań w sprawach publicznych. Pandemia, która opanowała świat w 2020 r., z całą mocą przypomniała, że ludzie, państwa i podmioty międzynarodowe muszą się liczyć z okolicznościami, które nie poddają się ich władzy.

Biorąc pod uwagę wymiar przedmiotowy, należy stwierdzić, że wśród strategicznych przesłanek zmian w rządzeniu wzrasta znaczenie kilku równolegle oddziaływających zjawisk i procesów. Coraz wyraźniej rysują się na horyzoncie egzystencjalne zagrożenia związane z możliwymi katastrofami ekologicznymi, na skutek zmian klimatycznych i degradacji środowiska naturalnego. Szybko następują przekształcenia cywilizacyjne i kulturowe w świecie. Dynamizuje się sytuacja geopolityczna na podłożu walki między państwami o zajęcie dominującej pozycji w świecie po rozpadzie systemu bipolarnego, złożonego z dwóch przeciwstawnych bloków ideologicznych, politycznych i militarnych. Nasilają się napięcia między państwami narodowymi a strukturami międzypaństwowymi i ponadnarodowymi. Narastają problemy demograficzne związane z gwałtownym starzeniem się ludności w państwach rozwiniętych. Wielorakie skutki – polityczne, społeczne, kulturowe – niesie za sobą niekontrolowana migracja dużych grup ludności między strefami współczesnego świata odmiennymi kulturowo i religijnie. Zachodzą istotne zmiany na rynku pracy. Kształtuje się nowa architektura społecznych podziałów i pojawiają się nowe obszary wykluczenia społecznego. Dały o sobie znać zagrożenia epidemiczne, które w warunkach globalizacji zablokowały lub znacznie utrudniły tradycyjne metody kontaktowania się ludzi oraz prowadzenia przez nich działalności, także w sprawach bezpośrednio związanych z polityką i rządzeniem.

2.2. Ekspansja władzy komunikacji, cywilizacji cyfrowej i sztucznej inteligencji jako zasadnicza przesłanka zmian w rządzeniu

Czynniki składowe nowego oblicza rzeczywistości: postęp naukowo-techniczny, technologiczna eksplozja informacyjna oraz cywilizacja cyfrowa i sztuczna inteligencja
- *Egzystencjalny wymiar wyzwań związanych z nowymi, inteligentnymi technologiami*
- *Umacnianie się podmiotowości politycznej globalnych firm technologicznych i relacji zindywidualizowanej komunikacji masowej*

Wśród okoliczności stymulujących przekształcenia w rządzeniu na czoło wysuwa się gwałtowne przyspieszenie postępu naukowo-technicznego i zmiany związane z eksplozją informacji w ramach cywilizacji internetowej oraz z perspektywą nadejścia epoki dominacji cyfrowej komunikacji, sztucznej inteligencji i algorytmów. Decyduje o tym nie tylko siła tych uwarunkowań, ale i fakt, że przenikają one do wszystkich dziedzin życia i pracy ludzi oraz w zasadniczy sposób modyfikują sytuację i mechanizmy w bardzo różnych obszarach ludzkiej aktywności.

Przyszłość rządzenia jest nieuchronnie związana z ekspansją władzy komunikacji, cywilizacji cyfrowej i sztucznej inteligencji. Procesy te już dziś wykraczają zdecydowanie poza sferę rozwiązań technologicznych, stają się problemem cywilizacyjnym, społecznym, ekonomicznym i politycznym. Można na nie spojrzeć zarówno z punktu widzenia oferowanych nowych możliwości, jak i stwarzanych zagrożeń. Obecnie to w nich dokonują się najszybsze zmiany, w ramach których pojawiają się nowe obszary konkurencji i konfrontacji między państwami, a także między ugrupowaniami politycznymi.

Rozpoznanie związków pomiędzy zjawiskami należącymi do sfery cywilizacji cyfrowej i sztucznej inteligencji a polityką i rządzeniem jest egzystencjalnym wyzwaniem. Rewizji ulegają bowiem tradycyjne relacje podmiotowe, przedmiotowe i funkcjonalne władzy. Wielkie globalne firmy technologiczne zyskują podmiotowość polityczną. Komunikacja społeczna zaczyna wywierać ogromny wpływ na życie ludzi – zarówno w makroskali, jak i w perspektywie indywidualnej. Z uwagi na swoją bezprecedensowość, te uwarunkowania wymagają szczególnej uwagi badawczej.

To właśnie przekształcenia związane z nowymi technologiami pozyskiwania, gromadzenia, przechowywania, przetwarzania, opracowywania oraz przesyłania informacji i danych oraz z nowymi możliwościami wykorzystywania w funkcjonowaniu państw, struktur niepaństwowych oraz poszczególnych ludzi narzędzi elektronicznych stanowią w tej książce główną przesłankę przewidywanego kierunku zmian w rządzeniu.

W swych rozważaniach opieram się na założeniu, że zmiany w obszarze technologii informacyjnych i komunikacyjnych oraz rozwój produktów sztucznej inteligencji będą modyfikowały warunki rządzenia w stopniu wymuszającym jakościowe przekształcenia w samych mechanizmach rządzenia, a w efekcie staną się one w dłuższej perspektywie przesłanką kształtowania się nowych rozwiązań modelowych w zakresie uzyskiwania i sprawowania władzy w przestrzeni publicznej.

2.3. Wstęp do strategicznej prognozy zmian w rządzeniu

Specyfika perspektywy krótko-, średnio- i długoterminowej • Przenikanie się świata online i offline • Nieuchronność włączania w najbliższych latach inteligentnych technologii do działań decyzyjnych w polityce i rządzeniu • Znaczne prawdopodobieństwo zmian modelowych w rządzeniu pod wpływem upowszechniania się inteligentnych technologii cyfrowych i mechanizmów decydowania maszynowego • Duże prawdopodobieństwo pojawienia się w rządzeniu w perspektywie długookresowej problemu przebudowy relacji między ludźmi i wytworzonymi przez nich, autonomizującymi się narzędziami technologii cyfrowej

W rozważaniach o przyszłości rządzenia, tak jak we wszystkich prognozach społecznych i politycznych, największą wartość mają ujęcia o charakterze strategicznym, łączące aspekt poznawczy z przygotowaniem do nowej, uznanej za prawdopodobną sytuacji, a także – co wydaje się bardziej istotne – z tworzeniem podstaw do kształtowania tej przyszłości[1]. W takim ujęciu niezbędne jest zróżnicowane potraktowanie perspektywy krótko-, średnio- i długoterminowej. O tym, co może się stać w ramach każdej z nich, można bowiem mówić z różnym stopniem pewności czy prawdopodobieństwa.

Kreśląc obraz zmian w przestrzeni społecznej w bliskiej perspektywie czasowej, można wskazywać z dużym prawdopodobieństwem określone stany rzeczy, których pojawienia należy się spodziewać. W odniesieniu do nieco dalszej przyszłości można przewidywać w sposób odpowiedzialny jedynie główne tendencje. Prognozując sytuację jeszcze bardziej oddaloną w czasie, trzeba się skoncentrować raczej już tylko na problemach, które mogą wystąpić, oraz zarysować alternatywne scenariusze. Pamiętając o tych okolicznościach, które wyznaczają ramy prognozowania społecznego, przedstawiam poniżej swoją projekcję zmian w rządzeniu i decydowaniu politycznym powiązanych z umacnianiem się władzy komunikacji i rozwojem inteligentnych technologii. Z wielu dostępnych narzędzi badawczych wybieram metodę analizy systemowej, która – jak się wydaje – jest w tym przypadku bardziej przydatna niż inne procedury badawcze[2]. Do poszczególnych elementów tej projekcji, mającej charakter ogólnego i wstępnego zarysu, wracam w dalszych rozdziałach książki. Są to hipotezy, które próbuję zweryfikować w świetle zebranego materiału empirycznego. Na tej podstawie, w zakończeniu książki wskazuję, które z tych hipotez zasługują na stanowcze potwierdzenie, które zaś pozwalają co najwyżej kreślić scenariusze alternatywne.

Współczesna sytuacja w rządzeniu jest wyznaczona przede wszystkim przez zjawiska i procesy związane ze sporami o granice swobody decyzyjnej państw narodowych i podmiotów międzynarodowych, wybór modelu państwa

---

1 W takim rozumieniu prognozowanie jest traktowane jako procedura prowadząca do oddziaływania na proces zmian, a w szczególności do wzmacniania szans scenariuszy uznanych za optymalne. Zob.: T. Bodio, A. Chodubski, *O prognostyce w politologii*, „Studia Politologiczne" 2004, t. 8; A. Karpiński, *Co trzeba wiedzieć o studiach nad przyszłością?*, Warszawa 2009; B. Sajduk, *Czy w nauce o stosunkach międzynarodowych możliwe jest efektywne prognozowanie?*, https://www.omp.org.pl/artykul.php?artykul=274.

2 Na temat zróżnicowanych sposobów podejścia oraz metod projekcji przyszłości w naukach politycznych zob. A. Chodubski, *Prognostyka jako wyzwanie metodologiczne w badaniu stosunków międzynarodowych*, Annales Universitatis Mariae Curie-Skłodowska, Lublin 2009, sectio K, vol. XVI, 2, s. 41 i nast. Zob. też: H. Świeboda (red.), *Prognozowanie w naukach społecznych. Wymiar narodowy i międzynarodowy*, Warszawa 2018; M. Sułek, *Prognozowanie i symulacja międzynarodowa*, Warszawa 2010; A. Gorgosz, *Perspektywa prognostyczna w polityce publicznej. Metody umożliwiające prognozowanie – ich rola w procesie formułowania polityk publicznych*, „Zarządzanie Publiczne" 2014, nr 1 (25), s. 3 i nast.

liberalnego bądź konserwatywnego oraz relacje między regulacjami hierarchiczno-administracyjnymi i partycypacyjno-sieciowymi. Tym sporom towarzyszy stopniowe umacnianie się w rządzeniu władzy komunikacji elektronicznej[3] i rozwój inteligentnych technologii cyfrowych. Te procesy nie stanowią już tylko otoczki rządzenia, lecz przenikają do samego jego wnętrza.

W kształtującym się obecnie społeczeństwie sieciowym[4] zindywidualizowane kontakty masowe odbywają się głównie za pomocą narzędzi elektronicznych. Internet obejmuje i zagarnia coraz więcej zjawisk mających zasadnicze znaczenie dla życia ludzi, funkcjonowania społeczeństw, rozwoju wszystkich dziedzin ludzkiej aktywności oraz dla działalności organizacji i struktur instytucjonalnych. Na świadomość ludzi w istotnej – i rosnącej – mierze wpływają media społecznościowe, zaś światy online i offline zaczynają się wzajemnie przenikać.

Powstał i powiększa się globalny zbiór danych elektronicznych. Informacje w nim zgromadzone nabierają znaczenia władczego, a dostęp do nich staje się przedmiotem zażartej konkurencji[5]. Podmioty uczestniczące w tej walce konkurencyjnej nie zawsze posługują się uczciwymi metodami, a nieraz wkraczają na drogę przestępczą.

Rozpoczął się jakościowo nowy etap rozwoju infrastruktury telekomunikacji, sztucznej inteligencji[6] oraz internetu rzeczy i internetu ciała. Inteligentne technologie zyskują wymiar polityczny. Są narzędziem kształtowania porządku geopolitycznego na świecie, w znacznym stopniu współdecydują o pozycji państw na arenie międzynarodowej, zaczynają odgrywać ważną rolę w działaniach ofensywnych i obronnych poszczególnych państw.

Cyberprzestrzeń jest obszarem, w którym instaluje się polityka rozumiana jako sfera działań związanych ze zdobyciem i utrzymaniem władzy w przestrzeni publicznej, realizacją polityk publicznych oraz kształtowaniem systemu artykulacji i agregacji interesów politycznych. Nie wydaje się przesadną opinia, że już w dzisiejszych czasach „Polityka przeniknęła do cyberprzestrzeni, a cyberprzestrzeń zaczyna pełnić funkcję coraz istotniejszej areny dla procesów politycznych" i staje się „równoprawnym polem rywalizacji o władzę"[7].

---

3 Zob. M. Castells, *Władza komunikacji*, Warszawa 2013.

4 Zob.: M. Castells, *Społeczeństwo sieci*, Warszawa 2007; D. Barney, *Społeczeństwo sieci*, Warszawa 2008.

5 Zob. W. Krztoń, *Walka o informację w cyberprzestrzeni w XXI wieku*, Warszawa 2017.

6 Zob.: J. Kaplan, *Sztuczna inteligencja. Co każdy powinien wiedzieć*, Warszawa 2019; M.A. Boden, *Sztuczna inteligencja. Jej natura i przyszłość*, Łódź 2020; A. Chłopecki, *Sztuczna inteligencja. Szkice prawnicze i futurologiczne*, Warszawa 2018; A. Przegalińska, P. Oskanowicz, *Sztuczna Inteligencja. Nieludzka, arcyludzka*, Kraków 2020.

7 M. Lakomy, L. Porębski, N. Szybut, *Polityka 2.0. Aktorzy polityczni w świecie nowych technologii. Dyskurs politologiczny*, Kraków 2014, s. 10–11. Zob. też: L. Porębski, *Elektroniczne oblicze polityki. Demokracja, państwo, instytucje polityczne w okresie rewolucji informacyjnej*, Kraków

Z obserwacji i analizy tendencji występujących na współczesnej scenie politycznej płynie wniosek, że nowe cyfrowe rozwiązania technologiczne staną się jednym z podstawowych narzędzi wykorzystywanych we wszystkich aspektach polityki. W coraz większym stopniu będą wyznaczać sposoby walki o zdobycie i utrzymanie władzy w przestrzeni publicznej, a także metody prowadzenia polityk publicznych oraz artykulacji i agregacji interesów politycznych. Aktorzy polityczni i instytucjonalni aktywni w rządzeniu będą w ciągu najbliższych kilkudziesięciu lat sięgać po środki i metody działania pochodzące ze świata nowych technologii. Same te technologie będą się stawać przedmiotem działań decyzyjnych podejmowanych w trakcie decydowania politycznego i rządzenia.

W dziedzinie bezpieczeństwa międzynarodowego i wewnętrznego wdrażanie technologii cyfrowych będzie jednym z głównych kierunków aktywności. Bezpieczeństwo polityczne, zwłaszcza rozumiane jako zespół procesów informacyjno-decyzyjnych[8] dotyczących polityki i – szerzej – całej domeny publicznej, zostanie silnie zintegrowane z bezpieczeństwem informacyjnym i informatycznym[9].

Kształt rządzenia w ujęciu globalnym oraz w poszczególnych państwach i grupach państw będzie jeszcze długo wyznaczany przede wszystkim przez spór między stronnikami liberalizmu a zwolennikami zachowawczych koncepcji eksponujących siłę władzy publicznej jako atrybut państwa. Politycy akcentujący ideę wolności, wartość wspólnot ponadpaństwowych i ponadnarodowych oraz zasady pomocniczości i subsydiarności będą się ścierać ze zwolennikami koncepcji mówiących o potrzebie zagwarantowania tradycyjnie rozumianej siły państwa, fundamentalnym znaczeniu tożsamości i interesów narodowych oraz wyższości sprawiedliwości nad innymi wartościami. Na ten spór będą się nakładać kontrowersje powstałe wokół przekształceń geopolitycznych oraz walki między największymi państwami i grupami państw o dominację w świecie. Zakres przedmiotowy sporów politycznych będzie się rozszerzać, obejmując konsekwencje zróżnicowanych interesów i stanowisk wobec wskazanych wyżej strategicznych wyzwań związanych w szczególności z ochroną środowiska naturalnego i nieuporządkowaną migracją.

Nie ma wątpliwości co do tego, że w polityce będzie się nasilać rywalizacja o dostęp do globalnego zasobu danych zawierającego różnego rodzaju informacje – m.in. o faktach, zdarzeniach i podmiotach, które można wykorzy-

2001; M. Majorek, S. Olszyk, M. Winiarska-Brodowska, *Cyberpolityka. Internet jako przestrzeń aktywności politycznej*, Warszawa 2018; A. Rothert, *Cybernetyczny porządek polityczny*, Warszawa 2005; D. Mider, *Partycypacja polityczna w Internecie. Studium politologiczne*, Warszawa 2008.

[8] S. Zalewski, *Bezpieczeństwo polityczne państwa. Studium funkcjonalności instytucji*, Siedlce 2010, s. 30.

[9] Zob.: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018; M. Kubiak, S. Topolewski (red.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce 2016; D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

stywać w komunikacji społecznej, przetwarzać i interpretować, a wszystko to w imię osiągania założonych celów[10]. Zasób ten staje się istotnym narzędziem w walce o władzę i w jej sprawowaniu. Zwolennicy określonych koncepcji i programów politycznych będą skwapliwie korzystać z możliwości działania pojawiających się w cyberprzestrzeni rozumianej jako synteza elementów technicznych, technologicznych i – co bardzo ważne w kontekście rozważań politologicznych – społecznych[11]. Dążenie do zawładnięcia sferą komunikacji internetowej i zgromadzonym w tej przestrzeni globalnym zbiorem danych będzie przedmiotem konkurencji i sporów politycznych między mocarstwami światowymi[12].

W perspektywie najbliższych lat musi dojść do ostrego starcia między zwolennikami wyraźniejszej standaryzacji i regulacji cywilizacji cyfrowej a rzecznikami pozostawienia tej sfery rzeczywistości, traktowanej jako matecznik wolności i postępu, poza reglamentacją dokonywaną przez państwa i organizacje międzynarodowe. Przybiorą na sile działania ukierunkowane na zagwarantowanie prywatności w cyberprzestrzeni, zostaną podjęte próby dekoncentracji i demonopolizacji mediów społecznościowych.

W drugiej połowie XXI wieku z pewnością konieczne będzie dokonywanie zmian modelowych w rządzeniu wynikających z upowszechnienia się nowej generacji inteligentnych technologii cyfrowych i mechanizmów decydowania maszynowego. Należy się spodziewać wdrażania nowych rozwiązań systemowych w organizacji i działaniu państw, które będą dostosowane do kształtu społeczeństwa w coraz większym stopniu sieciowego i zinformatyzowanego[13]. Wiele wskazuje na to, że już w najbliższej perspektywie obecne mechanizmy rządzenia uzyskają nowe systemowe oprzyrządowanie technologiczne w przestrzeni elektronicznej.

Trudno powiedzieć, na jaką skalę i w jakim tempie współczesny model decydowania w sprawach organizacji domeny publicznej jest wypierany przez różnego rodzaju mechanizmy decydowania maszynowego wykorzystujące algorytmy, które – jak przewiduje Jan Kreft – „zastępować będą ludzi w przetwarzaniu i wyciąganiu wniosków oraz podejmowaniu decyzji, coraz częściej zarządzając ludzkimi zachowaniami i decydując o pozycji społecznej człowieka”[14]. Nie ulega natomiast wątpliwości, że osobowe i instytucjonalne

---

10 Zob. C. Banasiński (red.), *Cyberbezpieczeństwo…*, s. 21 i nast.

11 Tamże, s. 23 i nast.

12 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.

13 Zob.: M. Kowalczyk, *Cyfrowe Państwo. Uwarunkowania i perspektywy*, Warszawa 2019; P. Maj, *Internet i demokracja. Ewolucja systemu politycznego*, Rzeszów 2009; R. Grabowski (red.), *Wpływ internetu na ewolucję państwa i prawa*, Rzeszów 2008.

14 J. Kreft, *Władza algorytmów. U źródeł potęgi Google i Facebooka*, Kraków 2019, s. 33.

podmioty polityki i administracji stopniowo będą włączać narzędzia cyfrowe do procesów decyzyjnych i działań administracyjnych.

Z czasem praktycznego znaczenia nabiorą problemy demokracji elektronicznej, która jak dotychczas stanowi w dużej mierze jedynie przedmiot rozważań teoretycznych (kwestię tę omawiam w końcowych fragmentach książki). Praktycznego charakteru nabierze też spór o możliwości wyrażania przez obywateli stanowiska politycznego na odległość – w wyborach i referendach przeprowadzanych za pomocą narzędzi internetowych. Należy oczekiwać, że upowszechni się aktywność polityczna prowadzona z użyciem interaktywnych narzędzi serwisów społecznościowych i mikroblogów. Nowy wymiar zyska partycypacja polityczna w internecie. Tradycyjne partie i ugrupowania polityczne znajdą dopełnienie w postaci internetowych grup dyskusyjnych oraz wspólnot wartości i interesu. Obecny model demokracji przedstawicielskiej będzie miał coraz mniejsze szanse utrzymania się w zderzeniu z różnymi nowymi mechanizmami demokracji bezpośredniej, w ramach których – przy wykorzystaniu narzędzi internetowych – ludzie będą mogli rozstrzygać w czasie rzeczywistym o sprawach zastrzeżonych teraz dla organów przedstawicielskich[15].

W dłuższym horyzoncie czasowym – nie da się go dzisiaj w sposób odpowiedzialny wyznaczyć – realnie pojawi się w rządzeniu problem przebudowy relacji między ludźmi i wytworzonymi przez nich, autonomizującymi się narzędziami technologii cyfrowej. W perspektywie długoterminowej zapewne wyraźnie wzrośnie znaczenie wytworów technologii cyfrowej. Mają one zdolność uczenia się, podlegającą stałemu doskonaleniu, i potrafią już wykraczać poza zaprogramowany przez ludzi zakres aktywności. Może to w przyszłości prowadzić do ukształtowania się relacji konkurencji między ludźmi i urządzeniami cyfrowymi. Badacze zajmujący się omawianą tu problematyką są zgodni co do tego, że za jakiś czas narzędzia elektroniczne mogą się wymknąć spod kontroli. Podkreślają oni równocześnie, że nie można polegać na kreślonych z całkowitą pewnością scenariuszach przyszłości. Można co najwyżej zakładać, że polityczne gremia decyzyjne będą się musiały liczyć z wynikami pracy różnorodnych elektronicznych automatów decyzyjnych działających na podstawie algorytmów współtworzących rzeczywistość cyfrową. W jakimś sensie byłby to dalszy krok na drodze ograniczenia autonomii decyzji podejmowanych

[15] Na ten temat zob.: G. Browning, *Elektroniczna demokracja. Wybory w Internecie*, Warszawa 1997; L.K. Grossman, *Republika elektroniczna*, w: J. Szczupaczyński (red.), *Władza i społeczeństwo 2. Antologia tekstów z socjologii polityki*, Warszawa 1998; M. Marczewska-Rytko (red.), *Demokracja elektroniczna. Kontrowersje i dylematy*, Lublin 2013; M. Musiał-Karg (red.), *Demokracja w obliczu nowych mediów. Elektroniczna demokracja, wybory przez Internet, kampania w sieci*, Toruń 2013; K. Oświecimski, A. Pohl, M. Lakomy (red.), *NetoDEMOkracja: Web 2.0 w sferze publicznej*, Kraków 2016; R. Olszowski, *Elektroniczna Republika: udział obywateli w życiu publicznym za pośrednictwem narzędzi ICT*, Fundacja Instytut Aurea Libertas, 2018, https://aurealibertas.org/elektroniczna-republika; L. Porębski, *Lokalny wymiar elektronicznej demokracji*, Kraków 2012.

formalnie w gabinetach politycznych, które dzisiaj są silnie uzależnione od rozstrzygnięć podmiotów finansowych.

Uzależnienie decyzyjne polityków od wyników pracy maszyn cyfrowych to coś, co teraz większości z nas może się kojarzyć raczej z narracjami *science fiction*. Szczególnie wówczas, gdy – idąc dalej tym tokiem rozumowania – wkroczymy w rozważania nad perspektywą autonomizowania się wytworów człowieka, wyzwalania się ich spod jego władzy. Człowiek od zawsze, osiągając jakościowe postępy w nauce i technice, równolegle doskonalił zdolności panowania nad uzyskanymi w tym procesie produktami. Tak było, gdy kształtowały się kolejne środki komunikacji i łączności, w tym różne narzędzia dźwiękowej i wizyjnej komunikacji społecznej, nowe wersje rozwiązań komputerowych i sieć internetowa. Dziś trudno jednoznacznie odpowiedzieć na pytanie, czy zasada supremacji będzie dotyczyć także relacji między ludźmi a wytworzonymi przez nich i coraz bardziej inteligentnymi narzędziami elektronicznymi. Należy poważnie liczyć się z tym, że z upływem kolejnych dekad zakres kontroli człowieka nad nimi będzie się kurczyć. Stopniowo zacznie się zmniejszać rozziew między *political reality* a *political fiction*…

Ekspansja narzędzi informatycznych, które wchodzą na rynek pracy, wypierając ludzi na wielu stanowiskach, postawi – w gruncie rzeczy już stawia – przed rządzeniem (i rządzącymi) istotne wyzwanie. Pojawi się bowiem znaczna liczba ludzi zbędnych w nowych stosunkach pracy. Świat inteligentnych technologii będzie oczywiście potrzebował aktywności ludzi na różnych nowych stanowiskach. Jednak zagospodarowanie osób tracących zatrudnienie w związku z rozwojem robotyzacji może się okazać niemożliwe. Jest to niezwykle ważny problem społeczny o dalekosiężnych konsekwencjach politycznych, który powinien być poddany uważnej analizie już obecnie.

Sprawą otwartą jest odpowiedź na pytanie o to, kiedy rzeczywistość doskonalonych narzędzi komunikacji cyfrowej i robotyki wymusi ukształtowanie się nowego modelu demokracji. Bo to, że dojdzie do zmiany dotychczasowego modelu, jest bardziej niż prawdopodobne. Zapewne zmiana ta będzie przebiegała w atmosferze sporów i kontrowersji, być może także niepokojów społecznych. Nie ulega wątpliwości, że kluczowe znaczenie w procesie przenoszenia się polityki do cyberprzestrzeni oraz do świata urządzeń sztucznej inteligencji będzie miała świadomość ludzi. Przykładowo można wskazać, że sięganie po instrumenty demokracji bezpośredniej w sprawach mechanizmów demokracji parlamentarnej oraz kompetencji organów stanowiących samorządu terytorialnego nie tylko wymaga stworzenia odpowiednio zabezpieczonych procedur, lecz także jest uzależnione od powszechnego opanowania przez ludzi umiejętności współdecydowania o biegu spraw publicznych oraz od poziomu zainteresowania społecznego tą formą partycypacji w decydowaniu publicznym. Dotychczasowe doświadczenia w sferze aktywności obywatelskiej,

w tym również w Polsce, pokazują, że to właśnie deficyty w zakresie kultury politycznej społeczeństwa oraz postaw prodemokratycznych (w tym osobowości demokratycznej) jego członków mogą jeszcze przez długi okres stabilizować przedstawicielski model decydowania w sprawach publicznych, oznaczający mniejszą aktywność polityczną obywateli.

Rozdział trzeci

Zmiany modelu społeczeństwa jako przesłanka przeobrażeń w sferze rządzenia

3.1. Stan społeczeństwa jako główne uwarunkowanie rządzenia

Strategiczne uzależnienie rządzenia od przekształceń w jego otoczeniu • Społeczeństwo jako podstawowy element aktywnego otoczenia decydowania politycznego i rządzenia • Wzrost znaczenia politycznego informacji, komunikacji i narracji kształtujących nowy model społeczeństwa • Polityczna tożsamość administratorów narzędzi internetowej komunikacji społecznej

Jak sygnalizowałem w poprzednim rozdziale, rządzenie i jego otoczenie pozostają ze sobą w silnych wzajemnych związkach. Rządzenie odznacza się w tych relacjach dużą kreatywnością, narzucając otoczeniu pewne regulacje, standardy etc., ale przede wszystkim cechuje się reaktywnością, jako że jest wyczulone na zmiany w swoim otoczeniu i musi szukać odpowiedzi na pojawiające się w nim zasilenia, poparcia i żądania. Stan nieuporządkowania występujący w danym okresie w otoczeniu rządzenia, objawiający się chaosem, napięciami i konfliktami społecznymi, często o podłożu politycznym, przekłada się na jakość systemu rządzenia, który – w dłuższej perspektywie – traci zdolność do zachowania uporządkowanego wewnętrznie i efektywnego społecznie charakteru i musi ulegać zmianom.

Podstawowym elementem aktywnego otoczenia decydowania politycznego i rządzenia jest i pozostanie społeczeństwo. Wszystkie zmiany modelowe społeczeństwa tworzą tym samym przesłanki zmian w rządzeniu. Społeczeństwo, bez względu na stopień odzwierciedlenia tego faktu w rozwiązaniach ustrojowych i normatywnych oraz w praktyce politycznej, jest w każdych warunkach nie tylko środowiskiem rządzenia, ale i jego przedmiotem i podmiotem. Prawo i praktyka działania władz mogą ową podmiotowość społeczeństwa wzmacniać lub osłabiać, nie są jednak w stanie jej wyeliminować[1]. Dla procesów rządze-

[1] Na ten temat zob. G. Rydlewski, *Polska polityczna…* i zawarta tam obszerna literatura.

nia fundamentalne znaczenie ma w związku z tym historia i tradycja danego społeczeństwa, jego struktura, tożsamość aksjologiczna, narodowa i światopoglądowa, stopień i charakter zróżnicowania, kultura prawna i polityczna.

Rządzenie musi się zmierzyć we współczesnych czasach z zasadniczym wyzwaniem, jakim jest dokonujące się jakościowe przeformatowanie tradycyjnego modelu społeczeństwa. Zamiast panującej dotąd wspólnotowości mamy postępującą atomizację. Typ społeczeństwa, w którym panują relacje zdominowane przez różne układy stanowe i grupowe, ustępuje miejsca społeczeństwu jednostek, które starają się dokonywać wyborów na podstawie swoich ocen, wizji świata oraz interesów – osobistych i rodzinnych. Nie znaczy to oczywiście, że kategorię interesów grupowych należy już usunąć poza nawias rozważań. Nadal bowiem dają o sobie znać podziały grupowe, związane głównie z odmiennościami sytuacji tych ludzi, którzy są beneficjentami zachodzących zmian transformacyjnych, i tych, którzy są ofiarami tych zmian. W dalszym ciągu dość wyraźnie rysują się różnice między mieszkańcami wielkich miast i prowincji. Równocześnie jednak znacznie się zwiększa pole wyborów zachowań dostępnych ludziom. Podstawowe znaczenie ma w tym zakresie stan świadomości społecznej, sposób rozumienia przez ludzi świata i wartościowania występujących w tym świecie zjawisk i procesów oraz stosunek do zachodzących zmian. Na tym tle rośnie ranga informacji pozyskiwanych przez ludzi w ramach komunikacji społecznej[2].

Często upraszczana, lecz w dużej mierze słuszna, teza mówiąca, że to byt określa świadomość, ulega modyfikacji. Ludzie, którzy – obiektywnie rzecz ujmując – znajdują się w takiej samej lub zbliżonej sytuacji bytowej, zachowują się w zróżnicowany sposób. Wpływ na to mają przede wszystkim indywidualne predyspozycje psychologiczne i zdolności intelektualne. Jednak w coraz większym stopniu liczą się przyswojone wzorce postępowania i zebrane doświadczenia życiowe.

Brak jednej dominującej w przestrzeni publicznej narracji doktrynalnej, ogólny kryzys autorytetów oraz indywidualizacja punktów odniesienia w myśleniu ludzi stwarzają przestrzeń dla równoległego funkcjonowania wielu różnych, w tym również skrajnie osobistych narracji. Owe zróżnicowane sposoby widzenia świata stają się równouprawnione, i to nawet wówczas, gdy – bezstronnie patrząc – można je ulokować w obszarze „fałszywej świadomości" jako efekt mieszania faktów z opiniami. Jak już powiedziałem, poszczególne jednostki starają się dokonywać wyborów na podstawie swoich osobistych ocen, widząc w tym instrument kształtowania własnej tożsamości. Precyzyjnie rzecz ujmując, najczęściej chodzi tu o oceny, które ludzie uznali za swoje, a które

---

[2] Zob. A. Rogala-Lewicki, *Informacja jako autonomiczny czynnik wpływu w przestrzeni publicznej. Studium władztwa informacyjnego*, Częstochowa 2015.

w istocie przyjmują pod wpływem pojawiających się w otoczeniu informacji i przedstawianych tam punktów widzenia.

Dlatego tak wielką rolę odgrywa umiejętność pozyskiwania przez nadawców informacji zaufania szerokiego grona ludzi – adresatów rozpowszechnianych wiadomości i interpretacji. To jedna z głównych przesłanek siły oddziaływania mediów, które polega na ukierunkowywaniu uwagi społecznej, kształtowaniu opinii i poglądów, definiowaniu rzeczywistości, formowaniu przekonań obywateli o charakterze i legalności władzy. Możliwość szybkiego i powszechnego informowania[3] daje mediom masowym symboliczną władzę, która „przejawia się zdolnością narzucania sposobu widzenia świata (…) poprzez prezentowanie tematów w dyskusji politycznej oraz wykluczanie innych, ustalanie ich hierarchii, odgrywanie roli gatekeepera”[4].

3.2. Informacyjne społeczeństwo sieciowe jako jakościowo nowe środowisko rządzenia

Społeczeństwo informacyjne i powstawanie społeczeństwa sieciowego • Zmiany pozycji państwa pod wpływem kształtowania się nowego modelu społeczeństwa • Internet i media społecznościowe jako podstawowy sposób komunikacji między ludźmi • Układy sieciowe jako dominująca relacja społeczna • Telefony komórkowe jako osobiste centra aktywności milionów ludzi

Wśród strategicznych zmian społecznych stymulujących zmiany w rządzeniu na plan pierwszy coraz wyraźniej wysuwają się następstwa kształtowania się społeczeństwa informacyjnego[5]. Stopniowo wyłaniają się zarysy społeczeństwa sieciowego[6], postępuje budowa modelu społeczeństwa cyfrowego.

Pod wpływem internetu i mediów społecznościowych zmienia się w zasadniczy sposób społeczeństwo, którego stan – jak uważam – jest podstawowym

[3] T. Goban-Klas, *Komunikowanie i media masowe. Teorie prasy, radia, telewizji i Internetu*, Warszawa 1999, s. 117. Zob. też: M. Adamik-Szysiak (red.), *Media i polityka. Relacje i współzależności*, Lublin 2014; J. Adamowski (red.), *Demokracja a nowe środki komunikacji społecznej*, Warszawa 2004; M. Jeziński (red.), *Nowe media i polityka. Internet, demokracja, kampanie wyborcze*, Toruń 2008; M. Lakomy, *Demokracja 2.0. Interakcja polityczna w nowych mediach*, Kraków 2013.

[4] J. Kreft, *Władza algorytmów*…, s. 187.

[5] Zob.: T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne. Szanse, wyzwania i zagrożenia*, Kraków 1999; M. Witkowska, K. Cholawo-Sosnowska (red.), *Społeczeństwo informacyjne. Istota – rozwój – wyzwania*, Warszawa 2006; M. Nowina-Konopka, *Społeczeństwo informacyjne a teorie demokracji*, w: M. Witkowska, K. Cholawo-Sosnowska (red.), *Społeczeństwo informacyjne…*; W.M. Maziarz, *Społeczny wymiar społeczeństwa informacyjnego*, Szczecin 2020.

[6] Zob.: M. Castells, *Społeczeństwo sieci*; D. Barney, *Społeczeństwo sieci…*

uwarunkowaniem rządzenia, w szczególności zdecydowanie wzmacniają się relacje sieciowe. Kształtujące się społeczeństwo sieciowe funkcjonuje w warunkach wielowymiarowej globalizacji i stanowi jeden z jej istotnych elementów. Proces jego powstawania ma swój aspekt technologiczny, związany z tym, że społeczeństwo jako struktura społeczna „skupia się wokół sieci aktywowanych przez oparte na mikroelektronice, cyfrowo przetwarzane informacje i technologie komunikacyjne", zaś „sieci cyfrowe mają charakter globalny, cechuje je zarówno zdolność rekonfigurowania samych siebie – w sposób zaplanowany przez programistów – jak i przekraczania granic terytorialnych i instytucjonalnych poprzez skomunikowane sieci komputerowe"[7].

W społeczeństwie sieciowym zmienia się pozycja państwa. Zachowując swoją specyfikę polegającą na możliwości stosowania legalnego przymusu, jednocześnie państwa są już tylko jednymi z – pozostających w relacjach kooperacji lub rywalizacji – węzłów sieci informacyjnych, politycznych, ekonomicznych oraz instytucjonalnych. Muszą się wpisać w układ „globalnych, narodowych i lokalnych sieci działających w wielowymiarowej przestrzeni społecznych interakcji"[8]. W tym układzie sztywne (w dużej mierze zamknięte) relacje hierarchiczne i wytworzone w ich ramach stosunki wertykalne ulegają ograniczeniu przez elastyczne (w dużej mierze otwarte) relacje sieciowe i związane z nimi stosunki horyzontalne[9].

Owe relacje sieciowe mogą się kształtować w czasie rzeczywistym ponad podziałami wyznaczonymi przez granice państwowe, zaś ich forma i treść w istocie nie zależą już od woli władz państwowych. Ta zmiana społeczna dokonuje się właśnie za sprawą globalnego przepływu informacji, dzięki komunikacji społecznej odbywającej się z wykorzystaniem mediów interaktywnych, bez pośrednictwa instytucji państwowych. Stanowi ona ważne uwarunkowanie procesów decydowania politycznego i rządzenia.

Tak więc, internet i media społecznościowe stają się podstawowym sposobem komunikowania się ludzi między sobą w czasie rzeczywistym i bez pośrednictwa państwa, zaś układy sieciowe urastają do rangi głównej relacji społecznej. Komunikowanie się za pomocą internetu i mediów społecznościowych upowszechnia się w największym tempie w państwach rozwiniętych gospodarczo. Jednak pozostałe kraje nie będą zapewne długo pozostawać w tyle pod tym względem. Wyraźny wzrost w statystykach nastąpił w latach 2000–2020. Wyniósł on aż 1266%. Według szacunkowych danych, w III kwartale 2020 r. na świecie abonentami internetu było łącznie ponad 4,9 miliarda

---

7 M. Castells, *Władza komunikacji*, s. 36; M.K. Zwierżdżyński, M. Lakomy, K. Oświecimski, *Technopolityka w świecie nowych mediów*, Kraków 2015.

8 Tamże, s. 23.

9 Zob. E. Bendyk, *Antymatrix. Człowiek w labiryncie sieci*, Warszawa 2004.

osób (tj. ponad 63% ogółu ludności). W marcu 2020 r. najwięcej użytkowników internetu było w Azji, gdzie mieszkało 51,8% wszystkich osób na świecie posługujących się tym narzędziem komunikacji. Osoby te stanowiły 59,5% wszystkich mieszkańców tego kontynentu. Dane dla innych regionów świata wynosiły odpowiednio – w przypadku Afryki: 12,8% i 47,1%; Europy: 14,8% i 87,2%; Ameryki Północnej: 6,8% i 90,3%; Ameryki Łacińskiej (wraz z Karaibami): 9,5% i 71,5%; Bliskiego Wschodu: 3,7% i 70,8%; Oceanii i Australii: 0,6% i 63,2%[10].

Na 445,2 miliona mieszkańców Unii Europejskiej z internetu korzystało w czerwcu 2020 r. już ponad 397 milionów osób (tj. ponad 89% wszystkich mieszkańców). W marcu 2020 r. ponad 249,7 miliona osób było użytkownikami Facebooka. W licznych państwach członkowskich UE odsetek użytkowników internetu przekraczał 90% mieszkańców (w Danii było to 97,8%, w Luksemburgu – 96,3%, w Estonii – 96,2%, w Szwecji – 96%, na Litwie – 95,7%, w Holandii – 95,6%, w Niemczech – 94,4%, w Finlandii – 94,3%, w Belgii – 93,7%, we Francji – 92,6%, w Chorwacji – 92,3%, w Hiszpanii – 91,9%, we Włoszech – 90,6%, w Irlandii – 90,2%). Według tych samych statystyk w Polsce w czerwcu 2020 r. z internetu korzystało 78,6% mieszkańców[11].

Rośnie znaczenie interaktywnej komunikacji odbywającej się za pomocą telefonów komórkowych, które są sukcesywnie wyposażane w kolejne aplikacje i dla coraz większej liczby ludzi stają się podstawowym narzędziem kontaktowania się z otoczeniem, a nawet więcej – swego rodzaju osobistymi centrami aktywności. Według danych Międzynarodowego Związku Telekomunikacyjnego, w 2015 r. liczba aktywnych kart SIM, która wynosiła wówczas na świecie 8,1 miliarda, przekroczyła już o pół miliarda liczbę ludności. Około jednego miliarda ludzi nadal nie ma dostępu do energii elektrycznej, co oznacza, że w państwach rozwiniętych wiele osób używa kilku telefonów. W 2018 r. ponad 5,2 miliarda abonentów miało dostęp do internetu (z tej grupy 45% abonentów wchodziło na swoje konto na Facebooku co najmniej raz w miesiącu)[12].

---

[10] *Statystyka użytkowania internetu. Światowi użytkownicy internetu i statystyki dotyczące populacji w 2020 r.*, https://www.internetworldstats.com/stats.htm.

[11] *Korzystanie z Internetu w Unii Europejskiej*, https://www.internetworldstats.com/stats9.htm. Dane te nie uwzględniają już Wielkiej Brytanii.

[12] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

3.3. Wzrost władzy komunikacji oraz rozwój technologii cyfrowych jako przesłanka dalszych zmian społecznego otoczenia rządzenia

Nowy sposób komunikowania się jako przesłanka jakościowych zmian procesów poznawczych • Załamywanie się tradycji udzielania odpowiedzi na pytania dotyczące historii, teraźniejszości oraz przyszłości na drodze procesów myślowych i refleksji intelektualnej • Początki i rozwój praktyki wyszukiwania odpowiedzi w przestrzeni internetowej • Przenikanie kultury sieci do przestrzeni publicznej

W społeczeństwie sieciowym dynamicznej zmianie ulega tryb znajdowania przez ludzi odpowiedzi na nurtujące ich pytania. Przeobraża się treść oraz sposób językowego artykułowania tych pytań i wartościowania poszczególnych zagadnień. Przyjęty w społeczeństwie sieciowym sposób komunikowania się prowadzi do jakościowych zmian w zakresie procesów poznawczych i zachowań językowych. Jak pokazały przeprowadzone w Wielkiej Brytanii badania językoznawców z University of Leeds, w ramach życia jednego pokolenia odmieniło się podstawowe znaczenie niektórych terminów; tradycyjnie były one używane w wypowiedziach w odniesieniu do sił i zjawisk natury, a obecnie są przez młodych ludzi używane przede wszystkim do określenia pewnych zjawisk ze świata technologii elektronicznej komunikacji masowej. Dotyczy to w szczególności takich terminów, jak tweet, sieć, strumień, pole czy też chmura[13].

W kształtującym się porządku cywilizacji cyfrowej ludzie stają się tylko jednym z elementów systemu, którego nieodłącznymi częściami są sprzęt komputerowy, oprogramowanie i administratorzy serwisów oraz platform internetowych[14]. Po okresie wyznawania dość utopijnej wiary w neutralny charakter technologicznych i korporacyjnych aspektów tego systemu dziś już nie ma wątpliwości, że są to ogniwa wyznaczające w sposób aktywny i nieprzypadkowy granice poznawczych i komunikacyjnych działań ludzi, o czym piszę w dalszej części tej książki. Tu wypada tylko zauważyć, że układ stosunków wewnątrz tego systemu jest asymetryczny, gdyż człowiek (przyjmując rolę użytkownika systemu) zostaje w sposób arbitralny podporządkowany regułom

[13] https://www.theguardian.com/environment/2019/jul/31/tweet-web-cloud-technology-transforms-meaning-of-nature-words.

[14] A. Adamski, *Media w analogowym i cyfrowym świecie. Wpływ cyfrowej rewolucji na rekonfigurację komunikacji społecznej*, Warszawa 2012; M. Jeziński (red.), *Nowe media w systemie komunikowania: polityka*, Toruń 2011; P. Gawrysiak, *Cyfrowa rewolucja. Rozwój cywilizacji informacyjnej*, Warszawa 2008; J.M. Osipow, A.Z. Nowak (red.), *Rewolucja cyfrowa. Wyzwania, problemy, perspektywy rozwoju*, Warszawa 2019; B. Poulet, *Śmierć gazet i przyszłość informacji*, Wołowiec 2011; A. Roguski, *Zrozumieć social media*, Gliwice 2020.

wyznaczonym przez działających na zasadach biznesowych dysponentów sieci medialno-komunikacyjnych[15].

W wyniku sygnalizowanych tu procesów w świecie komunikacji społecznej następuje konfiguracja przestrzeni międzyludzkiej[16] i kształtuje się nowy model człowieka i relacji międzyludzkich. Przekłada się to w sposób nieunikniony na środowisko rządzenia i rzutuje na samą praktykę rządzenia. Przy omawianiu tej problematyki nie można pomijać kwestii zmian generacyjnych w społeczeństwie. W socjologii (także w innych naukach społecznych i w naukach humanistycznych) operuje się terminem „pokolenie" (generacja), oznaczającym zbiorowość ludzi w mniej więcej tym samym wieku, których łączą doświadczenia i perspektywy życiowe, czasami także tzw. przeżycia pokoleniowe. Wyodrębnia się kolejne pokolenia, uwzględniając uwarunkowania społeczne, polityczne i ekonomiczne, które decydują o ich specyfice. W odniesieniu do ostatnich kilkudziesięciu lat w Polsce można wyróżnić pokolenie baby-boomers (ludzie urodzeni przed 1965 r.), pokolenie „X" (dorastające już w czasach zmian ustrojowych i technologicznych) oraz pokolenie oznaczane literą „Y" (tzw. pokolenie millenialsów), będące świadkiem rozwoju i wprawnym użytkownikiem nowych technik komunikacyjnych. Dla kształtowania się nowego modelu społeczeństwa zasadnicze znaczenie ma coraz silniejsza pozycja zajmowana przez osoby urodzone po 1990 r. To pokolenie, oznaczane literą „Z", a zamiennie literą „C" (od angielskiego słowa *connected* – podłączony do sieci), skupia ludzi, którzy nie znają już z autopsji świata innego niż ten, w którym interaktywna komunikacja społeczna odbywa się w ramach łączy sieciowych, za pomocą komputerów i internetu. Właśnie korzystając z tych narzędzi i technologii oraz informacji i kontaktów z nich pochodzących, członkowie pokolenia „C" poszukują odpowiedzi na większość nurtujących ich pytań, zawierają i utrzymują znajomości, rozwiązują setki codziennych problemów, dokonują swoich życiowych wyborów i kształtują styl życia. W odróżnieniu od reprezentantów pokolenia „Y" (millenialsów), bez większych trudności odróżniających rzeczywistość realną i wirtualną, członkowie pokolenia „C" w niebezpieczny sposób zacierają granicę między światem offline i online[17].

---

[15] Na temat zakresu i mechanizmów asymetrii zależności w środowisku mediów zob. J. Kreft, *Władza algorytmów…*, s. 129 i nast.

[16] Zob.: P. Sztompka, *Kapitał społeczny. Teoria przestrzeni międzyludzkiej*, Kraków 2016, s. 219 i nast.; H.A. Semetko, *Komunikacja polityczna*, w: R.J. Dalton, H.-D. Klingemann (red.), *Zachowania polityczne*, tom 1, Warszawa 2010.

[17] Zob.: A. Kalinowska-Żeleźnik, S. Kuczamer-Kłopotowska, A. Lusińska, *Znaczenie mediów społecznościowych w życiu codziennym młodszych millenialsów*, w: J. Kreft (red.), *Facebook. Oblicza i dylematy*, Kraków 2017, s. 93 i nast.; D. Tapscott, *Cyfrowa dorosłość. Jak pokolenie sieci zmienia świat*, Warszawa 2007; G. Polański, *Cechy pokolenia sieci w perspektywie pokolenia Y. Raport z badań*, w: J. Morbitzer, E. Musiał (red.), *Człowiek – media – edukacja*, Kraków 2014.

W efekcie wskazanych wyżej procesów, model społeczeństwa, którego członkowie zaspokajają swoje potrzeby poznawcze poprzez operowanie na zasobach w formie papierowej i – aby wyrobić sobie własny pogląd czy stanowisko – odwołują się do opinii autorytetów ze starszych pokoleń, powoli odchodzi w przeszłość. Nadchodzi era, w której źródłem wiedzy będą wyszukiwarki, dające ludziom natychmiastowe (acz w wielu wypadkach obciążone błędami i uproszczeniami) odpowiedzi na mnóstwo pytań. Komputery i telefony komórkowe już dziś wyręczają wielu ludzi w aktywności umysłowej, „przejmują pełnione dotąd przez mózg funkcje związane z magazynowaniem i przetwarzaniem danych”[18].

Nie jest to tylko zmiana o charakterze technicznym. Wyszukiwarki, jak celnie zauważa Jan Kreft, są bowiem, podobnie jak inne media, uzależnione „od kontroli redakcyjnej”, „od formuły algorytmu, dostępu i jakości baz danych oraz zakodowanych w nim założeń, od uprzedzeń jego interesariuszy, a zwłaszcza bezpośrednio zarządzających”[19]. Jest to niezmiernie ważne w sytuacji, gdy w relacjach ludzi ze światem realnym w coraz większym stopniu pośredniczy świat wirtualny. W skali masowej nie szuka się już odpowiedzi na pytania dotyczące np. historii, teraźniejszości czy przyszłości (i wszelkie inne) w zasobach wiedzy książkowej, na drodze pracy myślowej, w szczególności zaś głębszej refleksji intelektualnej[20]. Ukształtował się nawyk wyszukiwania informacji i gotowych odpowiedzi w przestrzeni internetowej. Jak podaje Kevin Kelly, ludzie klikają dzisiaj strony internetowe 100 miliardów razy dziennie, zaś w ciągu roku internetowe wyszukiwarki udzielają dwóch bilionów odpowiedzi na kierowane do nich pytania[21].

W powszechnie praktykowanym pozyskiwaniu gotowych odpowiedzi w internecie bardzo istotny staje się obraz i dźwięk. Ekran wypiera druk w tak szybkim tempie, że można mówić o konflikcie kulturowym między ludźmi (czytelnikami) książki i ludźmi (użytkownikami) ekranu[22]. Istnieje też głęboki rozziew między dawnym samodzielnym – i często mozolnym – dochodzeniem do wiedzy a teraźniejszym łatwym jej pozyskiwaniem; odbiorcy internetu chodzi przecież zwykle o to, by rozstrzygać daną kwestię w czasie rzeczywistym i w ujęciu zero-jedynkowym. Przy takim podejściu nie ma miejsca na złożone rozumowanie, wnioskowanie od ogółu do szczegółu lub od szczegółu do

---

18 Y.N. Harari, *Sapiens. Od zwierząt…*, s. 495.

19 J. Kreft, *Władza algorytmów…*, s. 127.

20 Zob.: A. Halavais, *Wyszukiwarki internetowe a społeczeństwo*, Warszawa 2012; A. Keen, *Kult amatora. Jak internet niszczy kulturę*, Warszawa 2007. Na temat wpływu internetowego poznania świata na indywidualną i zbiorową psychikę, zob.: E. Aboujaoude, *Wirtualna osobowość naszych czasów. Mroczna strona e-osobowości*, Kraków 2012, oraz P. Wallace, *Psychologia Internetu*, Poznań 2003.

21 K. Kelly, *Nieuniknione…*, s. 395 i 407.

22 Tamże, s. 125.

ogółu, na wątpliwości i żmudne dociekania, na sceptycyzm i postawę krytyczną. Skomplikowane wywody są zastępowane hasłowymi komunikatami.

W czasach ekspansji mediów społecznościowych świat jest zaludniany przez niewolników Facebooka (największego z tych mediów), dla których stała obecność w sieci, nieustanne obserwowanie innych osób i jak największy poziom własnej „widoczności" w internecie stają się niezbędnym warunkiem dobrostanu[23]. Cisza w kontaktach internetowych zaczyna być traktowana przez młodych ludzi jako przejaw wykluczenia społecznego. W relacjach związanych z obiegiem informacji liczą się przede wszystkim szybkość uzyskania informacji oraz emocje[24].

Kultura sieci przenika do wszystkich dziedzin, w tym do obszaru rządzenia w przestrzeni publicznej. Fundamentalne zmiany związane z kulturą sieci nie tylko dotyczą trybu porozumiewania się ze światem, lecz także przekładają się jakościowo na sposób rozumowania. Zmieniają się mechanizmy władzy. Błędem byłoby oczekiwać, że ukształtowanie wieloelementowego systemu sieciowego, w którym państwo jest tylko jednym z węzłów, oraz kulturowe zderzenie społeczeństwa ery słowa drukowanego ze społeczeństwem ery informatycznej nie odciśnie swojego piętna na świecie polityki i rządzenia. Jak zauważa Castells „obecny proces podejmowania decyzji politycznych odbywa się w sieci interakcji między instytucjami narodowymi, ponadnarodowymi, międzynarodowymi, współnarodowymi, regionalnymi i lokalnymi, a jednocześnie odwołuje się do organizacji społeczeństwa obywatelskiego"[25].

3.4. Ekspansja cywilizacji cyfrowej jako uwarunkowanie zmian modelu władzy

Systemowe powiązanie rządzenia z modelem władzy • Pojawianie się nowych modeli władzy i wzrost znaczenia władzy urzeczywistniającej się poprzez wpływ na świadomość ludzi • Władza informacji, komunikacji społecznej i zasobów danych cyfrowych

Rządzenie jest nierozłącznie związane z modelem władzy, w którego ramach się odbywa. W historii myśli społecznej i politycznej można znaleźć bardzo różne ujęcia władzy[26]. Nie będę jednak tutaj omawiać teorii władzy. Tytułem

[23] Tamże, s. 106 i nast. oraz 207.

[24] J. Bartlett, *Ludzie przeciw technologii. Jak Internet zabija demokrację (i jak ją możemy ocalić)*, Katowice 2019, s. 56.

[25] M. Castells, *Władza komunikacji*, s. 51.

[26] Zob.: J. Baszkiewicz, *Władza*, Wrocław 1999; J. Scott, *Władza*, Warszawa 2006; J. Staniszkis, *Zawładnąć! Zarys procesualnej teorii władzy*, Warszawa 2012; M. Juza, *Między wolnością a nadzorem…*, s. 132 i nast.

przykładu wspomnę, że w koncepcji Thomasa Hobbesa władza – ucieleśniona w Lewiatanie jako absolutnym suwerenie – wiąże się z gwarantowaniem porządku i bezpieczeństwa społecznego. Max Weber rozróżnia władzę opartą na tradycji, charyzmatyczną oraz legalną (czerpiącą swoje podstawy z prawa). Michel Foucault wiąże władzę z możliwością panowania nad dyskursem. Pierre Bourdieu traktuje władzę jako możliwość wyznaczania treści dominujących w świadomości ludzi.

W dotychczasowej historii władzy w przestrzeni publicznej najważniejszy był kontekst personalny i instytucjonalny. W analizie rządzenia zawsze należy rozgraniczać podmioty sprawujące władzę nominalnie, w myśl rozwiązań konstytucyjnych, i podmioty posiadające faktyczną władzę w ramach praktyki politycznej. Za każdym razem trzeba sobie odpowiedzieć na pytanie, kto naprawdę rządzi: władca czy jego dwór, polityk czy jego doradcy, rząd czy lider polityczny znajdujący się formalnie poza rządem, a decydujący o jego działaniu, zaś w skrajnym przypadku – ekipa rządowa czy *vox populi*… Obraz realnej sytuacji w świecie władzy w przestrzeni publicznej musi uwzględniać kwestie personalne i instytucjonalne.

Istotą stosunku władczego jest zdolność doprowadzenia przez jednych do określonego zachowania innych (chodzi o – jak to ujmuje Jadwiga Staniszkis – zdolność „stania się przyczyną”[27]). Dotyczy to zachowania rozumianego zarówno jako powstrzymanie się od pewnych działań, jak i podjęcie takich, a nie innych działań. Współcześnie władza w przestrzeni publicznej ulega zasadniczym zmianom. Przestaje mieć charakter całościowy (monolityczny), staje się tworem wewnętrznie zdywersyfikowanym, o złożonej strukturze. Stosując kryteria dziedzinowe i rodzajowe, można mówić o władzy: państwowej, politycznej, normatywnej, ideologicznej, ekonomicznej, nadawania znaczeń faktom, opinii publicznej. Cechą procesu zmian w sferze tożsamości władzy jest pojawianie się nowych rodzajów władzy. Można przywołać w tym kontekście modele: władzy siły (lub zagrożenia użycia siły), władzy prawa, władzy transakcyjnej, władzy partycypacyjnej oraz – będący raczej projektem doktrynalnym niż rozwiązaniem praktycznym – model władzy samorządzenia (w której ramach zanika podział na rządzących i rządzonych).

Na zapleczu rządzenia – w zależności dominującego modelu władzy – działają różne mechanizmy: siła, dostęp do strategicznych zasobów, własność, prawo, charyzma i autorytet, przywództwo i zaufanie, koncepcje strategiczne i ukierunkowanie innowacyjne. Mimo że zmienia się sam charakter władzy, nadal jej elementem centralnym jest zdolność kształtowania określonych zachowań przez podmioty mające władzę w stosunku do podmiotów tej władzy poddanych. Model, którego istotą jest utrzymywanie władzy przez podmioty

[27] J. Staniszkis, *O władzy i bezsilności*, Kraków 2006, s. 17.

personalne i instytucjonalne na wyodrębnionych terytoriach dzięki użyciu siły lub stosowaniu groźby jej użycia, jest jednak wypierany przez nowe mechanizmy legitymizowania i zagwarantowania władzy.

W państwach demokratycznych zyskuje na znaczeniu władza „miękka", pośrednia, urzeczywistniająca się i nabierająca mocy poprzez wpływanie na świadomość ludzi i stymulowanie ich zachowań. Mechanizmy władzy i wpływu upodabniają się do siebie. Zaczyna dominować władza, która jest w dużym stopniu ukryta i tylko w ostatecznej instancji odwołuje się do środków „twardych", w tym przymusu administracyjnego. Traci natomiast na znaczeniu władza sprawowana przy użyciu jednostkowych nakazów i zakazów. Ważnymi mechanizmami współczesnej władzy są standaryzacja, proceduralizacja, partycypacja, nadawanie znaczeń faktom, wyznaczanie głównych problemów i dopuszczalnych ram oraz języka dyskursu.

Z punktu widzenia zagadnień analizowanych w tej książce, na szczególną uwagę zasługuje fakt, że w dobie ekspansji informacji oraz nowoczesnych technik i technologii komunikacji społecznej wzrasta – jak wyżej wskazałem – znaczenie władzy urzeczywistniającej się poprzez wywieranie skutecznego wpływu na świadomość ludzi. Obecnie, w związku z pojawianiem się różnych nowych rodzajów władzy, na ważności zyskuje kontekst funkcjonalny. Trzeba zresztą zauważyć, że w swej istocie władza zawsze miała charakter relacyjny. Jak ujmuje to Manuel Castells, czołowy badacz społeczeństwa sieci, władza to „zdolność relacyjna, która umożliwia aktorowi społecznemu wywieranie asymetrycznego wpływu na decyzje innych aktorów społecznych w sposób sprzyjający umacnianiu jego woli, interesów i wyznawanych wartości"[28].

Na tle zachodzących zmian coraz większą rolę odgrywa zdolność dominowania nad światem informacji i określania pól społecznego dyskursu, a tym samym narzucania pewnej hierarchii wartości: ustalania, co jest ważne i zasługuje na uwzględnienie w działaniu, co zaś jest nieważne lub szkodliwe i na to nie zasługuje. W przyszłości zapewne będzie się umacniać władza informacji, komunikacji społecznej oraz dysponentów globalnych zasobów danych zgromadzonych w przestrzeni cyfrowej[29].

We współczesnym społeczeństwie na zachowanie ludzi w istotny sposób oddziałuje treść przyswojonych przez nich informacji. Dotyczy to także polityki. Żyjemy w świecie tzw. postprawdy – świecie, w którym wizerunki medialne stają się autonomicznym narzędziem kształtowania rzeczywistości[30]. Obrazy

---

28 M. Castells, *Władza komunikacji*, s. 23.

29 P. Bajor, A. Gruszczak (red.), *Między wiedzą a władzą. Bezpieczeństwo w erze informacji*, Kraków 2019.

30 T.W. Grabowski, M. Lakomy, K. Oświecimski (red.), *Postprawda jako zagrożenie dla dyskursu publicznego*, Kraków 2018; M. d'Ancona, *Postprawda*, Warszawa 2018; A. Rothert, *Demo-net. Wirtualna projekcja rzeczywistości*, Warszawa 2001.

umocowane w świadomości społecznej niejednokrotnie liczą się bardziej niż fakty. Dotarcie do ludzi z informacją, którą przekształcą oni w uznane za „swoje" (czyli zinternalizowane) wartości, normy, zainteresowania, oceny i dyspozycje do działania, okazuje się skuteczną metodą kształtowania rzeczywistości, zwłaszcza gdy jest stosowana wobec ludzi skłonnych do eksponowania swoich własnych preferencji, stwarza bowiem pozór zachowania podmiotowości i swobody wyboru. Jest ona o wiele bardziej efektywna od metody oddziaływania na zachowania ludzi poprzez system nakazów i zakazów.

W procesie kształtowania postaw i zachowań ludzi poprzez kierowane do nich informacje istotne jest uwzględnienie pewnego szczególnego aspektu. Otóż ludziom (zwłaszcza tym, którzy wyróżniają się aktywną postawą w społeczeństwie) na ogół zależy na uzyskiwaniu w czasie rzeczywistym możliwie stanowczego potwierdzenia słuszności swoich poglądów, ocen i preferencji (w zakresie wartości, interesów etc.) przez inne osoby lub instytucje. Takie potwierdzenie otrzymane w ramach komunikacji społecznej poprawia samoocenę i przyczynia się do podwyższenia poczucia dobrostanu poszczególnych podmiotów. Możliwość zaspokajania tego rodzaju potrzeb jest – rzecz jasna – jednym z powodów przewagi internetu nad tradycyjnymi mediami operującymi drukiem, a także nad telewizją i radiem. Tym bardziej że internet ma zdolność wchłonięcia przekazów informacyjnych tradycyjnych mediów za pomocą ich internetowych edycji, a równocześnie ma cechy – jak to określa Castells – „masowej komunikacji zindywidualizowanej"[31]. Dotyczy to także informacji i interpretacji występujących w przestrzeni publicznej, w tym odnoszących się do spraw związanych z rządzeniem.

3.5. Polskie społeczeństwo w procesie zmian związanych z nowymi technologiami komunikacyjnymi i cyfrowymi

Wpisywanie się społeczeństwa polskiego w tendencje wyznaczone przez globalną ofensywę elektronicznej, zindywidualizowanej komunikacji masowej • Pozostawanie wielu Polaków poza wspólnotą ludzi aktywnych online • Zwiększanie się liczby Polaków aktywnych w internecie i korzystających z telefonów komórkowych • Przewaga obaw w podejściu Polaków do sztucznej inteligencji

Polskie społeczeństwo nie jest liderem zmian napędzanych rozwojem zindywidualizowanej komunikacji masowej. Równocześnie jednak zmiany w społeczeństwie polskim związane z kształtowaniem się kultury sieciowej wpisują

[31] M. Castells, *Władza komunikacji*, s. 68 i nast.

się w tendencje wyznaczone przez globalną ofensywę elektronicznej, zindywidualizowanej komunikacji masowej. Odnosi się to przede wszystkim do młodego pokolenia.

W Polsce, tak jak i w innych państwach, zmiany związane z informatyzacją komunikacji społecznej mają, obok omawianego w dalszej części książki wymiaru technologicznego, ważny wymiar społeczny. Zjawiska i procesy zachodzące w obu tych wymiarach wzajemnie się warunkują. Jeśli chodzi o drugi z nich, należy stwierdzić, że słabną podziały społeczeństwa na grupy wyznaczone przez stosunki własności i produkcji oraz – w mniejszym stopniu – przez miejsce zamieszkania. Motywacje działania poszczególnych ludzi od dłuższego czasu kształtują w głównej mierze interesy osobiste i rodzinne. Można też mówić o rosnącym w społeczeństwie poczuciu sprawczości, bowiem w Polsce stopniowo zwiększały się możliwości partycypacji społeczeństwa w szeroko rozumianym rządzeniu. Następowało to dzięki wprowadzaniu: różnych mechanizmów demokracji pośredniej i bezpośredniej (w tym powszechnych wyborów organów władzy publicznej oraz referendum ogólnokrajowego i lokalnego, obywatelskiej inicjatywy ustawodawczej, konsultacji społecznych i instytucji wysłuchania publicznego), samorządu terytorialnego (tworzonego w okresie międzywojennym, zablokowanego przez zasadę jednolitości władzy w 1950 r., odtworzonego w 1990 r. oraz rozbudowanego i wyposażonego w latach następnych w prawo uczestnictwa w sprawowaniu władzy publicznej i zdolność wykonywania istotnej części zadań publicznych w imieniu własnym i na własną odpowiedzialność), samorządu zawodowego i gospodarczego (uprawnionego do reprezentowania osób wykonujących określone zawody lub prowadzących określoną działalność gospodarczą), samorządu pracowniczego, możliwości działania fundacji i stowarzyszeń oraz rozwiązań partnerstwa publiczno-społecznego.

Kluczowe znaczenie dla zmian społecznych związanych ze zindywidualizowaną komunikacją masową odbywającą się za pomocą narzędzi internetowych mają: dostępność szerokopasmowej sieci telekomunikacyjnej na terenie państwa, poziom opanowania przez społeczeństwo umiejętności cyfrowych oraz dostępność dużych zbiorów danych w przestrzeni internetowej w danym kraju. Dużą wagę przywiązuje się w Unii Europejskiej także do gotowości uruchomienia sieci piątej generacji (5G) i do kształcenia w zawodach związanych z technologiami informacyjno-komunikacyjnymi (*information and communication technologies*, ICT).

Znaczna część Polaków znajduje się nadal poza wspólnotą ludzi aktywnych online. Jak czytamy w sprawozdaniu na 2019 r. przesłanym do Unii Europejskiej na potrzeby sporządzanego od 2015 r. przez Komisję Europejską

corocznego indeksu gospodarki cyfrowej i społeczeństwa cyfrowego (DESI)[32], aż 18% ludności Polski nigdy jeszcze nie korzystało z internetu (w całej UE: 11% ludności), tylko 46% ludności miało podstawowe umiejętności cyfrowe (w UE: 57%), zaś ponadpodstawowe umiejętności cyfrowe posiadało zaledwie 21% ludności (w UE: 31%). W przywołanym wyżej sprawozdaniu, posługując się danymi z 2017 r., poinformowano, że 64% polskich użytkowników internetu korzystało z sieci społecznościowych (w UE: 65%), zaś 13% także z zawodowych sieci społecznościowych (w UE: 15%). Odnotowano, że 57% użytkowników internetu korzystało z bankowości elektronicznej (w UE: 64%). Podano, że zaledwie 5% użytkowników internetu wykorzystało narzędzia elektroniczne do udziału w konsultacjach. W całej UE, w tym samym czasie, w konsultacjach i głosowaniu przez internet uczestniczyło 10% wszystkich użytkowników internetu[33].

Polacy są coraz bardziej aktywni w internecie. W badaniach CBOS z 2020 r. ustalono, że z internetu korzystało przynajmniej raz w tygodniu 68% respondentów[34]. Jeszcze w 2002 r. było to zaledwie 17% badanych, zaś w 2019 r. – 69%[35]. W 2020 r. stwierdzono, że korzystanie z internetu jest powszechne wśród respondentów w wieku do 34 lat (98% w wieku do 24 lat, 95% w wieku od 25 do 34 lat) i bardzo rozpowszechnione wśród badanych mających od 35 do 44 lat (88%). W przedziale wieku od 45 do 54 lat internauci stanowili prawie dwie trzecie badanych. Wśród osób starszych odsetek aktywnych w internecie był niższy i wynosił 56% respondentów w wieku 55–64 lat, 33% w wieku 65–74 lat i zaledwie 11% w wieku powyżej 74 lat. W badaniach z 2019 r. wyższy wskaźnik korzystających z internetu dotyczył mężczyzn (69%) niż kobiet (63%), mających wykształcenie wyższe (95%) lub gimnazjalne (93%) niż podstawowe (22%) lub zasadnicze zawodowe (54%). Stosunkowo niski odsetek osób korzystających z internetu odnotowano w grupie robotników niewykwalifikowanych i rolników. Udział użytkowników internetu był najmniejszy na wsi (60%), zaś największy wśród mieszkańców miast liczących 500 tysięcy i więcej ludności (85%). Średnia liczba godzin

---

[32] *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI). Sprawozdanie krajowe na 2019 r. Polska*, https://ec.europa.eu/digital-single-market/en/desi.

[33] Wykorzystywanie przez Polaków narzędzi internetowych w czasie kampanii wyborczych jest przedstawione w dalszych częściach tej książki.

[34] *Korzystanie z internetu*, CBOS, komunikat z badań nr 85 z 2020 r. (badanie przeprowadzono w dniach 15–25 czerwca 2020 r. w ramach procedury mixed-mode na reprezentatywnej imiennej, liczącej 1378 osób próbie pełnoletnich mieszkańców Polski, wylosowanej z rejestru PESEL).

[35] *Korzystanie z internetu*, CBOS, komunikat z badań nr 95 z 2019 r. (badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 16–23 maja 2019 r. na liczącej 1079 osób reprezentatywnej próbie losowej dorosłych mieszkańców Polski).

spędzanych tygodniowo online wyniosła 12,87 (wśród respondentów w wieku 18–24 lat było to 21,30 godzin).

W latach 2002–2018 zdecydowanie wzrosła (z 45% do 94% ogółu korzystających z internetu) liczba osób, które łączyły się z internetem bezprzewodowo, np. używając urządzeń przenośnych, takich jak telefon komórkowy, laptop, netbook, tablet. Spośród osób deklarujących używanie internetu 33% stwierdziło, że w zasadzie było cały czas online i na bieżąco otrzymywało informacje i reagowało na wiadomości (w przedziale wieku do 24 lat takich osób było 57%).

Z przywołanych wyżej badań CBOS z 2019 r. wynika, że 83% osób aktywnych w internecie (tj. 57% wszystkich badanych) dokonało zakupów w sieci, 73% użytkowników internetu (50% wszystkich badanych) korzystało za pomocą tego narzędzia z usług bankowych. W ciągu ostatniego miesiąca przed badaniami, w grupie osób aktywnych w internecie: 26% (tj. 18% ogółu badanych) korzystało z materiałów nadawanych na żywo przez innych internautów, 25% (17% ogółu badanych dorosłych) zamieściło w internecie zrobione przez siebie zdjęcia lub filmy, 29% (20% badanych) czytało blogi, zaś 20% (14% badanych) wideoblogi, 74% (50% badanych) kontaktowało się ze znajomymi przez komunikator, 5% (4% badanych) prowadziło w chwili badania blog lub stronę internetową, 23% (16% badanych) zawarło znajomość online, a z poznaną w ten sposób osobą spotkało się poza siecią 16% internautów (11% ogółu respondentów). 66% internautów (tj. 46% wszystkich badanych) miało zarejestrowane konto na jakimś serwisie społecznościowym (wśród internautów w wieku 18–24 lat było to 96%, w wieku 25–34 lat 88%, zaś w wieku od 65 lat 37%). Wśród osób aktywnych w internecie 27% (tj. 18% ogółu badanych) wykorzystywało media społecznościowe do „rozmawiania na interesujące tematy, uczestniczenia w forach dyskusyjnych, komentowania informacji".

W badaniach z 2020 r., które – co trzeba zaznaczyć – były przeprowadzone w warunkach ograniczeń bezpośrednich kontaktów w związku z zagrożeniami pandemii, znaczna liczba użytkowników internetu deklarowała, że w ciągu miesiąca poprzedzającego badania korzystała ze stałego połączenia z internetem (70% internautów), zrobiła zakupy przez internet (65% użytkowników internetu, tj. 44% ogółu badanych) i korzystała z elektronicznych usług bankowych (79% internautów, tj. 53% ogółu badanych), kontaktowała się przez komunikatory internetowe (79% internautów, tj. 53% ogółu badanych). Stosunkowo liczna grupa badanych uczestniczyła w internetowej rozmowie wideo (wideokonferencji), w której udział brało kilka lub wiele osób (31% internautów, tj. 21% badanych). W badaniach z 2020 r. CBOS ustaliło też, że w ciągu ostatniego miesiąca 25% użytkowników internetu (17% badanych) oglądało przez internet transmisję mszy świętej lub innego nabożeństwa.

Jak wynika z badań CBOS z 2017 r., narzędziem coraz częściej wykorzystywanym w Polsce do kontaktów z otoczeniem stają się telefony komórkowe[36]. Rośnie przy tym liczba użytkowników smartfonów (z 50% w 2015 r. do 57% w 2017). Do najbardziej typowych sposobów wykorzystania telefonów komórkowych, poza prowadzeniem rozmów, należy: wysyłanie i odbieranie wiadomości SMS (78%), fotografowanie (62%), prowadzenie kalendarza czy terminarza (50%), przeglądanie stron internetowych (45%), słuchanie muzyki (30%), obsługiwanie konta w serwisie społecznościowym (29%), korzystanie z komunikatora (29%), załatwianie różnych spraw przez internet (17%). Po funkcje multimedialne i internetowe w największym stopniu sięgają użytkownicy mający od 18 do 34 lat, zwłaszcza najmłodsi (w wieku 18–25 lat jest 58% tych internautów).

W Polsce w wielu dziedzinach, w tym w komunikacji, medycynie, marketingu i wojskowości, są już wykorzystywane możliwości stwarzane przez sztuczną inteligencję (SI). Przybywa narzędzi, które zostały zaprojektowane przez człowieka i są w stanie działać bez ludzkiego nadzoru. Z badań NASK przeprowadzonych w 2019 r. wynikało jednak, że narzędzia sztucznej inteligencji[37] budzą wśród polskich internautów przede wszystkim nieufność i poczucie zagrożenia. Badani wyrażali obawy głównie przed zagrożeniem prywatności związanym ze zwiększeniem inwigilacji (60,5%), a także przed niekorzystnymi zmianami na rynku pracy i technologicznym bezrobociem (ponad 40%). Z drugiej strony, wiązali z SI nadzieje na: eliminowanie najcięższych i najbardziej niebezpiecznych prac wykonywanych przez człowieka (63,1%), wspomaganie pracy wykonywanej przez człowieka (59,1%), oszczędności w gospodarowaniu energią i zasobami naturalnymi (39,7%), poprawę komfortu życia (34%), poprawę bezpieczeństwa pracy (32,7%) oraz personalizację produktów i usług (30,3%). Zdecydowana większość (89,2%) uczestników badania NASK zetknęła się już z pojęciem „sztuczna inteligencja", ponad połowa respondentów (52,3%) uważała, że SI ma wpływ na ich codzienne życie, w tym m.in. w dziedzinie rozrywki i gier (40,6%), motoryzacji i komunikacji publicznej (37,9%) oraz mediów internetowych (37,7%). Prawie połowa (47,3%) respondentów oczekiwała, że powstaną regulacje chroniące miejsca pracy przed automatyzacją wprowadzaną przez pracodawców. Jest rzeczą charakterystyczną, że w dość powszechnej ocenie badanych na rozwoju SI najbardziej zyskają międzynarodowe korporacje (53,9% wskazań badanych), duże firmy (52,9%) specjaliści z branży ICT (47,4%), uczelnie

[36] *Korzystanie z telefonów komórkowych*, CBOS, komunikat z badań nr 99 z 2017 r. (badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 29 czerwca – 6 lipca 2017 r. na liczącej 977 osób reprezentatywnej próbie losowej dorosłych mieszkańców Polski).

[37] Dalej jako SI lub AI (*artificial intelligence*).

i naukowcy (40%) oraz inne państwa (w tym Chiny – 65,9%, USA – 58,4%), zaś zaledwie 6% uczestników badania spodziewało się związanych z tym korzyści dla Polski[38].

[38] *Sztuczna Inteligencja w społeczeństwie i gospodarce. Raport z badań społecznych. Analiza wyników ogólnopolskiego badania opinii polskich internautów*, red. R. Lange, https://www.nask.pl/pl/raporty/raporty/2594,Sztuczna-inteligencja-w-oczach-Polakow-raport-z-badan-spolecznych.html.

Rozdział czwarty

Internet, media społecznościowe i cywilizacja cyfrowa – konglomerat wolności i zorganizowanego nadzoru

4.1. Internet jako obszar wielkich oczekiwań, osiągnięć i niebezpieczeństw

Wartościowe cechy internetu • Możliwości wspomagania aktywności politycznej za pomocą internetu • Zjawiska niepokojące i groźne dla podstawowych wartości i interesów ludzi związane z komunikacją internetową

Obecnie wiemy już nie tylko, jak ogromną wartość i siłę polityczną ma internet, lecz także – jak liczne są problemy i zagrożenia wynikające z komunikacji internetowej. Niezwykle istotne, także w odniesieniu do spraw wiążących się z rządzeniem, staje się pytanie, w jakim stopniu wyszukiwarki i internetowe platformy informacyjne stanowią narzędzie pozyskiwania wiedzy i kształtowania u internautów obiektywnego obrazu świata, w jakim zaś stopniu są one – stale doskonalonym – instrumentem manipulacji i realizacji partykularnych interesów finansowych i politycznych. Nie jest łatwo udzielić jednoznacznej odpowiedzi na to pytanie.

Pojawienie się w przestrzeni publicznej internetu wzbudziło spore nadzieje i oczekiwania, które w dużej mierze zostały spełnione. Najpierw dotyczyło to upowszechniania i pozyskiwania informacji, później również masowej komunikacji społecznej w czasie rzeczywistym, bez ograniczeń wynikających z odległości, a w ostatnich latach także interaktywności tej komunikacji, która łączy w sobie masowość i zindywidualizowanie.

Za sprawą internetowej komunikacji w wielu dziedzinach nastąpił zasadniczy postęp. Internet zaczynają wykorzystywać nawet instytucje stroniące od nowych technologii, np. Kościół[1]. Ludzie uzyskali tą drogą łatwy i szybki – bez dużych nakładów czasu i wysiłku – dostęp do wiedzy. Internet pozwala,

[1] J. Kloch (red.), *Internet i Kościół*, Warszawa 2011.

w dużym stopniu ponad granicami państw i bez udziału urzędowych pośredników, pozyskiwać informacje, komunikować się z milionami osób, wyrażać swoje opinie, toczyć spory, nawiązywać i utrzymywać kontakty osobiste. Daje możliwość efektywnego korzystania z prawa dostępu do informacji publicznej, w tym z coraz liczniejszych rejestrów publicznych, i ułatwia kontrolę rządzących.

We wszystkich zasygnalizowanych powyżej zakresach internet nie ma poważnej konkurencji. Teza ta w pełni odnosi się do informacji i komunikacji politycznej. Siła oddziaływania, jaką daje internet, ujawnia się szczególnie w sprawach budzących społeczne zainteresowanie, polityczne emocje, tam gdzie chodzi na przykład o uzyskanie czyjegoś poparcia lub nakłonienie do odrzucenia kogoś/czegoś. Ilustracją możliwości rozpowszechnienia w krótkim czasie za pomocą narzędzi internetowych informacji o znaczeniu politycznym może być podana przez amerykański serwis Politico liczba odbiorców, którzy w 2019 r. sięgnęli w internecie do raportu ze śledztwa Roberta Muellera w sprawie rosyjskiej ingerencji w przebieg wyborów prezydenckich w USA w 2016 r. Dziennikarze ustalili na podstawie danych urzędowych, że dokument ten – w ciągu niespełna trzech miesięcy po jego ogłoszeniu – został pobrany w sumie prawie 800 milionów razy, w tym tylko 18 kwietnia (w pierwszym dniu dostępności) aż ponad 644 miliony razy[2]. Takiego wyniku nie można osiągnąć przy użyciu żadnego innego narzędzia komunikacji.

Cywilizacja internetowa ma wielką siłę wyzwalania społecznej energii i mobilizowania ludzi do działania, bez konieczności powoływania w tym celu formalnych organizacji. Pojawia się nowe zjawisko w postaci internetowych ruchów społecznych. Ruchy te są w sieci internetowej wzmacniane, a niejednokrotnie są w niej (albo za jej pomocą) tworzone. Powstają grupy poparcia wartościowych inicjatyw społecznych oraz ruchy protestu przeciwko naruszaniu praw i wolności człowieka i obywatela lub przeciwko innym patologicznym działaniom podmiotów władzy publicznej. Ruchy te coraz częściej stają się płaszczyzną mobilizacji społecznej, w skrajnych przypadkach znajdującej wyraz w wystąpieniach ulicznych przeciwko władzom prowadzących do zmian w sferze władzy publicznej, w tym zmian w zakresie systemu politycznego[3]. (Bez ryzyka popadnięcia w przesadę można więc mówić o pewnym potencjale wywrotowym internetu). To nie jest scenariusz *political fiction*, to rzeczywistość, w której w nowy sposób ukształtowały się relacje między władzą w przestrzeni publicznej i komunikacją społeczną. Liczne przykłady zjawisk ilustrujących te relacje można odnaleźć w książce Manuela Castellsa, w której przedstawił

[2] https://www.politico.com/story/2019/08/15/mueller-report-downloaded-1464189.

[3] D. Kotowicz, *Internet – szanse i zagrożenia dla demokracji*, w: D. Batorski, M. Marody, A. Nowak (red.), *Społeczna przestrzeń Internetu*, Warszawa 2006; M. Nowina-Konopka, *Rola internetu w rozwoju demokracji w Polsce*, Kraków 2008.

on udział wspólnot internetowych m.in. w przebiegu (między czerwcem 2010 i grudniem 2011 r.) rewolucji w Egipcie i innych państwach arabskich oraz w demonstracjach w Hiszpanii i Stanach Zjednoczonych w latach 2011–2012[4].

Wraz z powstaniem i rozwojem komunikacji internetowej, niejako w tle, w sposób mało widoczny na zewnątrz, pojawiają się niestety także zjawiska niepokojące i groźne z punktu widzenia podstawowych wartości i interesów ludzi. Towarzysząca tworzeniu świata mediów społecznościowych opowieść o neutralnym i usługowym charakterze cywilizacji internetowej dość szybko okazała się mitem – nie wytrzymuje zderzenia z praktyką funkcjonowania tych mediów. Administratorzy internetowych wyszukiwarek i platform informacyjnych oraz kanałów komunikacyjnych uzyskują, za sprawą stosowanych algorytmów, w zasadzie nieograniczoną możliwość dokonywania wyboru, standaryzowania, pozycjonowania i strukturalizacji dostarczanych informacji. Stają się oni także dysponentem globalnego zasobu danych, w tym danych uznawanych powszechnie za wrażliwe. Tym samym występują w roli podmiotów mających pozycję władczą w sferze informacji. Dziś nie ulega już wątpliwości, że korzystają z tej pozycji, postępując zgodnie ze swoimi interesami finansowymi.

Zaistnienie w świecie cyfrowym ma nadal dla większości ludzi wyłącznie posmak wolności – daje sposobność pozyskiwania informacji i interaktywnego komunikowania się poza kontrolą instytucji państwowych. Stanowi bezprecedensową możliwość publicznego prezentowania wypowiedzi i opinii, które docierają w czasie rzeczywistym do milionów ludzi. Nawiązując do systematyki wolności zaproponowanej przez Isaiaha Berlina[5], wypada zauważyć, że jest to nienotowany w przeszłości przypływ wolności – zarówno w jej ujęciu pozytywnym: wolności do czegoś (możliwość swobodnego decydowania o swoim postępowaniu), jak i w ujęciu negatywnym: wolności od czegoś (uwolnienie się od nakazów i zakazów ze strony innych osób). Nic więc dziwnego, że akcesowi do świata cyfrowego towarzyszy wiele pozytywnych emocji.

Internet i swoboda dostępu do niego są powszechnie uznawane za ogromną wartość, zaś wszelkie próby reglamentowania zachowań w tej sferze przez władze publiczne rodzą sprzeciw społeczny. Jest rzeczą zaskakującą, że próby eliminowania patologii w funkcjonowaniu internetu i mediów elektronicznych są traktowane – bez względu na sposób ich uzasadniania – jako zamach na wolność. Świadczy to o tym, jak mocno w świadomości społecznej ugruntował się pozytywny wizerunek korporacji administrujących mediami internetowymi. Pokazuje też, jak trafny był zamysł biznesowy leżący u podstaw działania tych korporacji oraz jak skutecznie te podmioty gospodarcze „opanowały trudną

[4] M. Castells, *Siła oburzenia i nadziei. Ruchy społeczne w erze Internetu*, Warszawa 2013. Zob. też: E. Bendyk, *Bunt sieci*, Warszawa 2012; A. Rothert, *Technopolis: wirtualne sieci polityczne*, Warszawa 2003.

[5] I. Berlin, *Cztery eseje o wolności*, Warszawa 1994, s. 178 i nast.

sztukę przybierania szat ‘prohumanistycznych’, ‘społecznościowych’, w imię dobra społecznego”[6].

Wejście do świata cyfrowego, obecnie coraz łatwiejsze, technicznie prostsze, relatywnie tanie i otwierające nowe możliwości, wydaje się przy tym bezpieczne i – w pewnym sensie – oczywiste. Bycie w tym świecie jest już, szczególnie w przypadku ludzi młodych, jakby „naturalną” formą życia. Koszty uczestnictwa w rzeczywistości cyfrowej są głęboko ukryte, świadomość ich występowania jest znacznie ograniczona. Wśród tych kosztów na pierwszym miejscu trzeba wymienić zgodę na operowanie naszymi wrażliwymi danymi osobowymi oraz utratę prywatności. Ludzie bez głębszego zastanowienia udostępniają drogą elektroniczną swoje – starannie wcześniej skrywane – dane osobowe. Bez oporów wchodzą w sferę zorganizowanego nadzoru, którego są przedmiotem.

4.2. Polityczny wymiar ekspansji mediów społecznościowych i cywilizacji cyfrowej

Operatorzy internetowych platform komunikacyjnych w roli graczy biznesowych i współkreatorów debaty publicznej • Hipotezy na temat zbliżającej się ery imperializmu informatycznego

Z politycznego punktu widzenia istotne jest, że najwięksi operatorzy internetowych platform komunikacyjnych są już nie tylko graczami biznesowymi, lecz także kreatorami debaty publicznej, określającymi jej kształt i ramy. W świecie władzy informacji zarządzanie danymi internetowymi, które wyznacza reguły obowiązujące w komunikacji odbywającej się za pomocą mediów społecznościowych, wychodzi wyraźnie poza zakres problemów ekonomicznych oraz zachowań związanych z zakupem usług i towarów. Świat algorytmów wkracza bezpośrednio do sfery polityki i jest narzędziem kształtowania postaw politycznych. Monopole z branży nowych technologii administrujące algorytmami stają się, jako podmioty „miękkiej władzy”, aktywnymi graczami w świecie polityki i – bez legitymizacji demokratycznej – uzyskują zdolność koncentracji w dziedzinie władzy, danych i kontroli publicznej oraz poszerzania swoich wpływów[7]. Nauczyły się przy tym korzystać z tych możliwości w sposób arbitralny, nieprzejrzysty, w dużym stopniu władczy i pozbawiony kontroli zewnętrznej. W kontekście szybkiego rozwoju internetowych technologii

[6] J. Kreft, *Władza algorytmów*…, s. 19.

[7] J. Bartlett, *Ludzie przeciw technologii*…, s. 141.

komunikacyjnych często pojawiają się, istotne w wymiarze politycznym, pytania dotyczące władzy informacyjnej mediów społecznościowych[8]. Towarzyszą im zapowiedzi zbliżającej się ery swoistego imperializmu informatycznego, głosy ostrzegające przed kształtowaniem się „technototalitarnego porządku świata", w którym – jeśli nie podejmie się kroków zaradczych – decydujące znaczenie w kwestiach informacji i zasobów danych będą miały efekty kompleksowej elektronizacji, digitalizacji, komputeryzacji narzędzi, algorytmizacji, globalnego usieciowienia, wirtualizacji oraz zintegrowanego sterowania środowiskiem cyfrowym i sieciowym[9].

Freedom House, niezależna organizacja zajmująca się monitorowaniem stanu wolności i demokracji na świecie[10], w swoim raporcie z 2019 r., sporządzonym na podstawie szczegółowego przeglądu sytuacji w 65 państwach, ocenia jednoznacznie, że od dziewięciu lat nasila się zjawisko „autorytaryzmu cyfrowego", który zagraża wolności internetowej. Jak wskazano w raporcie: „Media społecznościowe pozwalają zwykłym ludziom, grupom obywatelskim i dziennikarzom docierać do szerokiego grona odbiorców przy niewielkich lub zerowych kosztach, ale stanowią także niezwykle użyteczną i niedrogą platformę dla operacji wywierania złego wpływu przez podmioty zagraniczne i krajowe. Przywódcy polityczni zatrudniali osoby, które ukradkiem kształtowały opinie online w 38 z 65 krajów objętych (…) raportem (…). W wielu krajach wzrost populizmu i skrajnie prawicowego ekstremizmu zbiegł się z rozwojem hiperpartyjnych mobów internetowych, które obejmują zarówno autentycznych użytkowników, jak i fałszywe lub zautomatyzowane konta. Budują dużą widownię wokół podobnych zainteresowań, łączą polityczne przesłanie z fałszywymi lub zapalającymi treściami i koordynują ich rozpowszechnianie na wielu platformach"[11].

---

[8] J. Kreft (red.), *Facebook. Oblicza…*; J.-H. Lorenzi, M. Berrebi, *Przyszłość naszej wolności. Czy należy rozmontować Google'a… i kilku innych?*, Warszawa 2019; K. Mazurek, *Facebook: od portalu społecznościowego do narzędzia polityki*, Lublin 2018; R. McNamee, *Nabici w Facebooka. Przestroga przed katastrofą*, Poznań 2020; S. Vaidhyanathan, *Antisocial Media. Jak Facebook oddala nas od siebie i zagraża demokracji*, Warszawa 2018; Ł. Walewski, *Władza w sieci. Jak nami rządzą social media*, Kraków 2020.

[9] J. Jankowski, *Trendy cywilizacji informacyjnej. Nowy technototalitarny porządek świata*, Warszawa 2019, s. 11 i 22. Autor stwierdza, że wskazane procesy są wynikiem postępu technologicznego, a w istocie stanowią one „sprzężenie supertechnologii inwazji informacyjnej (informatyzacji) oraz superideologii postępu informacyjnego (informatyzmu)", tamże, s. 19. Zob. też: J. Angwin, *Społeczeństwo nadzorowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji*, Warszawa 2020.

[10] https://freedomhouse.org/about-us.

[11] https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media.

4.3. Polityczna siła administratorów narzędzi komunikacji internetowej i algorytmów

Instytucje oraz sieci administrujące komunikacją w sferze informacji jako struktury władzy • Algorytmy znajdujące się w dyspozycji globalnych administratorów sieci jako nowy mechanizm władczy

Gwałtowny rozwój i wzrost znaczenia internetu rozumianego jako narzędzie pozyskiwania, upowszechniania i wymiany informacji oraz społecznej komunikacji sieciowej nakazuje dokładnie rozważyć mechanizmy działania i stronę podmiotową administratorów internetu oraz znajdującego się w internecie zasobu danych. Powracając do przywołanej już wcześniej relacyjnej koncepcji władzy autorstwa Manuela Castellsa, trzeba zauważyć, że w epoce radykalnego zwiększenia roli informacji, jako struktury władcze funkcjonują już nie tylko indywidualne i zbiorowe podmioty władzy publicznej na terenie poszczególnych państw, lecz także instytucje oraz sieci administrujące komunikacją w sferze informacji.

Mechanizmy władzy w coraz mniejszym stopniu polegają na stosowaniu przemocy, wydawaniu nakazów i zakazów, w coraz większym zaś – na organizacji i kontroli dyskursu w zindywidualizowanej komunikacji masowej. Nie można jednak poprzestać na tej konstatacji. Jeśli bowiem prawdziwa jest teza, że to dyskurs i interaktywne relacje komunikacyjne decydują obecnie w dużej mierze o kształtowaniu się relacji władczych w układach społecznych, to narzuca się pytanie o podmioty, które wyznaczają ramy formalne i treściowe owego dyskursu. Castells odróżnia w tym kontekście władzę sieciową (związaną z kontrolowaniem dostępu do sieci), władzę sieci (skupioną wokół narzucania globalnych standardów sieci), władzę usieciowioną (powiązaną z dominującą pozycją danej sieci w stosunku do innych) i władzę tworzenia sieci (powiązaną ze zdolnością tworzenia i programowania sieci oraz zdolnością kształtowania siatki kooperacji między sieciami w ramach kontroli punktów łącznikowych między sieciami)[12].

W komunikacji społecznej pojawia się mechanizm władczy, którego bazą i narzędziem stają się w relacjach sieciowych algorytmy znajdujące się w dyspozycji globalnych administratorów sieci. Za pomocą algorytmów[13], w następujących po sobie instrukcjach opisywanych językiem matematycznym, tworzone

[12] M. Castells, *Władza komunikacji*, s. 53 i nast.

[13] W polskiej literaturze na ten temat: J. Kreft, *Władza algorytmów*… – interesujące studium zawierające liczne odwołania do obszernej literatury światowej, ukazujące zagadnienie w sposób systemowy i całościowy, z uwzględnieniem różnych sposobów rozumienia pojęcia „algorytm". Zob. też C. O'Neil, *Broń matematycznej zagłady. Jak algorytmy zwiększają nierówności i zagrażają demokracji*, Warszawa 2017.

są ściśle określone schematy grupowania, sortowania, dopasowywania i wyszukiwania informacji. Algorytmy działają z wielką szybkością na bardzo dużych zbiorach danych. Oferują możliwości wyszukiwania w kontaktach międzyludzkich kluczowych słów oraz kierunków aktywności. Są podporządkowane realizacji zadań wskazanych przez ich twórców. Stanowią narzędzia wykonawcze w procesach decyzyjnych, ze względu na to, że w sposób automatyczny rozpoznają, dostarczają, porządkują i przetwarzają dane obecne w zbiorze informacji internetowych. Są nietransparentnym mechanizmem selekcji informacji dostępnych użytkownikom sieci. Zarządzają widocznością użytkowników w internecie. Nie chodzi w tym przypadku tylko o filtrowanie rzeczywistości, lecz także o monopolizowanie kierunków zainteresowań.

W świetle powyższego można powiedzieć, że odbiorcy oferty informacyjnej, jaką niosą ze sobą wyszukiwarki i platformy, w których są wykorzystywane algorytmy, stają się w sensie poznawczym więźniami polityki informacyjnej owych narzędzi, zaś w sensie komunikacyjnym – instrumentem wzmocnienia oddziaływania autorów i administratorów tych narzędzi. Wolność wyboru dokonywanego przez odbiorców jest w takim razie pozorna, faktycznie zaś muszą się oni poddać wyborowi (pozycjonowaniu) danych wynikającemu z preferencji administratorów wyszukiwarek i platform informacyjnych.

Siła algorytmów musi być uwzględniana w rządzeniu jako uwarunkowanie bezpośrednio oddziałujące na społeczeństwo i jako narzędzie stosowane w kształtowaniu działań samych rządzących. Algorytmy uczestniczą (pośredniczą) w każdym elektronicznym kontakcie między człowiekiem i jego otoczeniem. Odwołując się do literatury światowej[14], Jan Kreft zwraca uwagę na to, że nie mają one charakteru matematycznej abstrakcji i stanowią „rodzaj socjo-technologicznego związku, część rodziny autorytatywnych systemów tworzenia wiedzy lub podejmowania decyzji, w których ludzie dostarczają dane i są umieszczani dzięki nim w systematycznych/matematycznych relacjach, a następnie otrzymują zasoby informacyjne na podstawie analizy danych wejściowych i ich ocen”[15]. Należy się zgodzić z opinią, że w tych warunkach władza algorytmów przenika się z władzą polityczną i siłą gospodarczą[16]. Kto ma władzę nad algorytmami, uzyskuje władzę w sprawach dotyczących domeny publicznej. Nie trzeba chyba dowodzić, jak ważna jest to zależność, tym bardziej że społeczeństwo, stanowiące aktywne środowisko rządzenia, coraz wyraźniej przybiera kształt „społeczeństwa algorytmicznego”[17].

---

14 Zob.: T. Gillespie, *The Relevance of Algorithms*, w: T. Gillespie, P. Boczkowski, K.A. Foot (eds.), *Media Technologies: Essays on Communication, Materiality, and Society*, Cambridge 2014.

15 J. Kreft, *Władza algorytmów*…, s. 31.

16 Tamże, s. 285.

17 K. Krzysztofek, *Społeczeństwo w dobie internetu: refleksyjne czy algorytmiczne?*, w: W. Jonak (red.) i in., *Re: internet – społeczne aspekty medium. Polskie konteksty i interpretacje*, Warszawa 2006.

4.4. Prywatność jako wielka przegrana rozwoju cywilizacji cyfrowej

Nasilanie i doskonalenie uprzemysłowionej inwigilacji w przestrzeni internetowej • Napięcia między cyfrowością i prywatnością • Wszechobecność procedur elektronicznej identyfikacji i stałe powiększanie się zbioru danych „cyfrowego wszechświata"

Masowa inwigilacja w przestrzeni internetowej stale się nasila i podlega udoskonalaniu. Odbywa się ona za pomocą mechanizmów w dużej mierze niewidocznych, pozbawionych cech represyjności i pozornie wolnych od rozwiązań dyscyplinujących, co sprawia, że inwigilowani i nadzorowani mogą mieć niezachwiane przekonanie o własnej podmiotowości i poczucie bezpieczeństwa w sieci. Nadzór w obrębie cywilizacji cyfrowej ma charakter specyficzny, „inteligentny"[18], „wręcz niekiedy przyjemny"[19]. Uwzględnia prawidła psychologii społecznej.

Komunikat pojawiający się w chwili wejścia do kolejnego programu elektronicznego, który głosi, że przejście do aplikacji jest równoznaczne z akceptacją jej regulaminu, przez większość ludzi jest traktowany jako informacja nieistotna i rutynowa. Liczy się przede wszystkim to, że z pobraniem danego programu lub aplikacji zazwyczaj nie wiążą się koszty finansowe, a równocześnie pojawiają się nowe możliwości poruszania się w przestrzeni cyfrowej. Miliony ludzi bez zastanowienia akceptują regulaminy zorganizowanej inwigilacji ukryte pod zwodniczą nazwą „zasady prywatności", ale zapoznanie się z regulaminem nie chroni przed przykrymi niespodziankami, w sytuacji gdy każdy z nich zawiera pozornie niewinne zobowiązanie: „akceptuję dokonywanie zmian regulaminu". Zdarza się, że administratorzy sieci nawet nie starają się uzyskać od użytkowników zgody na dokonywane zmiany. Przykładem tego może być działanie firmy Google, która zmieniła hasła prawie dwóm miliardom użytkowników jednej z wersji systemu Android pod pozorem kontroli autentyczności klientów, a w istocie – jak uważają obserwatorzy – w związku z przygotowaniem do zastąpienia hasła danymi biometrycznymi[20].

Pod adresem internetu – a zwłaszcza wielkich firm internetowych – często jest formułowany zarzut łamania prawa użytkowników do prywatności. Niestety, do nadużyć w tej dziedzinie dochodzi także dlatego, że ludzie dobrowolnie udostępniają w internecie swoje dane, mimo że na ich wykorzystywanie i przetwarzanie nie mają żadnego wpływu, odbywa się to całkowicie poza ich kontrolą. Niefrasobliwie wprowadzają do przestrzeni internetowej szczegółowe

[18] Tamże, s. 141.

[19] M. Juza, *Między wolnością a nadzorem…*, s. 153.

[20] https://cyfrowa.rp.pl/it/36708-bez-pytania-google-zmienilo-hasla-prawie-dwom-miliardom-ludzi?utm_source=cyfrowa&utm_medium=red_poleca.

informacje, których nie byliby skłonni ujawnić w bezpośrednim kontakcie. Operatorzy kanałów komunikacji elektronicznej kamuflują prawdziwy stan rzeczy, gwarantując użytkownikom bezpieczeństwo w sieci, tak naprawdę bowiem w tym świecie obowiązuje zasada, że to, co jest cyfrowe, przestaje być prywatne. To, co w tym systemie się pojawia, nie podlega zapomnieniu. Jak podkreślają informatycy, dostępna w poszczególnych urządzeniach komenda „usuń" oznacza najczęściej wyłącznie możliwość ukrycia określonych danych przed… samym sobą. Procedury doprowadzenia do „zapomnienia" danych w przestrzeni internetowej są skomplikowane i mało efektywne.

Miliony ludzi korzystają każdego dnia z narzędzi informatycznych, na ogół nie zdając sobie sprawy z tego, że niemal w tym samym czasie podlegają swoistej obróbce: „czytaniu", mapowaniu, formatowaniu i klasyfikowaniu przez te narzędzia. W sposób całościowy są zestawiane i analizowane treści dotyczące ich elektronicznych kontaktów telefonicznych i tekstowych, wizerunków utrwalonych na fotografiach, wskazań geolokalizacji, wyszukiwanych informacji, operacji elektronicznych dokonywanych za pomocą różnych urządzeń etc.

Trwa permanentna analiza zachowań użytkowników internetu. Dzięki monitorowaniu zachowań w sieci danego odbiorcy informacji, algorytmy „uczą się" jego osobistych preferencji i pozwalają tworzyć profil zawierający wskazówki co do najlepszej drogi oddziaływania na niego. Trzeba się więc zgodzić z opinią, że w efekcie dochodzi do powstania rzeczywistości, której konstrukcja obejmuje „widzialną wolność" oraz „niewidzialny nadzór"[21]. Ten nadzór jest wpisywany w zasady funkcjonowania systemu internetowej komunikacji i mediów społecznościowych.

Współcześnie trudno już wskazać obszar spraw, w którym można się poruszać bez zostawiania śladów elektronicznych. By zostawiać takie ślady, nie trzeba być aktywnym członkiem portalu społecznościowego czy korzystać z poczty elektronicznej lub dokonywać elektronicznej archiwizacji swoich zasobów dokumentów tekstowych i głosowych oraz różnego rodzaju innych dokumentów, w tym zdjęć. Wystarczą rutynowe, codzienne działania… Nasze wynagrodzenia i emerytury trafiają na rachunki bankowe prowadzone w systemie bankowości elektronicznej. Coraz większą liczbę operacji wykonujemy za pomocą kart kredytowych lub elektronicznych przelewów. Swoje, często bardzo szczegółowe i wrażliwe, elektroniczne dane zostawiamy w miejscach, w których przebywaliśmy (np. w hotelach), a także w firmach, z których usług korzystaliśmy (np. w liniach lotniczych). Wiele procedur dopuszcza lub wręcz nakazuje posługiwanie się komunikacją internetową w przestrzeni publicznej i urzędowej (by wspomnieć tylko rozliczenia podatkowe, historie chorób, zwolnienia lekarskie i recepty). Rośnie liczba osób, które rezygnują

[21] M. Juza, *Między wolnością a nadzorem…*, s. 319.

z prowadzenia papierowych kalendarzy do zapisywania planowanych zajęć, różnych informacji etc. i sięgają po terminarze elektroniczne w swoich telefonach. Okazji do zostawienia elektronicznego śladu przybywa z każdym dniem.

Nieustannie rosną zbiory danych „cyfrowego wszechświata" zgromadzone w zasobach mediów społecznościowych. Peter W. Singer i Emerson T. Brooking, amerykańscy analitycy cyberbezpieczeństwa, w publikacji wydanej w 2018 r. przywołali następujące statystyki: „W ciągu jednej minuty na Facebooku pojawia się 500 000 nowych komentarzy, 293 000 nowych statusów i 450 000 nowych fotografii. Do You Tube zostaje wysłanych ponad 400 godzin wideo, a z Twittera zostaje wysłanych ponad 300 000 twitów. Kryją się w tym miliardy danych i metadanych takich jak znakowanie osób, które znajdują się na danej fotografii, albo identyfikacja stacji przekaźnikowej, skąd wysłano wiadomość"[22]. Ci sami specjaliści szacują, że jeśli zostanie utrzymane obecne tempo robienia „selfie" udostępnianych online, „przeciętny Amerykanin wykona w ciągu życia około 26 000 selfie"[23].

Stałe doskonalenie programów analitycznych znajdujących się w zasobie narzędzi operatorów sieci powoduje, że zgromadzone w przestrzeni elektronicznej dane zaczynają dotyczyć nie tylko naszych zachowań, lecz także kontaktów, motywów, zainteresowań, preferencji czy – rzecz niezwykła – zamiarów i schematów myślenia. Zorganizowany nadzór będący immanentnym elementem świata internetowej komunikacji „ujawnia też często takie informacje o nadzorowanym, których on sam nie jest nawet świadomy"[24].

Jacek Jankowski, w swojej książce stanowiącej swoisty manifest sprzeciwu wobec ekspansji „nowego technototalitarnego porządku świata", szczegółowo indeksuje zagrożenia, które czyhają na użytkowników sieci telekomunikacyjnych. Autor przedstawia następujący katalog stosowanych metod i technik (w tym praktyk przestępczych): profilowanie, rankingowanie, penetracja historii aktywności cyfrowej, zbieranie materiałów kompromitujących, monitorowanie, lokalizowanie, konsolidowanie (grupowanie), cenzurowanie (selekcja informacji), upublicznianie danych, szantażowanie, dedykowanie informacji, stymulowanie zachowań, ewaporowanie (wymazywanie ze zbiorowej pamięci śladów o danej osobie), znakowanie (zdalne identyfikowanie), kategoryzowanie, diagnozowanie zachowań, mapowanie (odtwarzanie historii życia), pilotowanie (automatyczne obserwowanie) oraz wizerunkowanie[25].

---

22 P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny. Media społecznościowe jako broń*, Kraków 2019, s. 86.

23 Tamże, s. 88.

24 M. Juza, *Między wolnością a nadzorem…*, s. 154.

25 J. Jankowski, *Trendy cywilizacji informacyjnej…*, s. 59–60.

4.5. Patologiczne zjawisko urynkowienia danych użytkowników mediów społecznościowych

Komunikacja internetowa jako sfera działań biznesowych • Dane osobowe jako towar handlowy udostępniany na zasadach komercyjnych • Projekt Facebooka w sprawie waluty cyfrowej Libra jako przykład przyjmowania orientacji biznesowej przez administratorów mediów społecznościowych

Komunikacja internetowa stała się biznesem. Działalność gigantów internetowych wykorzystujących siłę algorytmów i możliwości technik cyfrowych ściśle wiąże się z procesami globalizacji, monopolizacji i komercjalizacji, w tym z olbrzymimi zyskami czerpanymi z handlowego obrotu danymi użytkowników. Do największych internetowych graczy należą Facebook, Google, Twitter, YouTube, Instagram i Amazon. To podmioty właścicielskie tych platform i narzędzi komunikacji internetowej dzielą się współcześnie w globalnej sieci, opierając się na przedmiotowej specjalizacji, całą przestrzenią internetowej „wolności" informacyjnej i komunikacyjnej. Nastąpiła też monopolizacja systemów operacyjnych, wśród których dominuje system Android (firmy Google) oraz system iOS (firmy Apple). W 2019 r. Facebook nakazał nawet swoim niektórym serwisom uwidocznić powiązania korporacyjne już w samej nazwie. W efekcie aplikacja WhatsApp ma występować pod nazwą „WhatsApp from Facebook", a Instagram ma używać nazwy „Instagram from Facebook". Zależności w ramach korporacji internetowych są jeszcze wyraźniej widoczne, gdy uwzględnia się układy właścicielskie w tym środowisku. Okazuje się wtedy, że globalnych, oddziaływających z wielką siłą graczy jest mniej, niż wydawałoby się na pierwszy rzut oka. Faktu tego nie zmienią konsekwentne zapewnienia ze strony właścicieli i administratorów narzędzi komunikacji internetowej, że nie ma mowy o monopolach, gdyż rynek ten jest wewnętrznie zróżnicowany.

Nie ulega wątpliwości, że algorytmy stosowane w serwisach internetowych są tworzone głównie z myślą o interesach finansowych ich właścicieli. Chodzi tutaj o gigantyczne zyski. Wartość firm technologicznych rośnie w szybkim tempie. W grupie amerykańskich firm, których wartość rynkowa przekroczyła na giełdzie już bilion dolarów, znajdują się Apple (z wartością ponad 1,4 biliona dolarów), Microsoft (z wyceną na poziomie prawie 1,3 biliona dolarów), Amazon i spółka macierzysta Google'a – Alphabet[26]. Wartość samego Facebooka oszacowano w 2019 r. na ponad 580 miliardów dolarów[27]. Alex Hern, redaktor naczelny działu technologii „Guardiana" w Wielkiej Brytanii, słusznie

[26] https://tvn24bis.pl/wiadomosci-gieldowe,76/alphabet-spolka-matka-google-warta-bilion-dolarow,1000878.html.

[27] https://www.politico.com/story/2019/07/12/facebook-ftc-fine-5-billion-718953.

zauważa, że strategie biznesowe gigantów mediów społecznościowych opierają się na operowaniu danymi użytkowników, zaś duża część sukcesu na tym rynku zależy od zdolności uzyskiwania kolosalnych przychodów ze sprzedaży ukierunkowanych reklam, co prowadzi do wykorzystywania ogromnych ilości danych osobowych[28]. W ten sposób właściciele mediów społecznościowych, którzy mogą w czasie rzeczywistym identyfikować użytkowników sięgających po określone treści i następnie wykorzystywać biznesowo te informacje, górują nad podmiotami zlecającymi zamieszczanie reklam w mediach drukowanych. Typ tradycyjnej (drukowanej) reklamy jest dziś w odwrocie.

Dane osobowe są traktowane jak towar handlowy, co prowadzi do nadużyć polegających na ich udostępnianiu innym podmiotom na zasadach komercyjnych. Na fali dochodzeń po aferach związanych z udostępnianiem danych użytkowników, wiedza na temat tego procederu, uprawianego bez zgody zainteresowanych osób przez poszczególne korporacje mediów społecznościowych, jest coraz większa. Przykładowo, jak ustalono w trakcie dochodzenia prowadzonego w Izbie Gmin, Facebook przekazywał na zasadach komercyjnych dane użytkowników firmom współpracującym (m.in. Airbnb, Netflix i Lyft). Właściciele mediów społecznościowych działają jak przedsiębiorcy i występując w tej roli, konsekwentnie poszukują sposobów wzmacniania swojej pozycji finansowej. Temu właśnie celowi służą – ryzykowne dla użytkowników ich produktów – komercyjne transfery danych osobowych.

Projekt Facebooka z 2019 r. dotyczący waluty cyfrowej Libra pokazuje, że należy się spodziewać prób rozszerzania wachlarza produktów, które dają właścicielom mediów społecznościowych nadzieję na zysk. W związku z tym projektem powołano organizację non profit Libra Association, która ma zarządzać obrotem tą cyfrową walutą wraz z Facebookiem i jego partnerami. Facebook planuje operować cyfrowym „portfelem" o nazwie Calibra, który umożliwi jego użytkownikom dokonywanie transakcji w nowej walucie. W obliczu rosnącej nieufności wobec tego giganta branży mediów społecznościowych w organach ustawodawczych i regulacyjnych USA, spółka prowadzi na wielką skalę działalność lobbingową na rzecz swojego projektu, korzystając z firm znanych ze skuteczności w operowaniu na rynku usług finansowych oraz z wyspecjalizowanych zespołów prawników. Przeznacza ogromne sumy na zorganizowany lobbing, który ma stanowić przeciwwagę dla obaw przed zagrożeniami prywatności, zmniejszeniem ochrony konsumentów i bezpieczeństwa systemu finansowego, a także dla podejrzeń o pranie pieniędzy. Tak jak w przypadku innych produktów, głównym argumentem kierownictwa Face-

[28] https://www.theguardian.com/technology/audio/2019/aug/06/how-much-does-google-know-about-you-podcast.

booka jest to, że ludzie są zainteresowani wprowadzeniem waluty cyfrowej[29]. Wiele wskazuje na to, że zbiorowa krytyka ze strony władz państwowych, instytucji finansowych i banków spowoduje opóźnienie wprowadzenia cyfrowej waluty. W istocie taką deklarację złożył w parlamencie amerykańskim Mark Zuckerberg, dyrektor generalny Facebooka, jesienią 2019 r., choć zwrócił również uwagę na fakt, że podobne projekty są już zaawansowane w Chinach, co powszechnie odebrano jako próbę wpisania swoich interesów w amerykańsko-chiński spór o przywództwo finansowe i technologiczne w świecie[30]. Mimo sygnalizowanych przeszkód, nie wydaje się, by administratorzy mediów społecznościowych porzucili myśl o realizacji tego projektu.

4.6. Trudności w równoczesnym zagwarantowaniu w internecie wolności i prywatności

Narastanie presji politycznej na poddanie komunikacji internetowej szczegółowej reglamentacji ze strony władz państwowych • Zróżnicowane modele przeciwdziałania patologicznym następstwom nadużywania pozycji przez komercyjne podmioty administrujące mediami społecznościowymi • Pytania dotyczące relacji między reglamentacją w cyberprzestrzeni a unikalnym charakterem internetowej indywidualnej komunikacji masowej

Odpowiedź na pytanie o sposób pogodzenia wolnościowej istoty komunikacji internetowej z wymogami zachowania prywatności i ochrony danych oraz zasadą wolnej konkurencji nie jest łatwa. Po aferach z nieuprawnionym wykorzystaniem danych osobowych użytkowników mediów społecznościowych, w tym szczególnie po posłużeniu się danymi użytkowników Facebooka w wyborach prezydenckich w USA w 2016 r., narasta presja polityczna na poddanie tej dziedziny szczegółowej reglamentacji. Narasta również sprzeciw wobec wykorzystywania w sposób nietransparentny internetowych reklam politycznych, upowszechniania się różnorodnych form manipulowania informacją w mediach społecznościowych oraz nasilania się mowy nienawiści i ekstremistycznych treści online. Z wielu stron dochodzą głosy nawołujące do przeciwdziałania tym zjawiskom i do skutecznego ich zwalczania. O tym, jak trudne to jest zadanie, może świadczyć fakt, że dopiero po kilkunastu miesiącach rozmów, w 2020 r., przedstawicielom mediów społecznościowych oraz reklamodaw-

[29] https://www.politico.com/story/2019/07/23/facebook-amasses-army-to-lobby-on-libra-1609394; https://www.politico.com/story/2019/07/15/facebook-libra-digital-currency-congress-1591429.

[30] https://www.politico.com/news/2019/10/22/zuckerberg-says-hes-willing-to-delay-libra-to-satisfy-regulators-054534.

ców udało się sformułować definicję mowy nienawiści i określić cechy treści szkodliwych, przy których nie powinny być publikowane reklamy[31]. Symptomatyczna jest również sytuacja w Niemczech, gdzie zwolennicy ochrony prywatności wystąpili z ostrym atakiem na projekt przepisów nakazujących ujawniać tożsamość użytkowników mediów społecznościowych, którzy posługują się mową nienawiści[32].

Jak szerzej pokazuję w dalszych fragmentach książki, w ramach organizacji międzynarodowych, w szczególności w Unii Europejskiej, oraz w niektórych państwach, głównie w Stanach Zjednoczonych, pojawiają się, częściowo już wdrażane, różnorodne inicjatywy zmierzające do ograniczenia swobody działania w tych sprawach administratorów mediów społecznościowych. Wszystko, co wiąże się z tym tematem, staje się przedmiotem sporów politycznych. Przybywa opinii, że aktywność państw w powstrzymywaniu zagrożeń płynących z arbitralnych finansowych decyzji korporacji mediów społecznościowych jest niedostateczna.

Istnieją zróżnicowane sposoby przeciwdziałania następstwom nadużywania pozycji przez komercyjne podmioty administrujące mediami społecznościowymi. W USA są uruchamiane przede wszystkim procedury antymonopolowe. Zgłaszane są projekty podziału korporacji nowych technologii; z taką inicjatywą wystąpiła senator Partii Demokratycznej Elizabeth Warren, kandydatka w prawyborach prezydenckich 2020 r. W Europie rozważa się wprowadzenie pełnej odpowiedzialności właścicieli platform internetowych za zamieszczone na nich treści pochodzące od użytkowników. Coraz częściej na administratorów mediów społecznościowych są nakładane różnego rodzaju kary finansowe.

W obecnej sytuacji, obok postulatów wprowadzenia dalej idących ograniczeń swobody mediów internetowych, pojawiają się też pytania o to, w jakim stopniu kierunek zmian reglamentacyjnych w cyberprzestrzeni uwzględnia unikatowy charakter internetowej indywidualnej komunikacji masowej. Nie jest rzeczą zaskakującą, że takie pytania stawiają zwłaszcza eksperci współpracujący z czołowymi koncernami ze sfery mediów i komunikatorów internetowych. Na przykład Nick Pickles, doradca strategiczny Twittera, ostrzegał w 2019 r., że sięganie po kolejne środki reglamentacji przez poszczególne państwa grozi rozszczepieniem globalnego internetu, a utrata otwartego charakteru i globalnego zasięgu internetu będzie niezmiernie szkodliwa dla demokracji na całym świecie oraz dla rozwoju innowacyjnych przedsiębiorstw[33]. Nawet jeśli potraktuje się tego rodzaju wypowiedzi jako element działań lobbingowych

---

31 https://www.pap.pl/pap-technologie/723033%2Cmedia-spolecznosciowe-i-reklamodawcy-zdefiniowali-mowe-nienawisci.html.

32 https://www.politico.eu/article/germany-hate-speech-internet-netzdg-controversial-legislation.

33 https://www.politico.com/story/2019/07/25/online-extremists-shake-the-internet-economy-1617531.

potężnych korporacji internetowych, nie można uznać wskazanego w nich problemu za nieistotny.

Kwestie związane z wolnością komunikacji internetowej stanowią realny problem, który musi być uwzględniony w działaniu decyzyjnym polityków i rządów. Wolność internetu jest szczególnie zagrożona w systemach niedemokratycznych, w których władze polityczne próbują blokować swobodny przepływ informacji i komunikację ponad granicami państwowymi. Współcześnie – bardziej szczegółowo przedstawiam to zagadnienie w dalszej części książki – można mówić wręcz o wzmożonych działaniach licznych państw mających na celu odzyskanie wpływu na treści przekazów internetowych dostępnych obywatelom tych państw i objęcie państwowym nadzorem komunikacji internetowej. Pogląd, że pozbawienie państw wpływu na treści obecne w komunikacji internetowej jest źródłem patologii, ma usprawiedliwiać projekty cenzorskie forsowane pod hasłem konieczności zagwarantowania suwerenności informacyjnej państwa. Właśnie taka filozofia leży u podstaw działań władz Chin prowadzonych w ramach systemu tzw. wielkiej zapory ogniowej.

Postulaty zapewnienia właściwych standardów komunikacji internetowej wykraczają poza sferę postępowania administratorów mediów społecznościowych. W zgłaszanych projektach naprawy (czy wręcz, jak nieraz się to określa, ratowania) sieci komunikacyjnych kontaktów internetowych zwraca się uwagę na potrzebę upowszechniania dobrych zachowań użytkowników sieci oraz zagwarantowania współdziałania państw, firm technologicznych i poszczególnych ludzi. Przykładem może być przedstawiony jesienią 2019 r. projekt swoistego kontraktu z udziałem rządów, firm technologicznych i komunikacyjnych oraz osób prywatnych w sprawie zasad ratowania sieci przed manipulacjami i fałszerstwami politycznymi oraz naruszaniem prywatności – zjawiskami wywierającymi negatywny wpływ na życie pojedynczych osób i całych społeczeństw. Dokument ten, opracowywany przy udziale 80 różnych organizacji i mający poparcie kilkudziesięciu innych podmiotów, firmował Tim Berners-Lee, jeden z twórców komunikacji internetowej. Jego przesłanie brzmi następująco: „Wolna i otwarta sieć staje przed prawdziwymi wyzwaniami. Połowa światowej populacji wciąż nie może uzyskać dostępu do Internetu. Z drugiej strony korzyści płynące z sieci wiążą się ze zbyt wieloma zagrożeniami: dla naszej prywatności, naszej demokracji, naszych praw”[34]. W dokumencie wskazuje się na: znaczenie praw dostępu do internetu połączonego z gwarancjami prywatności (w tym gwarancjami dostępu do przechowywanych w zasobie elektronicznym swoich danych osobowych); zapewnienie dostępności internetu także dla osób niepełnosprawnych i mówiących językami mniejszościowymi; ułatwienia zarządzania w jednym miejscu

[34] https://webfoundation.org.

swoimi danymi; dywersyfikację administratorów sieci oraz testowanie przez tych administratorów swoich produktów pod kątem oceny ryzyka rozprzestrzeniania się dezinformacji i szkodliwych zachowań ludzi oraz naruszania dobrostanu poszczególnych ludzi; potrzebę budowania otwartych społeczności internetowych opartych na wartościach[35].

4.7. Polskie standardy w zakresie granic wolności w komunikacji internetowej

Wypadkowa tradycyjnych rozwiązań prawa krajowego i regulacji wypracowanych w prawie międzynarodowym • Model ochrony danych osobowych w cyberprzestrzeni • Model odpowiedzialności za treści cyfrowe • Rola państwa w sprawach dotyczących wolności i odpowiedzialności w komunikacji elektronicznej

Standardy obowiązujące w Polsce w zakresie granic wolności w internecie są wypadkową tradycyjnych rozwiązań prawa krajowego i regulacji wypracowanych w prawie międzynarodowym. Formalną podstawą jest w tych kwestiach porządek prawny ONZ, Rady Europy i Unii Europejskiej. Polskie regulacje są podporządkowane – zarówno w ramach unijnego prawa obowiązującego bezpośrednio, jak i na poziomie uzupełniających i konkretyzujących regulacji prawa wewnętrznego – filozofii, zgodnie z którą podstawowe znaczenie ma ochrona danych osobowych, zaś wspomagającą rolę odgrywają przesłanki związane z prawem konkurencji oraz prawami autorskimi. W licznych punktach regulacje te słabo przystają do nowej sytuacji w świecie zindywidualizowanej komunikacji masowej i będą musiały ulegać w przyszłości zmianom.

Zagadnienia wiążące się z granicami wolności w cyberprzestrzeni przenikają się w polskim systemie prawnym z innymi aspektami zjawiska cyberaktywności. Należy tu wymienić przede wszystkim: bezpieczeństwo krajowego systemu teleinformatycznego oraz systemu cyberbezpieczeństwa, ochronę danych osobowych, bezpieczeństwo w prawie gospodarczym, ochronę praw własności intelektualnej (w tym szczególnie praw autorskich), prawo konkurencji, prawną ochronę dzieci i młodzieży (w tym szczególnie ochronę przed pornografią i przestępczością seksualną), karnoprawną odpowiedzialność za przestępstwa popełniane w cyberprzestrzeni oraz kryminalistykę cyfrową.

Przedmiotem tej książki nie jest analiza obowiązujących w Polsce przepisów dotyczących działalności prowadzonej przy wykorzystaniu narzędzi

[35] https://www.theguardian.com/technology/2019/nov/24/tim-berners-lee-unveils-global-plan-to-save-the-internet.

elektronicznych. Istnieje na ten temat obszerna literatura fachowa, w której szczegółowo przedstawiono stan oraz problemy prawne i technologiczne cyberbezpieczeństwa[36] i cyberodpowiedzialności[37]. O niektórych aspektach tych regulacji piszę w dalszych częściach książki, które są poświęcone kształtowaniu w Polsce rozwiązań państwa cyfrowego oraz administracji cyfrowej. W tym miejscu ograniczam się tylko do komentarza na temat modelowego ujęcia kwestii wolności i odpowiedzialności w komunikacji elektronicznej. W tym kontekście należy postawić dwa zasadnicze pytania. Pierwszym z nich jest pytanie o to, jak są chronione w polskiej przestrzeni prawnej dane osobowe udostępniane przez użytkowników mediów społecznościowych administratorom tych mediów. Drugim jest pytanie, jak wygląda odpowiedzialność administratorów mediów społecznościowych za upowszechniane przez nich w przestrzeni publicznej treści pochodzące od użytkowników tych mediów.

Jeśli chodzi o ochronę prawną danych osobowych użytkowników mediów społecznościowych, podstawowe znaczenie mają obecnie regulacje w postaci rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[38] (zwanego rozporządzeniem o ochronie danych osobowych – RODO) oraz powiązane z nimi akty prawa wewnętrznego[39]. Stanowią one ogólne regulacje w sprawach przetwarzania danych osobowych i stosują się do wszystkich podmiotów prywatnych i publicznych, które przetwarzają dane osobowe, oraz do większości procesów przetwarzania danych.

Istotne znaczenie ma fakt, że za sprawą zgody wyrażonej przy aktywizacji większości programów i innych narzędzi komunikacji elektronicznej, w tym przy pobieraniu danej aplikacji lub włączeniu się do danego systemu, użytkownicy mediów społecznościowych sami przystają na warunki ustalone przez administratorów tych narzędzi. Po wejściu w życie przepisów RODO media

---

[36] Zob.: C. Banasiński (red.), *Cyberbezpieczeństwo…*; S. Goździewicz, K. Tomaszycki (red.), *Prawne i społeczne aspekty cyberbezpieczeństwa*, Warszawa 2017; P. Podrecki (red.), *Prawo Internetu*, Warszawa 2007; M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009; G. Szpor, A. Gryszczyńska (red.), *Internet. Strategie bezpieczeństwa*, Warszawa 2017; A. Bułat, D. Jaroszewska-Choraś, A. Kilińska-Pękacz (red.), *Prawne aspekty cyberprzestrzeni*, Bydgoszcz 2020; A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001.

[37] Zob.: K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019; D.K. Gęsicka, *Wyłączenie odpowiedzialności cywilnoprawnej dostawców usług sieciowych za treści użytkowników*, Warszawa 2014.

[38] Dz.U. L 119, s. 1. Zob. też E. Milczarek, *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w internecie*, Warszawa 2020.

[39] Przede wszystkim ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, tekst jedn. Dz.U. z 2019 r., poz. 1781.

społecznościowe i komunikatory elektroniczne zostały jednak zmuszone do wprowadzenia zmian w swoich regulaminach pod kątem gwarancji prywatności użytkowników. Nie podejmując szczegółowej analizy tego zagadnienia, trzeba wskazać przede wszystkim na zmiany polegające na: wprowadzeniu wymogu uzyskiwania jednoznacznej zgody na wyraźnie opisane sposoby przetwarzania danych osobowych, nałożeniu na administratorów nowych obowiązków informacyjnych, nakazie domyślnego ograniczania przetwarzania oraz minimalizacji przetwarzania danych osobowych, ustanowieniu ograniczeń wykorzystywania tych danych w celach reklamowych, a także stworzeniu możliwości wycofania przez użytkownika zgody na przetwarzanie jego danych.

Trzeba zauważyć, że regulacje te tracą na znaczeniu w przypadku przetwarzania danych w relacjach transgranicznych wykraczających poza Europejski Obszar Gospodarczy. Przepisy RODO odnoszą się w głównej mierze do działalności prowadzonej przez podmioty mające siedzibę w jednym z państw członkowskich Unii Europejskiej. Przyjęto równocześnie zasadę, że przepisy RODO obowiązują także w odniesieniu do przetwarzania danych osób przebywających w Unii. W sytuacji, w której większość portali społecznościowych pochodzi spoza Europy, zasada ta formalnie prowadzi do objęcia także tych podmiotów obowiązkami wynikającymi z RODO. W praktyce jednak sprawy nie przedstawiają się tak jednoznacznie, zaś nowy stan prawny nie eliminuje arbitralności w interpretowaniu swoich obowiązków przez administratorów mediów społecznościowych.

Należy podkreślić, że nie mają mocy prawnej oświadczenia użytkownika składane w trybie innym niż przewidziany w regulaminie danego portalu społecznościowego w sprawie braku zgody na arbitralne wykorzystywanie udostępnionych materiałów. Równocześnie istotne jest, że obowiązujące przepisy dają możliwość dochodzenia przez poszczególnych użytkowników mediów społecznościowych swoich praw w relacjach z administratorami tych mediów w zakresie sposobów wykorzystania ich danych osobowych. Dotyczy to prawa do przenoszenia danych osobowych, a także: sprzeciwu wobec ich przetwarzania, ograniczenia wykorzystywania ich do profilowania, uzyskania informacji o operacjach przetwarzania oraz sprostowania i uzupełnienia danych, ograniczenia przetwarzania danych, usunięcia danych (w ramach tzw. prawa do bycia zapomnianym) i dostępu do danych. W systemie organów państwowych w Polsce funkcjonuje specjalny organ właściwy w sprawach dochodzenia wskazanych wyżej praw, tzn. Prezes Urzędu Ochrony Danych Osobowych. Istnieje też możliwość dochodzenia swoich praw przed sądem powszechnym, w tym również w zakresie uzyskania odszkodowania od administratora lub podmiotu przetwarzającego dane. Praktyka jednak pokazuje, że skuteczne wyegzekwowanie swojego prawa przez użytkownika jest bardzo trudne, zwłaszcza gdy administrator serwisu jest spoza Europy.

W kontekście pytania o zakres odpowiedzialności administratorów elektronicznych narzędzi zindywidualizowanej komunikacji masowej (w tym administratorów mediów społecznościowych) za upowszechniane przez nich treści pochodzące od użytkowników tych narzędzi trzeba zauważyć, że taka odpowiedzialność jest w dużej mierze wyłączona. Odpowiedzialność za treści jest przypisywana użytkownikom narzędzi komunikacji elektronicznej, którzy wykorzystują możliwości stworzone w cyberprzestrzeni, w tym w mediach społecznościowych, do zamieszczania swoich treści zawartych w plikach dźwiękowych, tekstowych i filmowych. Dotyczy to treści zamieszczanych zarówno w elektronicznej komunikacji publicznej, jak i na profilach zamkniętych. Biorąc pod uwagę znaczne możliwości ukrycia faktycznej tożsamości przez uczestników komunikacji elektronicznej, wypada uznać, że odpowiedzialność w tym zakresie ma charakter raczej teoretyczny.

W obecnym stanie prawnym, co do zasady, z wyjątkami wyraźnie określonymi w ustawach, administratorzy narzędzi internetowych nie mają obowiązku wstępnego lub bieżącego monitorowania treści pochodzących od zewnętrznych użytkowników ich infrastruktury elektronicznej. Chodzi także o treści, które przechowują oni w swoich zasobach danych i udostępniają publicznie (tj. nieograniczonemu kręgowi odbiorców) lub też przekazują w ramach relacji z innymi podmiotami (w tym relacji komercyjnych). Zakłada się, że taki obowiązek prowadziłby w następstwie do ustanowienia niedopuszczalnej cenzury prewencyjnej i byłby formą ograniczania wolności słowa. Z tym założeniem wiąże się daleko idące wyłączenie odpowiedzialności administratorów narzędzi internetowych za różne operacje przetwarzania danych, w tym pobieranie, przechowywanie, upowszechnianie i przekazywanie innym podmiotom danych dostarczonych przez użytkowników ich infrastruktury. Nie jest to jednak wyłączenie bezwarunkowe. Administratorzy mogą być pociągani do odpowiedzialności wówczas, gdy można dowieść, że wiedzieli oni, iż treści dostarczone przez użytkowników są prawnie niedopuszczalne, a mimo to nie interweniowali w tej sprawie. W praktyce pojawia się jednak w tym przypadku możliwość powoływania się na obiekcje co do wiarygodności wiadomości o niedopuszczalności zamieszczonego materiału (nie odnosi się to do wiadomości zawartej w urzędowym zawiadomieniu). Szczególnie wówczas, gdy nie chodzi o treści wulgarne czy obraźliwe, ale przykładowo o naruszenie dóbr osobistych osób wzmiankowanych w materiale, przez podanie informacji nieprawdziwych lub nieaktualnych. Ramy prawne interpretacji w tym zakresie wyznaczają przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[40]. Przykłady licznych wyroków sądów, w tym wyroków

[40] Tekst jedn. Dz.U. z 2019 r., poz. 123 z późn. zm.

Sądu Najwyższego[41], pokazują, że sprawy te są niejednokrotnie przedmiotem sporów i są w różny sposób interpretowane.

Przepisy szeroko definiują pojęcie administratora i odnoszą je do każdego podmiotu, który świadczy usługę hostingu, czyli udostępnia w celu przechowywania w pamięci serwerów miejsce na dane, które zamieszczą osoby trzecie (usługobiorcy), i udostępnia te dane. Tym samym, administratorami są nie tylko właściciele portali społecznościowych, ale także właściciele portali dających możliwość publikowania treści przez użytkowników, organizatorzy forów internetowych oraz platformy handlowe, na których użytkownicy publikują ogłoszenia bądź aukcje[42]. Odrębnym problemem jest ustalenie statusu autora strony prowadzonej w ramach możliwości wyznaczonych przez właściciela portalu społecznościowego, w sytuacji gdy dopuścił on do zamieszczania na tej stronie danych przez osoby trzecie. Sąd Najwyższy stanął na stanowisku, że osoba prowadząca taką stronę na Facebooku może być uznana za hostingodawcę, co wyznacza granice jej odpowiedzialności za treści pojawiające się na tej stronie pochodzące od osób trzecich[43]. Zagadnienie obecności, oceny i eliminacji z obiegu treści niedopuszczalnych w przestrzeni elektronicznej wykracza poza ramy mediów społecznościowych. Odrębne problemy związane z odpowiedzialnością za zamieszczane treści stwarza stale poszerzający się rynek wyszukiwarek, katalogów adresów internetowych, reklam.

Trzeba pamiętać, że państwo i jego organy przyjmują w Polsce w kwestiach wolności i odpowiedzialności w komunikacji elektronicznej aktywną postawę w każdej sytuacji, gdy pojawia się zachowanie, które ma cechy cyberprzestępstwa[44]. Przestępstwa związane z treścią materiałów znajdujących się w cyberprzestrzeni stanowią tylko fragment zdarzeń przestępczych, do których zaliczają się także niezgodne z prawem działania przeciwko systemom komputerowym i sieciom łączności elektronicznej lub też mające takie cechy działania z użyciem komputerów i sieci elektronicznych. W wielu przypadkach mają w tych sprawach zastosowanie ogólne regulacje prawa karnego i cywilnego. Kształtuje się jednak coraz wyraźniej prawo tworzone specjalnie w związku z rozwojem nowych technologii[45]. Należy zauważyć, że państwo, już choćby na podstawie samych przepisów konstytucji, ma obowiązek ogra-

---

41 Zob. K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, s. 170 i nast.

42 E. Górnisiewicz-Kaczor, *Zasady odpowiedzialności administratora portalu internetowego za bezprawne treści zamieszczane przez użytkowników*, http://www.codozasady.pl/zasady-odpowiedzialnosci-administratora-portalu-internetowego-za-bezprawne-tresci-zamieszczane-przez-uzytkownikow.

43 https://www.rp.pl/Dobra-osobiste/304269898-Sad-Najwyzszy-odpowiedzialnosc-administratora-strony-za-wpisy-na-Facebooku.html.

44 Zob.: M. Siwicki, *Cyberprzestępczość*, Warszawa 2013; J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015.

45 Zob.: K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015; P. Podrecki (red.), *Prawo Internetu*.

niczania cyberprzestępczości, a jego działalność w tej sferze stanowi istotne zadanie publiczne.

W warunkach rozwoju komunikacji elektronicznej dodatkowego znaczenia nabiera bezpieczeństwo informacyjne[46] i wypracowanie systemowych zasad ochrony przed dezinformacją i manipulacją internetową. Wiąże się to mocno z bezpieczeństwem telekomunikacyjnym i teleinformacyjnym, ale też wykracza poza te zagadnienia. Jak pokazuję w dalszej części tej publikacji, prace nad całościowymi regulacjami bezpieczeństwa informacyjnego, w przeciwieństwie do regulacji bezpieczeństwa informatycznego, dotychczas nie wyszły w Polsce poza fazę projektów. Nie ulega wątpliwości, że wynika to również z kalkulacji politycznych. Rządzący, zabiegając o poparcie w kolejnych wyborach, z dużą ostrożnością podchodzą do działań, które mogą być odebrane przez zwolenników pełnej wolności w internecie jako zagrożenie. Wyraźnie zaznacza się dążenie ugrupowań politycznych do zaspokojenia oczekiwań środowiska internautów – niezwykle licznego (ze znaczną przewagą liczebną ludzi młodych) i potrafiącego się zorganizować w przestrzeni komunikacji elektronicznej. Sytuacja, z jaką obecnie mamy do czynienia, świadczy o tym, jak trudno jest wypracować model łączący gwarancję wolności z regulacjami chroniącymi inne wartości podstawowe, uwzględniając przy tym uwarunkowania wynikające ze stanu otoczenia społecznego, politycznego i gospodarczego.

[46] Zob.: W. Kitler, J. Taczkowska-Olszewska (red.), *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne*, Warszawa 2017; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.

Rozdział piąty

Dane zgromadzone w cyberprzestrzeni jako zasób polityczny

5.1. Unikatowa wartość danych cyfrowych

Dane internetowe kluczem do wiedzy na temat zdarzeń przyszłych • Asymetria wiedzy związana z zasobem danych internetowych • Początek epoki kapitalizmu inwigilacji

Dane internetowe zawierają nie tylko informacje o zdarzeniach przeszłych oraz o aktualnych zachowaniach ludzi i funkcjonowaniu struktur instytucjonalnych, lecz także przesłanki prognozowania przyszłych stanów rzeczy, procesów, zdarzeń. To, co znajduje się w zasobie danych internetowych, dostarcza bowiem – przy wykorzystaniu algorytmów i narzędzi sztucznej inteligencji – materiału do wnioskowania o zdarzeniach przyszłych. Pozwala przewidywać zachowania przez rozpoznawanie nastrojów i intencji uczestników zindywidualizowanej komunikacji elektronicznej. Daje obraz sytuacji decyzyjnej użytkowników internetu, a tym samym staje się podstawą optymalizacji i ukierunkowania oferty handlowej i – co dla rządzenia najważniejsze – oferty politycznej. Dane internetowe są stale uzupełniane w trybie interaktywnym. Żaden inny sposób zdobywania wiedzy o świecie i ludziach nie może być bardziej efektywny od analizy tych danych. Nawet najbardziej pracowita i skuteczna służba specjalna, używając klasycznych metod pozyskiwania informacji, nie jest w stanie dowiedzieć się tylu rzeczy i – co ważne – uporządkować wiedzę w swoim zasobie informacyjnym z taką precyzją i szybkością.

Wartość danych internetowych jest tym większa, że nadawcy zbioru informacji, zasilający w szybkim tempie zasób danych wpisywanych do przestrzeni cyfrowej, często nie zdają sobie sprawy z faktu, iż „ślady" zostawiane przez nich w różnych miejscach internetowej przestrzeni są grupowane i zbiorczo analizowane. Podmiot, który ma dostęp do naszych elektronicznych śladów oraz narzędzia niezbędne do tego, aby te przejawy naszej aktywności grupować

i analizować w czasie rzeczywistym, dzięki temu wie o nas bardzo dużo, o wiele więcej, niż moglibyśmy przypuszczać, a nawet – zaryzykowałbym – w pewnym sensie więcej, niż my sami wiemy o sobie. Podmioty zewnętrzne dysponują dużą wiedzą o nas i mogą ją wykorzystać do swoich celów. Mniejsze znaczenie ma to, czy są to cele ściśle komercyjne czy też wiążą się one, bezpośrednio lub pośrednio, z polityką.

Informacje dostarczane przez nas samych do zasobu internetowego stają się towarem, nad którym tracimy kontrolę. Jak ujmuje to Shoshana Zuboff, profesor psychologii społecznej na Uniwersytecie Harvarda, żyjemy już w epoce kapitalizmu inwigilacji[1]. Biorąc pod uwagę wszechobecność infrastruktury cyfrowej, musimy przyznać, że rozważania o pełnej prywatności i nieograniczonej autonomii jednostki w dużej mierze odnoszą się już do przeszłości. Zaczynamy być współautorami nadzoru nad nami samymi. Swoją własną aktywnością wspieramy dążenie potężnych korporacji do przewidywania i kontrolowania naszego zachowania.

5.2. Dane zgromadzone w cyberprzestrzeni jako przedmiot zorganizowanych nadużyć

Informacje jako strategiczne zasoby rządzenia • Potrzeby sztucznej inteligencji jako przesłanka zwiększania wartości danych internetowych • Kluczowe znaczenie umiejętności selekcji, analizy i rozumienia danych • Powszechne nadużycia w zakresie gromadzenia, magazynowania, przetwarzania i dystrybucji danych w cyberprzestrzeni

Dane internetowe są już dzisiaj towarem powszechnie pożądanym. Informacje zawsze były strategicznym zasobem rządzenia. Współcześnie, w ramach mechanizmów, które starałem się wskazać w poprzednich fragmentach książki, rośnie niepomiernie ranga informacji zgromadzonych w przestrzeni internetowej oraz władza nad kanałami przepływu informacji. Informacje te stają się stopniowo dominującym zasobem władzy. Zaczynają odgrywać rolę, która w poprzednich okresach historii była przypisana własności ziemi i środków produkcji oraz posiadaniu strategicznych surowców. Nic więc dziwnego w tym, że specjaliści już teraz oceniają, iż dane zgromadzone w zasobach internetowych mają większą wartość niż złoża ropy naftowej.

[1] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York 2019. Zob. też: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy; *Algorytmy, które przepowiadają przyszłość*, rozmowa M. Kokota z S. Zuboff, „Gazeta Wyborcza" z 12 października 2019, s. 8–9.

W miarę jak w ujęciu geopolitycznym coraz większe znaczenie będą zyskiwać narzędzia sztucznej inteligencji, będzie też wzrastać wartość danych internetowych. Kai-Fu Lee, czołowy chiński kreator rozwiązań sztucznej inteligencji, dowodzi w swojej książce, że do rozwoju sztucznej inteligencji potrzebny jest, obok zdolnych inżynierów i znacznych środków finansowych, dostęp do bardzo dużych zbiorów danych z wszystkich dziedzin życia i pracy człowieka oraz funkcjonowania struktur instytucjonalnych. Te dane są niczym tlen w procesie uczenia maszynowego i przenoszą sztuczną inteligencję z fazy rozwoju internetowego i biznesowego oraz percepcyjnego (związanego z kompresją danych i digitalizacją) do fazy autonomizacji maszyn[2].

W sprawach danych zgromadzonych w zasobie internetowym można wskazać trzy główne dążenia podmiotów aktywnych w przestrzeni publicznej, w tym podmiotów politycznych i gospodarczych. Po pierwsze, jest to dążenie do uzyskania maksymalnego dostępu do zbioru danych w cyberprzestrzeni. Po drugie, jest to dążenie do zagwarantowania sobie wpływu na zasady i metody zarządzania stale powiększającym się zasobem informacji internetowych. Wreszcie, po trzecie, jest to – jak można sądzić najważniejsze i zarazem najtrudniejsze do realizacji – dążenie do nabycia umiejętności rozumienia i wykorzystania informacji zawartych w zasobie elektronicznym do obrony swoich interesów i wykonywania swoich zadań[3]. Uzyskanie dostępu do danych internetowych w każdym przypadku stanowi bowiem tylko pierwszy krok do ich wykorzystania. W sytuacji gdy w niezwykłym tempie powiększa się zasób informacji, podstawowego znaczenia nabiera umiejętność ich selekcji, analizy i rozumienia. Do tego zaś nieodzowne stają się narzędzia sztucznej inteligencji.

Prawie każdego dnia przybywa informacji o tym, że w ramach gromadzenia, magazynowania i przetwarzania oraz dystrybucji danych w cyberprzestrzeni dochodzi niejednokrotnie do poważnych nadużyć o podłożu politycznym. Dla administratorów zbiorów danych informacje zgromadzone w przestrzeni internetowej mają, jak już wcześniej wskazywałem, wartość towaru handlowego. Są one przedmiotem obrotu komercyjnego, który generuje zyski. Dotyczy to w całej rozciągłości także informacji politycznych, gdyż w obrocie nimi znajdują zastosowanie klasyczne zasady marketingu. Informacje te są formatowane, pozycjonowane w przestrzeni internetowej i traktowane jak swoiste „produkty polityczne”[4]. W związku z tym siła oddziaływania poszczególnych informacji jest w wielu wypadkach ważniejsza niż ich istota i standardy etyczne posługiwania się nimi.

Coraz więcej wiemy o licznych przypadkach nadużyć popełnionych przy korzystaniu z zasobu danych w internecie, które mają wyraźny kontekst poli-

[2] Kai-Fu Lee, *Inteligencja sztuczna…*, s. 75 i nast.

[3] G. Szpor, K. Czaplicki (red.), *Internet. Analityka danych. Data Analytics*, Warszawa 2019.

[4] K. Zajdowski, *Marketing produktu politycznego. Analiza porównawcza*, Warszawa 2017.

tyczny. Kwestie te stały się szczególnie głośne w związku ze skandalem wywołanym oskarżeniami o nieuprawnione wykorzystanie danych zgromadzonych w zasobie internetowym w czasie kampanii wyborczej 2016 r. w USA, a także w związku z głosowaniem w referendum w sprawie dalszej obecności Wielkiej Brytanii w Unii Europejskiej. Te dwa przypadki można bez wahania określić jako zdarzenia przełomowe w podejściu poszczególnych państw i rządów do problemu ochrony danych osobowych w internecie oraz identyfikowania i ograniczania niedopuszczalnych zachowań w cyberprzestrzeni. O nich też szerzej piszę w dalszych częściach tego opracowania.

5.3. Batalia wokół dyskrecjonalnego dostępu do globalnego zasobu informacji elektronicznych

Walka o uzyskanie kontroli nad siecią informacji elektronicznych • Dążenia państw do utrzymania dominującej pozycji na swoim terytorium w zakresie ładu informacyjnego i komunikacyjnego

Równolegle do batalii wokół jak największego, dyskrecjonalnego dostępu do globalnego zasobu informacji elektronicznych o ludziach, instytucjach i podmiotach państwowych zgromadzonych w przestrzeni cyfrowej nasila się walka o uzyskanie kontroli nad siecią komunikacji elektronicznej. W sposób bezpośredni wiąże się to z problemem granicy suwerenności państw i kwestią odpowiedzialności państwa za dane jego obywateli. Ranga tych zagadnień wzrasta wówczas, gdy pojawia się zagrożenie bezpieczeństwa informacyjnego, które stanowi przecież jeden z warunków bezpiecznego rozwoju państwa. W tej dziedzinie nasila się konfrontacja państw z pozapaństwowymi i komercyjnymi administratorami zasobów internetowych.

Początkowo rządy w dużej mierze nie doceniły wartości dostępu do danych zgromadzonych w cyberprzestrzeni i obecnie podejmują energiczne działania zmierzające do odzyskania swojej dominującej pozycji w świecie informacji. Współcześnie widać wyraźnie dążenia państw do ograniczania sytuacji, w których ład informacyjny i komunikacyjny dotyczący ich obywateli oraz podstawy funkcjonowania systemów istotnych dla bezpieczeństwa są wyznaczone przez zasady i rozwiązania (oprogramowanie i technologię) pozostające (bezpośrednio lub pośrednio) w gestii administracji podmiotów gospodarczych nadzorowanych przez inne kraje. Jednym z przykładów mogą być prowadzone przez Francję prace nad wdrożeniem wyszukiwarki Qwant jako alternatywy dla systemu Google. Trzeba jednak dodać, że proces odzyskiwania przez Francję rynku wyszukiwarek znajduje się w fazie wstępnej, czego ilustracją może

być porównanie 18 miliardów wyszukań w systemie Qwant w całym 2018 r. z 3,5 miliarda wyszukań dziennie w Google[5]. Nie znaczy to, że próby unarodowienia narzędzi komunikacji elektronicznej można uznać za epizodyczne. W rozgrywce o funkcjonowanie w cyberprzestrzeni państwa dążą przede wszystkim do tego, aby administratorzy mediów społecznościowych zaczęli ponosić odpowiedzialność za treści publikowane w ich globalnych sieciach. Jak dotychczas, mimo licznych dochodzeń, grzywien i nowych przepisów mających powstrzymać falę fałszywych informacji (*fake news*) i obraźliwych komentarzy w tych mediach, dążenia państw do zagwarantowania sobie wpływu na kształt internetowej oferty informacyjnej nie przynoszą większych efektów.

W najbliższym czasie będą się wzmagać starania różnych podmiotów o uzyskanie możliwie pełnego, w tym dyskrecjonalnego, dostępu do informacji zostawianych przez miliony ludzi w cyberprzestrzeni. Chodzi oczywiście o wykorzystywanie tych informacji do osiągania określonych celów, m.in. politycznych. W tym trwającym już dziś wyścigu biorą udział zwłaszcza operatorzy komunikacji internetowej, producenci środków komunikacji elektronicznej i poszczególne państwa. Zasób informacji zgromadzonych w przestrzeni elektronicznej staje się przedmiotem zainteresowania i manipulacji ze strony cyberprzestępców.

5.4. Nasilanie się systemowej inwigilacji komunikacji elektronicznej prowadzonej przez służby państwowe

Zjawisko globalnej i permanentnej inwigilacji elektronicznej prowadzonej na przemysłową skalę przez amerykańskie służby specjalne • Wzrost zapotrzebowania na świecie na stale doskonalone elektroniczne narzędzia inwigilacji i nadzoru • Rozwój maszynowego monitorowania przez władze państwowe zachowań obywateli w przestrzeni publicznej i w mediach społecznościowych

Za sprawą dokumentów ujawnionych przez Edwarda Snowdena opinia publiczna ujrzała poruszający obraz globalnej i permanentnej inwigilacji elektronicznej prowadzonej na przemysłową skalę przez amerykańskie służby specjalne. W świetle tych dokumentów nie można mieć wątpliwości, że służby te, w tym NSA (National Security Agency), prowadziły stale usprawnianą działalność zmierzającą do uzyskania za pomocą narzędzi elektronicznych dostępu do rozbudowanych metadanych o aktywności internetowej, a często również samych

[5] P. Szostak, *Stary kontynent w erze cyfrowej. Czy Polska odzyska technologiczną suwerenność?*, wyborcza.pl/naszaeuropa z 27.04.2019.

treści przekazywanych w ramach różnych form komunikacji (m.in. rozmów). Motywy ujawnienia przez Snowdena wspomnianych dokumentów są niejednoznaczne. (Mogło się nasuwać pytanie, kto za nim stoi…). Ich szczegółowe treści są wręcz sensacyjne[6]. Na potrzeby tej publikacji wypada jedynie stwierdzić, że służby specjalne podejmują skoordynowane działania polegające na zagwarantowaniu sobie, częstokroć przy użyciu rozwiązań balansujących na granicy legalności, dostępu do danych zgromadzonych w przestrzeni internetowej, w tym danych znajdujących się w zasobach mediów społecznościowych.

Ujawnione dokumenty dotyczyły sytuacji z przełomu pierwszej i drugiej dekady XXI wieku. Pokazują one, że służby specjalne USA, niejednokrotnie we współpracy z korporacjami mediów społecznościowych oraz we współdziałaniu ze swoimi odpowiednikami w innych państwach (w tym m.in. brytyjską służbą GCHQ – Government Communications Headquarters), stworzyły za pomocą różnorodnych programów mechanizmy permanentnej inwigilacji komunikacji elektronicznej milionów ludzi na świecie, w tym także obywateli amerykańskich. W 2012 r. przetwarzały one codziennie ponad 20 miliardów połączeń telefonicznych i internetowych na całym świecie. Dane pobierane z serwerów dziewięciu największych amerykańskich dostawców usług internetowych (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple) stały się efektywnym dopełnieniem danych pozyskiwanych z innych źródeł wywiadu elektronicznego (w tym przede wszystkim z nieautoryzowanych podłączeń do kabli światłowodowych i pozostałych elementów infrastruktury telekomunikacyjnej, z umieszczanego w komputerach złośliwego oprogramowania oraz z programów do łamania szyfrów).

Można zasadnie przyjąć, że ujawniona nielegalna aktywność służb specjalnych USA nie jest czymś wyjątkowym i podobne przykłady, rzecz jasna w różnej skali, dałoby się odnaleźć w innych państwach. O tym, że takie działania są prowadzone, świadczy stały wzrost zapotrzebowania na sukcesywnie doskonalone narzędzia inwigilacji i nadzoru przy wykorzystaniu komunikacji elektronicznej. Przewiduje się, że globalny popyt na ofensywne systemy cybernetyczne wzrośnie do 2027 r. o blisko 40% i osiągnie poziom 9,7 miliarda dolarów[7]. Obok Stanów Zjednoczonych i Wielkiej Brytanii czołowym dostawcą takiego sprzętu i oprogramowania jest Izrael, który pomimo krytyki ze strony organizacji zajmujących się ochroną praw człowieka złagodził w 2018 r. zasady eksportu ofensywnej broni cybernetycznej. Broń taka, produkowana m.in. przez NSO Group i Verint oraz Elbit Systems, pozwala włamywać się do urządzeń elektronicznych i niejawnie monitorować komunikację online.

---

6 Na ten temat zob. G. Greenwald, *Snowden. Nigdzie się nie ukryjesz*, Warszawa 2014.

7 https://www.reuters.com/article/us-israel-hackers-factbox/factbox-israel-a-global-leader-in-growing-market-for-cyber-weapons-idUSKCN1VC0Y4.

Według szczegółowych informacji zawartych w raporcie *Freedom on the Net 2019*[8], rządy licznych państw – i to nie tylko państw niedemokratycznych – coraz częściej kupują zaawansowane technologie do monitorowania swoich obywateli w przestrzeni publicznej i w mediach społecznościowych. Postępy w rozwoju narzędzi sztucznej inteligencji pozwalają szybko mapować aktywność użytkowników mediów internetowych, ustalać miejsca lokalizacji urządzeń oraz określać nastrój, poglądy polityczne, interakcje społeczne, orientację seksualną czy też wyznanie poszczególnych osób. Co najmniej 40 z 65 państw uwzględnionych w wymienionym wyżej raporcie ustanowiło zaawansowane programy monitorowania zachowań internautów w mediach społecznościowych. W 2019 r. w przypadku 15 państw z tej listy odnotowano znaczne inwestycje w sprzęt służący do nadzoru elektronicznego.

W przywołanym wyżej raporcie można odnaleźć informację, że w ramach przygotowań do targów sprzętu służącego do inwigilacji cyberprzestrzeni (w Dubaju w 2020 r.) chińska firma Knowlesys prowadziła pokazy instruujące, jak za pomocą jej produktów „monitorować wiadomości, profile, lokalizacje, zachowania, relacje i inne cele" oraz „monitorować opinię publiczną pod kątem wyborów". Oferowano sprzęt w przedziale cenowym od 1,5 miliona do 2,5 miliona dolarów pozwalający monitorować działania online populacji liczącej pięć milionów ludzi. Inna chińska firma, Semptian, reklamowała swój system nadzoru Aegis, jako „pełny widok wirtualnego świata" zapewniający możliwość „przechowywania i analizowania nieograniczonej ilości danych", który z powodzeniem jest wykorzystany do monitorowania ponad 200 milionów mieszkańców Chin.

W połowie 2019 r. głośna stała się sprawa instalowania przez chińskie służby graniczne oprogramowania szpiegującego (*spyware*) na telefonach turystów, którzy przekraczają granicę z Chinami w regionie autonomicznym Sinciang-Ujgur, graniczącym z Rosją, Tybetem, Mongolią i Afganistanem. Działania te miały ułatwić kontrolowanie ewentualnych kontaktów przybyszów z grupami muzułmańskimi w tym regionie. Jak zwykle w takich razach, władze usprawiedliwiały się pragnieniem zagwarantowania bezpieczeństwa[9]. Działania te stanowiły część szerszego systemu nadzoru za pomocą gromadzenia i analizy danych, w którym wykorzystuje się narzędzia sztucznej inteligencji[10].

---

[8] https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance.

[9] J. Snoch, *Chińskie służby graniczne instalują spyware na telefonach turystów*, serwis Onet.pl z 3.07.2019.

[10] https://www.reuters.com/article/us-china-xinjiang/more-secrets-of-chinas-xinjiang-camps-leaked-to-foreign-media-idUSKBN1XZ0DH.

Coraz więcej wiadomo o produkowanym przez izraelską firmę NSO specjalnym oprogramowaniu (znanym pod nazwą Pegasus), które służy do nieautoryzowanego przejęcia kontroli nad urządzeniami komunikacyjnymi i tym samym pozwala na niejawne śledzenie aktywności użytkowników tych urządzeń. Według licznych nieoficjalnych informacji produkt ten jest wykorzystywany także do użytku komercyjnego, w tym związanego z działaniami godzącymi w prawa człowieka[11]. Jak zawsze w takich sytuacjach, producenci sprzętu zapewniają, że w swojej działalności przestrzegają regulacji prawa międzynarodowego, zaś ich urządzenia szpiegowskie nie są wykorzystywane do nieuzasadnionych włamań do systemów komunikacji elektronicznej i służą wyłącznie do walki z najgroźniejszymi przestępstwami. Wypada dodać, że zespół badawczy CitizenLab z uniwersytetu w Toronto zidentyfikował ślady używania oprogramowania Pegasus także w Polsce. Z niepotwierdzonych ustaleń dziennikarzy jednej z komercyjnych stacji telewizyjnych wynika, że wspomniane narzędzie do inwigilacji zostało zakupione za kilkadziesiąt milionów złotych przez Centralne Biuro Antykorupcyjne[12].

5.5. Nowe zależności związane z elektronicznym zasobem danych

Zacieśnianie związków między technologią i polityką • Praktyczny wymiar politycznych zależności związanych z dostępem do zasobu danych elektronicznych • Elektroniczne chmury obliczeniowe jako problem państwowej suwerenności informacyjnej

Zagwarantowanie sobie wpływu na zasady i metody zarządzania stale powiększającym się zasobem informacji internetowych staje się nowym narzędziem budowania zależności o znaczeniu politycznym. Można więc mówić o ścisłym związku między technologią informacyjną i polityką. Decyzje producenta oprogramowania o blokadzie dostępu do jego produktów lub zmianie klucza wymaganego do uzyskania takiego dostępu, a także działania administratorów platform, na których są gromadzone elektroniczne dane, nabierają kluczowego znaczenia zarówno dla poszczególnych państw oraz instytucji, jak i dla osób prywatnych. W każdym przypadku dotyczy to bezpieczeństwa i dostępności danych przechowywanych w przestrzeni elektronicznej, które są wykorzystywane w coraz większym stopniu do obsługi infrastruktury publicznej lub gospodarczej, w tym także państwowej infrastruktury krytycznej.

---

11 https://www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ.

12 https://www.tvn24.pl/system-pegasus-i-pytania-do-cba-czarno-na-bialym,964972,s.html.

Problemy politycznych zależności związanych z dostępem do zasobu danych elektronicznych mają współcześnie wymiar praktyczny. Spór między Chinami i USA w sprawie technologii 5G skutkował zablokowaniem dostępu kolejnej generacji telefonów komórkowych produkowanych przez koncerny chińskie do oprogramowania dostarczanego przez amerykańskie firmy elektroniczne. Chodzi o to, że oprogramowania poszczególnych producentów nie można używać w żadnej innej infrastrukturze chmury bez istotnych modyfikacji, co sprawia, iż jego brak pociąga za sobą odcięcie od danych zgromadzonych w danej chmurze.

Rozwijająca się technologia chmur obliczeniowych (*cloud computing*) postawiła na nowo problem suwerenności informacyjnej[13]. Poważne wątpliwości w niektórych państwach wywołuje bowiem uzależnianie się, w ramach usługi hostingu, od zachowań administratorów tychże chmur w dziedzinie bezpieczeństwa danych elektronicznych. Trzeba dodać, że niejednokrotnie są to dane o istotnym znaczeniu dla interesów politycznych i gospodarczych. Żywa dyskusja na ten temat, połączona z propozycjami uruchomienia własnych projektów, wybuchła w 2019 r. w Niemczech. Stało się to po wydaniu przez niemiecki federalny organ ochrony danych opinii, że chmura Web Services Amazon jest podatna na szpiegowanie przez władze USA, które powołując się na wewnętrzne prawo amerykańskie (ustawę CLOUD), mogą uzyskać dostęp do poufnych danych rządowych o dużym znaczeniu dla interesów RFN, w tym informacji gromadzonych przez policję oraz danych objętych ochroną prywatności[14]. Kwestie te stały się przedmiotem debaty politycznej, w której dominuje przekonanie, że państwo powinno chronić swoje dane elektroniczne, w tym dane gospodarcze, przed uzależnieniem od zagranicznych dostawców chmury, zwłaszcza tych, którzy znajdują się poza zasięgiem prawa europejskiego. Spór o miejsce przechowywania danych cyfrowych nasila się wraz ze wzrostem świadomości znaczenia danych w rozwoju narzędzi sztucznej inteligencji. Coraz większym poparciem cieszy się projekt utworzenia europejskiego systemu usługi hostingu w chmurze o nazwie Gaia-X, w ramach którego poszczególne podmioty będą mogły przechowywać, przetwarzać i wymieniać dane[15].

---

13 G. Szpor (red.), *Internet. Cloud computing. Przetwarzanie w chmurach*, Warszawa 2013.

14 https://www.politico.eu/article/german-privacy-watchdog-says-amazon-cloud-vulnerable-to-us-snooping.

15 https://www.politico.eu/article/germanys-plan-to-control-its-own-data-digital-infrastructure.

5.6. Polityczny wymiar mikrotargetowania behawioralnego za pomocą danych internetowych

• Możliwości mikrotargetowania behawioralnego w prowadzeniu kampanii politycznych ujawnione przy okazji wyborów prezydenckich w USA w 2016 r. • Psychograficzne mikrotargetowanie jako sposób dopasowywania przekazu do konkretnej osoby na podstawie systemowej obserwacji jej zachowania w sieci • Sygnały o zmasowanej akcji internetowej dezinformacji związanej z brexitem

Wykorzystanie w okresie wyborów prezydenckich w USA w 2016 r. danych z komunikacji internetowej profilujących preferencje wyborcze użytkowników Facebooka pokazało możliwości mikrotargetowania behawioralnego w projektowaniu i prowadzeniu kampanii politycznych. Analitycy i specjaliści od kampanii wyborczych są w dużym stopniu zgodni co do tego, że na wybór Donalda Trumpa na urząd prezydenta USA wielki wpływ miało wykorzystanie przez jego sztabowców profili politycznych ponad 80 milionów wyborców. Istotne jest to, że te profile, jak ujawniły w marcu 2018 r. „The Observer" i „New York Times", były tworzone na podstawie danych pozyskanych od firmy konsultingowej Cambridge Analytica, śledzącej i analizującej wizerunki użytkowników Facebooka. Firma ta zajmowała się sporządzaniem profili psychologicznych wyborców i dobieraniem treści, które za pomocą zindywidualizowanej komunikacji masowej (blogów, filmików i reklam) były kierowane do internautów podatnych na określony sposób agitacji politycznej. Przed włączeniem się do kampanii prezydenckiej w USA spółka zbierała doświadczenia we wspomaganiu kampanii politycznych w innych krajach. Z dokumentów spółki publikowanych na anonimowym koncie na Twitterze, które – jak ustalono – należy do Brittany Kaiser, byłej dyrektor w Cambridge Analytica, wynika, że firma ta prowadziła działalność w 68 państwach, w tym w związku z wyborami w Malezji, Kenii i Brazylii[16].

Badania i śledztwa w sprawie wyborów amerykańskich w 2016 r. ukazują coraz lepiej sposób wykorzystywania techniki mikrotargetowania w kampaniach politycznych. Dobór treści i formy komunikatów politycznych odbywa się poprzez mikrotargetowanie psychograficzne, przekaz jest więc precyzyjnie dopasowywany do konkretnej osoby na podstawie systemowej obserwacji jej zachowania w sieci. Okazuje się bowiem, że – tak uważa większość analityków – istnieje związek między zachowaniami w sprawach treściowo bardzo odległych od polityki a wyborami i preferencjami politycznymi. Poddane odpowiedniej analizie zbiory danych psychograficznych dają obraz osobowości,

[16] https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation.

oczekiwań i lęków potencjalnych wyborców. Jest to możliwe tylko wówczas, gdy operuje się na zbiorach zawierających bardzo dużą liczbę zmiennych. Ułatwia to specjalistom opracowanie klucza, dzięki któremu agitacyjny przekaz dociera pod właściwy adres, oraz budowanie za pomocą przekazów komunikacyjnych siatki darczyńców[17].

Jak wynika ze śledztw prowadzonych w tych sprawach, dane, które w sposób systemowy wykorzystano w 2016 r. w sztabie wyborczym Donalda Trumpa, pochodziły z kont ponad 270 tysięcy użytkowników Facebooka. Dotyczyły osób, które pobrały aplikację quizu służącego w istocie do rozpoznania ich osobowości i – co w całym mechanizmie miało zasadnicze znaczenie – rejestrowania ich kontaktów na Facebooku[18]. Na tej podstawie, w ramach kolejnych kroków obejmujących analizę „polubień", uzyskano w sumie profile kilkudziesięciu milionów osób[19]. O poszczególnych użytkownikach tego medium społecznościowego zgromadzono w tym trybie do pięciu tysięcy informacji. Kierownictwo Cambridge Analytica nigdy nie przyznało się do naruszenia w tej sprawie prawa. Brytyjski kanał telewizyjny Channel 4 News wyemitował jednak nagrany ukrytą kamerą materiał, w którym dyrektor generalny Cambridge Analytica Alexander Nix otwarcie mówił o nieetycznych metodach działania swojej firmy w czasie zbierania informacji oraz o pracy na rzecz kampanii Trumpa. Po ujawnieniu omawianej tu afery oraz podaniu do publicznej wiadomości materiałów, które obnażyły mechanizm zdobywania, przetwarzania i wykorzystywania danych użytkowników Facebooka – bez informowania ich o tym, spółka uległa likwidacji. Liczne fakty związane z działaniem Cambridge Analitytica przedstawiły późniejsze obszerne publikacje skruszonych pracowników tej firmy[20].

Wykorzystanie danych osób korzystających z Facebooka naruszało prawa konsumentów. Gigantowi na rynku zindywidualizowanej komunikacji społecznej udało się przetrwać aferę związaną z nieprawidłowościami w zarządzaniu danymi użytkowników. Decyzją Federalnej Komisji Handlu (FTC) z 2019 r. Facebook został jednak ukarany grzywną w wysokości 5 miliardów dolarów za niedopełnienie obowiązku ochrony prywatności swoich użytkowników[21].

---

17 Zob. M. Kowalczyk, *Cyfrowe Państwo…*, s. 272 i nast., gdzie znajduje się również bogata baza źródeł na ten temat. Zob. też *Internetowy Frankenstein. Prof. Michał Kosiński o tym, jak nowoczesne metody marketingowe pozwalają wpływać na polityczne decyzje każdego człowieka*, rozmowa Jacka Żakowskiego z Michałem Kosińskim, https:www.polityka.pl/tygodnik polityka/społeczeństwo/1690344,4.

18 Dotyczy to aplikacji Facebooka o nazwie „This Is Your Digital Life", pozwalającej na przekazywanie pozyskiwanych danych.

19 https://www.politico.com/story/2019/07/12/facebook-ftc-fine-5-billion-718953.

20 Zob.: B. Kaiser, *Dyktatura danych. Kulisy działania Cambridge Analytica. Jak big data, Trump i Facebook zniszczyły demokrację i dlaczego może się to powtórzyć*, Warszawa 2020; C. Wylie, *Mindf*ck. Cambridge Analytica, czyli jak popsuć demokrację*, Kraków 2020.

21 B. Kaiser, *Dyktatura danych…*

Jak bowiem ustalono, kierownictwo spółki wiedziało o problemie naruszenia prywatności użytkowników od 2015 r. i nie zareagowało właściwie na ten problem. Kara została wymierzona w ramach ugody, co z jednej strony uchroniło kierownictwo Facebooka przed procesem sądowym, ale z drugiej strony świadczyło o tym, że zdawało sobie ono sprawę z procederu naruszania prywatności milionów osób; można zaryzykować tezę, że pośrednio było to przyznanie się do winy. Grzywna była jak dotąd największą karą egzekucyjną za naruszenia prywatności, „a według IAPP Westin Research Center jest to ponad dwukrotność łącznej liczby globalnych kar regulacyjnych w zakresie prywatności i bezpieczeństwa nałożonych w historii”[22].

Na marginesie trzeba zauważyć, że wysokość kary wywołała negatywne komentarze, uznano bowiem, że jest na tyle mała, iż po jej ogłoszeniu notowania finansowe Facebooka wyraźnie wzrosły. Powszechnie oczekiwano dalej idących restrykcji. Ujawniona korespondencja wewnętrzna pokazała, że Facebook zlekceważył obawy przed nielegalnym pozyskiwaniem i wykorzystaniem danych swoich użytkowników, które były zgłaszane w zespole korporacji już na wczesnym etapie kontaktów z Cambridge Analytica[23]. Wysokość kary stała się też w USA przedmiotem ostrego sporu politycznego. Politycy uznający ją za zbyt niską wskazywali, że swoimi działaniami Facebook zawiódł zaufanie swoich użytkowników i zszokował amerykańską opinię publiczną, a mimo to będzie mógł zachować nienaruszony swój model biznesowy. Krytycy ugody wskazywali również, że błędna jest decyzja FTC w sprawie nierozstrzygania o winie Facebooka oraz o zrzeczeniu się wszelkich przyszłych roszczeń z tytułu naruszeń popełnionych przez spółkę lub jej funkcjonariuszy od czerwca 2012 r.[24]. Podobny spór dotyczy też innych kar nakładanych przez FTC na koncerny internetowe, by przywołać tylko kontrowersje, jakie powstały po ukaraniu w 2019 r., w ramach ugody, Google (wraz z grzywną na rzecz stanu Nowy Jork – na łączną sumę 170 milionów dolarów) za naruszenie w serwisie YouTube prawa do prywatności dzieci. Dane osobowe dzieci były gromadzone bez zgody ich rodziców i wykorzystywane do precyzyjnego profilowania reklam kierowanych do tychże dzieci[25].

Specjaliści zajmujący się kampaniami politycznymi są w większości zgodni co do tego, że zmasowana akcja internetowej dezinformacji miała również zasadniczy wpływ na wynik głosowania w referendum w 2016 r. w sprawie brexitu. W tej akcji wykorzystywano szczegółową wiedzę o obawach – głównie

---

22 https://iapp.org/resources/article/iapp-infographic-ftc-facebook-vs-largest-global-privacy-and-security-fines.

23 https://www.theguardian.com/technology/2019/aug/23/cambridge-analytica-facebook-response-internal-document.

24 https://www.politico.com/story/2019/07/24/facebook-ftc-2020-democrats-1614722.

25 https://www.politico.com/story/2019/08/30/google-ftc-investigation-youtube-1479044.

politycznych – mieszkańców Wielkiej Brytanii związanych z dalszą obecnością ich państwa w Unii Europejskiej. W trakcie dochodzenia w sprawie Facebooka potwierdzono, że w sposób nieuprawniony przekazano z serwisu do firmy doradczej Cambridge Analytica dane około 2,7 miliona użytkowników z Unii Europejskiej. Dane te później wykorzystano do mobilizacji zwolenników brexitu, bez skrupułów grając na ich lękach przed napływem do państw Unii Europejskiej imigrantów.

Wypada w tym miejscu przypomnieć, że między liczbą głosów za pozostaniem w UE i jej opuszczeniem była stosunkowo niewielka różnica (48,1% do 51,9%), co nadaje praktyczne znaczenie zmasowanemu oddziaływaniu propagandowemu w tym referendum. Według informacji, których udzieliła wspomniana już Brittany Kaiser, firma Cambridge Analytica prowadziła w 2016 r. prace dla kampanii Leave.EU i Partii Niepodległości Zjednoczonego Królestwa (UKIP) na rzecz opuszczenia Unii Europejskiej. Podobne wnioski wynikają z przeprowadzonej w parlamencie brytyjskim analizy wewnętrznych e-maili między Cambridge Analytica a grupami politycznymi opowiadającymi się za wyjściem Wielkiej Brytanii z Unii Europejskiej. Ze źródeł tych wynika, że w ramach Leave.EU wykorzystano zbiory danych wytworzone przez Cambridge Analytica, mając na celu dotarcie do profilowanych uczestników referendum za pomocą odpowiednio dobranych wiadomości politycznych w internecie, oczywiście po to, aby potencjalnie oddziaływać na ich opinię[26].

Warto odnotować, że wraz z przeprowadzeniem w 2016 r. referendum nie zakończyło się wykorzystywanie narzędzi internetowych do kształtowania opinii politycznej w sprawie brexitu. Według ustaleń dziennikarzy śledczych, które zostały przedstawione w tekstach opublikowanych w połowie 2019 r., już po upadku gabinetu Theresy May, reklamy umieszczane na Facebooku w kampanii prowadzonej w 2018 r. przez Mainstream Network z inspiracji firmy Lyntona Crosby'ego (CTF Partners) miały wzmacniać poparcie w parlamencie dla „twardego" wyjścia Wielkiej Brytanii z Unii Europejskiej. Zgromadzono w czasie tej akcji adresy e-mail około miliona aktywnych odbiorców reklamy, które wykorzystano później do sygnowania anonimowej korespondencji elektronicznej inspirującej do wysyłania członkom Izby Gmin listów wzywających do opuszczenia Unii Europejskiej. Elizabeth Denham, brytyjska komisarz ds. informacji, uznała za wysoce prawdopodobne, że w ten sposób uruchomiono fałszywą kampanię oddolną, która miała sprawiać wrażenie, iż opinia publiczna w Wielkiej Brytanii opowiada się za takim rozwiązaniem. Jak ujawnił „The Guardian", cała akcja reklamowa online na Facebooku została wsparta wpłatą w wysokości jednego miliona funtów dokonaną przez nieznany podmiot. Denham ostrzegła, że utworzona baza danych dotyczących

[26] https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook.

osób zainteresowanych brexitem może być w przyszłości wykorzystywana do mikrotargetowania politycznego. Przemawiając na posiedzeniu komisji zajmującej się dezinformacją internetową, komisarz oświadczyła, że omawiany tu przypadek potwierdza, iż kampania polityczna „trwa 365 dni w roku i istnieją nowe sposoby zbierania danych", co należy uwzględnić przy organizacji kolejnych wyborów[27].

Sprawy obecności Wielkiej Brytanii w Unii Europejskiej stały się przedmiotem intensywnej kampanii internetowej prowadzonej także przez operatorów spoza tego kraju. Według informacji Katarzyny Kucharczyk z marca 2019 r., firma F-Secure, na podstawie analizy 24 milionów tweetów zawierających słowo „brexit", wysłanych z 1,65 miliona kont w okresie od 4 grudnia 2018 do 13 lutego 2019 r., stwierdziła próby ingerowania w debatę poprzez podejrzane działania. W większości przypadków intencją było wzmocnienie obozu zwolenników opuszczenia Unii przez Wielką Brytanię. Ustalono, że w ramach tych działań wysyłano niejednokrotnie z jednego źródła nawet sto tweetów na godzinę[28]. Temat zagranicznej ingerencji za pomocą kampanii internetowej w sprawy wyjścia Wielkiej Brytanii z Unii Europejskiej stał się w 2020 r. przedmiotem ostrego sporu politycznego. Premier Boris Johnson odrzucił sugestię, że na głosowanie Wielkiej Brytanii za opuszczeniem Unii Europejskiej wpłynęła rosyjska ingerencja, zaś grupa posłów do Izby Gmin domagająca się śledztwa w sprawie ingerencji rosyjskiej oskarżyła szefa gabinetu o blokowanie takiego śledztwa[29].

Rozwój wydarzeń, który doprowadził w grudniu 2019 r. do wyniku wyborczego dającego większość w Izbie Gmin zwolennikom opuszczenia przez Wielką Brytanię Unii Europejskiej, można – uwzględniając przy tym złożoność uwarunkowań sytuacji – traktować w dużej mierze jako potwierdzenie skuteczności oddziaływania na świadomość ludzi poprzez korzystanie z narzędzi komunikacji internetowej. Na tle opisywanej tu sprawy bardzo charakterystyczna jest wypowiedź jednego z byłych członków ścisłego kierownictwa Cambridge Analytica wyemitowana w filmie dokumentalnym pt. *Hakowanie świata*[30]. Stwierdził on, że likwidacja jego spółki nic w tej sprawie nie jest już w stanie zmienić. Skuteczność psychografii w walce politycznej okazuje się bowiem tak duża, że żadne przyszłe kampanie polityczne, w tym kampanie wyborcze, nie obędą się bez wykorzystania tej metody do identyfikowania,

[27] https://www.theguardian.com/politics/2019/apr/23/secretive-hard-brexit-facebook-campaign-got-1m-responses.

[28] https://cyfrowa.rp.pl/it/32361-brexit-skrajna-prawica-atakuje-na-twitterze.

[29] https://www.reuters.com/article/uk-britain-eu-johnson-russia/johnson-says-britain-was-not-influenced-by-russia-in-brexit-vote-idUSKCN24N1KR; https://www.theguardian.com/politics/2020/aug/21/mps-threaten-to-sue-boris-johnson-unless-he-acts-over-russian-meddling-in-uk-polls.

[30] *The Great Hack*, reż. Karim Amer, Jehane Noujaim, prod. USA 2019, Netflix.

opracowywania preferencji i pozyskiwania „przekonywalnych" niezdecydowanych, którzy rozstrzygają o wyniku tych kampanii.

Trzeba przyjąć, że cyfrowe mikrotargetowanie i spersonifikowane oddziaływanie przez podmioty polityczne dążące do zwiększenia swoich szans na powodzenie weszło już na trwałe do środków wykorzystywanych w prowadzeniu kampanii politycznych, w tym kampanii wyborczych. Najważniejsze w tej sytuacji jest nie tyle zablokowanie możliwości politycznego mikrotargetowania, ile wyeliminowanie z tych procedur patologii oraz metod wątpliwych etycznie, np. podstępnego zdobywania danych osobowych pozwalających ukierunkowywać przekaz i sposób oddziaływania. Kwestie te bezsprzecznie muszą być poddane szczegółowym regulacjom przez podmioty państwowe i ponadpaństwowe, w których powinny zostać ustalone standardy legalnego mikrotargetowania oraz mechanizmy interwencji w przypadku naruszenia tych standardów. Według ekspertów International Institute for Democracy and Electoral Assistance (International IDEA) istotne znaczenie mogą mieć w tym przypadku odpowiednio uzupełnione przepisy unijnego rozporządzenia o ochronie danych osobowych oraz przepisy prawa wyborczego. Szczególnie ważne staje się w tym kontekście zapewnienie przejrzystości internetowych reklam politycznych, co samo w sobie jest niezmiernie trudnym zadaniem[31].

5.7. Zagrożenia bezpieczeństwa danych osobowych zgromadzonych w cyberprzestrzeni jako wyzwanie dla rządzenia

Zagrożenie bezpieczeństwa internetowych danych osobowych • Obrót danymi internetowymi jako forma aktywności komercyjnej • Lista podejrzanych w sprawie manipulacji zasobem danych elektronicznych

Utrzymujące się na poziomie sprzętowym i sieciowym zagrożenie bezpieczeństwa danych osobowych zgromadzonych w przestrzeni internetowej jest problemem nabierającym coraz większego znaczenia politycznego. Nie sposób dokładnie określić skali wykorzystywania pozyskanych w sposób nieuprawniony wrażliwych danych osobowych pochodzących z internetu (a przynajmniej wykracza to poza ramy tego opracowania). Wiadomo, że wycieki danych są niejednokrotnie połączone z późniejszym ich wykorzystaniem w prowadzeniu różnych kampanii promocyjnych (również kampanii politycznych) oraz w działaniach przestępczych. Ataków hakerskich na zbiory danych dokonują

[31] https://www.idea.int/news-media/news/digital-microtargeting-%E2%80%93-challenges-european-regulators-0.

przeważnie cyberprzestępcy – w celu osiągania korzyści finansowych. Jednak pojawiają się również informacje (będzie o tym mowa w dalszych fragmentach książki), że za niektórymi tymi atakami stoją państwa.

Dla zilustrowania rozmiarów zjawiska wykradania danych internetowych można wspomnieć kilka najgłośniejszych takich przypadków z ostatnich lat. Przykładowo w 2014 r. z systemu Yahoo wypłynęły imiona, nazwiska, daty urodzenia, adresy e-mail i numery telefonów trzech miliardów użytkowników tego systemu. W latach 2014–2018 cyberprzestępcy mieli dostęp do danych osobowych ponad 500 milionów klientów sieci hoteli Starwood, które były przechowywane w systemie Marriott International. W 2016 r. wyciekły dane (gromadzone przez ponad 20 lat) przeszło 400 milionów osób korzystających z portalu Adult Friend Finder, który służy m.in. do wyszukiwania partnerów erotycznych. W 2018 r. hakerzy uzyskali dostęp do danych 29 milionów użytkowników Facebooka, przy czym w przypadku 14 milionów osób były to nie tylko podstawowe dane, ale także dane o miejscu zamieszkania i historii wyszukiwań w internecie[32]. Liczne włamania do zbiorów danych zarejestrowano w 2019 r. Forbes poinformował o kradzieży szczegółowych danych osobowych z 23 milionów kont użytkowników CafePress[33]. Equifax – amerykańska firma zajmująca się sprawozdawczością kredytową – przyznała, że hakerzy przejęli dane osobowe, w tym numery kart kredytowych 143 milionów Amerykanów[34]. Hakerzy uzyskali dostęp do danych osobowych ponad 100 milionów osób ubiegających się o kredyt w Banku McLean[35]. Z bazy danych agencji podatkowej w Bułgarii wyciekły nie tylko numery identyfikacyjne, adresy, nazwiska i dane o dochodach 4,66 milionów Bułgarów i poufne informacje 300 tysięcy podmiotów prawnych, ale także dane dotyczące płac, umów-zleceń, emerytur, środków finansowych otrzymywanych z zagranicy, ubezpieczeń zdrowotnych i rejestracji na stronach hazardowych (te ostatnie znajdowały się w zbiorze danych agencji bez wyraźnej podstawy prawnej)[36].

W niektórych wypadkach trudno jednoznacznie orzec, czy doszło „tylko" do zachowania niebezpiecznego czy już do zachowania nielegalnego. Istnieją przecież firmy, które zawodowo, w sposób legalny, trudnią się obrotem danymi pozyskanymi z zasobów internetowych i „wzbogacaniem" tych danych. O nieprzejrzystości sytuacji w tej dziedzinie może świadczyć następujący przypadek. Oto jesienią 2019 r. analitycy z firmy Data Viper, zajmującej się identyfikacją

32 https://tvn24bis.pl/ze-swiata,75/naruszono-bezpieczenstwo-niemal-50-milionow-kont-na-facebooku,872086.html.

33 https://iapp.org/news/a/data-breach-affects-23m-online-retailer-users.

34 https://www.politico.com/story/2017/09/07/equifax-hack-exposes-millions-data-242458.

35 https://www.cbsnews.com/news/capital-one-data-breach-2019-more-than-100-million-people-applying-for-credit-affected-today-2019-07-29.

36 https://www.polsatnews.pl/wiadomosc/2019-07-31/przez-wlamanie-do-systemu-podlewania-kwiatow-chcieli-zdestabilizowac-panstwo/?ref=kafle.

zagrożeń nowej generacji, odkryli zamieszczone na powszechnie dostępnym serwerze unikalne dane łącznie około 1,2 miliarda ludzi. Ten wyjątkowy zbiór, liczący ponad 4 terabajty, obejmował imiona i nazwiska, adresy, numery telefonów oraz profile z serwisów Facebook, Twitter, GitHub i LinkedIn. Były to informacje pozyskane w różnym czasie i z różnych źródeł. Zostały pogrupowane w sposób tworzący profile poszczególnych osób. Nie zawierały one tak wrażliwych danych, jak hasła czy numery rachunków bankowych. Niosły jednak ze sobą ryzyko agresji elektronicznej, tym bardziej że były to niejednokrotnie informacje na temat własności nieruchomości, sytuacji finansowej, aktywności politycznej, religijnej i społecznej. W trakcie postępowania wyjaśniającego trop doprowadził do firmy People Data Labs zajmującej się zawodowo przeszukiwaniem i porządkowaniem danych internetowych w celu późniejszej sprzedaży skonfigurowanych w ten sposób informacji o konkretnych osobach i instytucjach oraz przekazywaniem ich do drugiej, podobnej firmy: OxyData.io. Nie udało się jednak ustalić faktycznego właściciela końcowego zbioru danych. Nie trzeba chyba dodawać, że osoby, których zintegrowane dane dotyczyły, nic nie wiedziały o ich istnieniu w przestrzeni internetowej[37].

Największe firmy technologiczne na świecie próbują redukować lęk ludzi przed wykorzystaniem ich danych oraz przed śledzeniem ich zachowań w sieci, wprowadzając zasadę usuwania po pewnym czasie postów i tworząc procedury kasowania historii aktywności poszczególnych użytkowników komunikacji internetowej. Jak się jednak nieraz okazuje, są to w istocie wykluczenia danej informacji z obiegu w sieci, nie zaś z zasobu danych samych tych firm technologicznych, który stanowi przedmiot transferu do innych podmiotów.

Koncerny będące właścicielami mediów społecznościowych nierzadko musiały przyznać, że znajdujące się w ich dyspozycji zasoby danych osobowych nie są dostatecznie chronione. Przykładem może być Facebook, z którego zasobów wielokrotnie wyciekały dane osobowe. Korzystając z zestawienia dokonanego przez Urszulę Lesman, warto podać, że tylko we wrześniu 2019 r. dostępna była niezabezpieczona baza danych 419 milionów osób, zawierająca ID poszczególnych użytkowników portalu i ich numery telefonów, zaś podobna niezabezpieczona baza danych 267 milionów użytkowników została wykryta w grudniu tego samego roku. W 2018 r. hakerzy opublikowali prywatne informacje dotyczące 29 milionów użytkowników tego portalu społecznościowego[38].

Problem bezpieczeństwa zbiorów danych administrowanych przez firmy technologiczne – a tym samym niebezpieczeństwa utraty kontroli nad tymi danymi – staje się tym poważniejszy, że w tych zbiorach znajdują się rów-

[37] https://www.dataviper.io/blog/2019/pdl-data-exposure-billion-people/.

[38] https://cyfrowa.rp.pl/it/42613-facebook-idzie-na-rekord-wyciek-danych-267-mln-uzytkownikow?utm_source=rp&utm_medium=teaser_redirect; https://www.theguardian.com/technology/2019/sep/04/facebook-users-phone-numbers-privacy-lapse.

nież bardzo wrażliwe informacje osobiste. Przykładowo, firma DeepMind z Wielkiej Brytanii przetwarzająca, w ramach procedur uczenia maszynowego we współpracy ze służbą zdrowia, dane 1,6 miliona brytyjskich pacjentów, przeniosła w 2019 r. własne zasoby do Google, swojej spółki macierzystej (DeepMind Technologies Ltd zostało przejęte przez Google w 2014 r.)[39].

Podejrzenia o tworzenie narzędzi do pozyskiwania i nielegalnego wykorzystywania danych znajdujących się w obrocie elektronicznym bardzo często padają na producentów sprzętu i oprogramowania internetowego. Mocno ugruntowane jest przekonanie, że mają oni techniczne możliwości wyposażania swoich produktów w „tylne furtki" ułatwiające zdalny, nieuwierzytelniony dostęp do znajdujących się w ich zasięgu danych i że mogą instalować w swoich produktach sekretne oprogramowanie pozwalające na przejęcie pełnej kontroli nad funkcjonowaniem produkowanych narzędzi. To, w jakim stopniu korzystają z tych możliwości, stanowi przedmiot sporów. Jest rzeczą oczywistą, że odkrycie takiego tajemnego oprzyrządowania może prowadzić do kosztownych strat wizerunkowych, producenci sprzętu i oprogramowania muszą się zatem liczyć z ryzykiem ich poniesienia. Faktycznie pod ich adresem padają nieraz daleko idące zarzuty czy oskarżenia, mające niejednokrotnie podtekst polityczny.

Polityczny wymiar konfliktów na tle zagrożeń danych i zasad funkcjonowania sprzętu internetowego w związku z możliwością nieautoryzowanej ingerencji ze strony producenta tego sprzętu ilustruje – zasygnalizowany już we wcześniejszym fragmencie książki – amerykańsko-chiński spór z powodu sprzętu produkowanego przez chiński koncern Huawei, który nabrał ostrości na początku 2019 r. Na marginesie tego sporu warto zauważyć, że Amerykanie dobrze wiedzą z własnych doświadczeń, jakie możliwości daje wbudowanie do sprzętu komunikacyjnego elementów pozwalających uzyskać nieautoryzowany dostęp do treści przekazów telekomunikacyjnych. Na początku 2020 r. ujawniono trwający kilkadziesiąt lat proceder celowego osłabiania zabezpieczeń przez szwajcarską spółkę produkującą sprzęt szyfrujący kontakty telekomunikacyjne, jak się okazało zależną od CIA i – przez długi czas – od wywiadu niemieckiego. Służby USA i RFN nie miały trudności z przełamaniem tych zabezpieczeń szyfrowych. Sprzęt produkowany przez Crypto AG był sprzedawany do ponad 120 państw, gdzie wykorzystywano go do szyfrowania kontaktów dyplomatycznych, które w ramach operacji prowadzonej pod kryptonimem „Thesaurus", a następnie „Rubicon", były monitorowane przez CIA i BND (Bundesnachrichtendienst – Federalna Służba Wywiadu)[40].

---

[39] https://tech.wp.pl/google-przejmuje-piecze-nad-danymi-medycznymi-w-wielkiej-brytanii-6426544758924929a.

[40] https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/?itid=hp_rhp-top-table-main_crypto-730am%3Ahomepage%2Fstory-ans.

Wśród sprawców niejawnych ingerencji w internetowy zasób danych ważne miejsce zajmują służby publiczne poszczególnych państw. Podmioty te – zwłaszcza służby specjalne – prowadzą na wielką skalę przeszukiwania zasobów danych internetowych, uzyskując dostęp do wrażliwych informacji. Państwa od zawsze, przy użyciu różnorakich środków i procedur, zbierały i wykorzystywały informacje o zdarzeniach, zjawiskach oraz ludziach i strukturach instytucjonalnych. W tej dziedzinie instytucje państwowe tradycyjnie są uprzywilejowane, w niektórych obszarach wręcz mają one pozycję monopolistyczną.

Współcześnie władze publiczne stają wobec wyzwań związanych z faktem, że informacje, na których pozyskiwanie miały dotąd monopol, gromadzą także podmioty pozapaństwowe, które niejednokrotnie dysponują już nieporównywalnie większym zasobem danych niż one same. Jest to zmiana jakościowa. Rządzący muszą sobie w związku z tym zadać sporo pytań. Dwa z nich wydają się podstawowe. Po pierwsze, jest to pytanie o to, jak wykorzystać instrumenty władzy publicznej, w tym prawo, do monitorowania, standaryzacji i reglamentacji procesu pozyskiwania i wykorzystywania danych przez administratorów komunikacji internetowej oraz do ograniczenia pojawiających się w tej dziedzinie nieprawidłowości. Po wtóre, jest to pytanie o to, jak zagwarantować dostęp organów publicznych do danych zgromadzonych w zasobie cyfrowym mających znaczenie dla wykonywania zadań i obowiązków tych organów.

Praktyka ostatnich lat pokazuje, że służby publiczne wykorzystują do penetracji zasobów danych internetowych i nadzoru nad komunikacją elektroniczną skomplikowane programy, w tym wypracowane przez informatyków programy identyfikacji i rozpoznawania danych biometrycznych. Istnieją m.in. narzędzia do rozpoznawania twarzy na podstawie zdjęć zgromadzonych i opracowanych przez korporacje będące właścicielami mediów społecznościowych. Najczęściej działalność taka jest prowadzona na mocy rozszerzającej interpretacji nieprecyzyjnych przepisów prawa, z odwoływaniem się do potrzeby zapewnienia bezpieczeństwa publicznego i osobowego.

5.8. Nowy wymiar rozbieżności między wolnością a bezpieczeństwem w sferze danych internetowych, sztucznej inteligencji i upowszechnienia systemów nadzoru elektronicznego

Trudność wyboru między ochroną wolności, prywatności i bezpieczeństwa • Skok jakościowy w dziedzinie inwigilacji przez organy państwowe pod wpływem komunikacji internetowej i rozwoju inteligentnych technologii • Kontrowersje wokół doskonalenia narzędzi sztucznej inteligencji służących do rozpoznawania twarzy i głosu • Wzrost świadomości zagrożeń w sferze danych biometrycznych

W epoce komunikacji elektronicznej, stałego powiększania zasobu danych internetowych oraz rozwoju narzędzi sztucznej inteligencji pojawia się w nowej odsłonie klasyczny problem rozbieżności między wolnością a bezpieczeństwem. Toczy się spór o możliwości i sposób niwelowania tych rozbieżności. Z zasadniczych względów spór ten trudno jest jednoznacznie rozstrzygnąć. Nie ulega bowiem wątpliwości, że tam, gdzie w grę wchodzi kolizja dwóch podstawowych wartości, jakimi są wolność i bezpieczeństwo, a także konieczność uznania jednej z nich za wartość prymarną, podlegającą szczególnej ochronie, stajemy przed bardzo trudnym wyborem. Z jednej strony trzeba uwzględniać uwarunkowania wynikające z konsekwentnie rozbudowywanych gwarancji praw i wolności człowieka i obywatela. Z drugiej strony trzeba pamiętać, że informacje są jednymi z najważniejszych narzędzi do ochrony bezpieczeństwa państw oraz do walki z przestępstwami, trudno byłoby więc zrozumieć niewykorzystanie w tej walce posiadanych zasobów danych.

Wykorzystanie danych cyfrowych niejednokrotnie może ustrzec przed zdarzeniem o tragicznych skutkach. Przykładem na to są prewencyjne działania podjęte dzięki wejściu w posiadanie informacji na temat planowanych operacji terrorystycznych. Właściwe organy państwa niezaprzeczalnie muszą mieć możliwość prowadzenia w ściśle określonych ramach prawnych – z wykorzystaniem nowoczesnych narzędzi – inwigilacji polegającej na niejawnym pozyskiwaniu i zatrzymywaniu informacji w celu zapobiegania przestępstwom lub ich wykrycia oraz wskazania osób odpowiedzialnych za popełnienie przestępstw. Jednak poważnym problemem pozostaje w tym przypadku przestrzeganie zasad i granic prowadzenia inwigilacji.

W wyniku komunikacji internetowej i rozwoju inteligentnych technologii wzrosły do niespotykanych wcześniej rozmiarów możliwości inwigilacji prowadzonej także przez organy władzy państwowej. W związku z tym powstają warunki do – niekiedy drastycznego – naruszania granic prywatności człowieka. Obowiązujące w tym zakresie przepisy gwarancyjne, jak np. artykuł 8 Europejskiej Karty Praw Człowieka, nie stanowią już wystarczającej osłony przed nadużywaniem argumentu bezpieczeństwa do ingerencji w życie prywatne i nie są już skutecznym narzędziem ochrony danych osobowych przed niejawną, nieuzasadnioną i arbitralną penetracją. W tych sprawach pojawiają się bardzo rozbieżne interpretacje i dochodzi do licznych sporów prawnych sięgających szczebla Europejskiego Trybunału Praw Człowieka[41].

Ujawnione przez Edwarda Snowdena działania amerykańskich służb specjalnych pokazują, że inwigilacja jest niejednokrotnie prowadzona na granicy prawa lub wręcz z naruszeniem jego przepisów. Dzieje się tak zwłaszcza

[41] Szerzej zob. M. Szuniewicz, *Ochrona bezpieczeństwa państwa jako przesłanka ograniczenia praw i wolności jednostki w świetle Europejskiej Konwencji Praw Człowieka*, Warszawa 2016, s. 208 i nast.

w przypadku inwigilacji masowej oraz dyskrecjonalnego pozyskiwania metadanych charakteryzujących kontakty telekomunikacyjne. W związku z tym pojawia się problem polegający na tym, że ingerencja w prawa i wolności człowieka jest nieproporcjonalna w stosunku do potrzeby ochrony demokratycznych instytucji oraz bezpieczeństwa państwa i jednostek.

Systemowa inwigilacja elektroniczna prowadzona przez służby państwowe upowszechnia się w szybkim tempie i zaczyna być traktowana jako standardowe działanie. W przywołanym już wcześniej raporcie na temat wolności w internecie, przygotowanym przez amerykańską organizację Freedom House, zestawiono przykłady wskazujące, że dotyczy to w pierwszym rzędzie państw niedemokratycznych, w których prywatność obywateli nie stanowi wartości chronionej. Narzędzia sztucznej inteligencji służą w tych państwach coraz częściej do permanentnego nadzoru społecznego, a nierzadko także do ukierunkowywania działań represyjnych. Powołując się na konieczność przeciwdziałania zachowaniom patologicznym, władze państwowe w wielu przypadkach wykorzystują inteligentne technologie do obrony swoich interesów politycznych i zwalczania oponentów, w tym uczestników protestów społecznych.

Za modelowy – i zarazem zatrważający – przykład tego zjawiska można uznać nadzór elektroniczny w Chinach, o którego rozmiarach świadczy odkryta baza danych składająca się z regularnie aktualizowanych profili mediów społecznościowych, wiadomości i udostępnionych plików około 364 milionów chińskich użytkowników internetu[42]. Liczne przypadki niebezpiecznego kurczenia się sfery prywatności w warunkach cywilizacji cyfrowej stwierdzono w Rosji, państwach Bliskiego Wschodu, Afryki Północnej i Ameryki Południowej.

W raporcie *Freedom on the Net 2019* odnotowano takie przypadki również w państwach demokratycznych, w tym w Stanach Zjednoczonych, gdzie można było zaobserwować wzmożone wykorzystywanie narzędzi elektronicznych do inwigilacji imigrantów prowadzonej według niejasnych procedur. Trudno uznać za przypadek fakt, że także rządy państw demokratycznych naciskają na firmy technologiczne, aby te stwarzały im możliwości uzyskania dostępu do szyfrowanej korespondencji internetowej i dokumentów przechowywanych na smartfonach oraz innych urządzeniach cyfrowych, i rozważają wprowadzenie przepisów zmuszających te firmy do wykonywania takich zadań. Zazwyczaj władze uzasadniają swoje poczynania koniecznością poprawy bezpieczeństwa, śledzeniem potencjalnej działalności przestępczej i gromadzeniem dowodów w sprawach karnych[43].

Wątpliwości natury prawnej i moralnej dotyczące relacji – czy też, mówiąc wprost, kolizji – między ochroną bezpieczeństwa a gwarancjami praw człowieka

[42] https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance.

[43] https://www.politico.eu/article/encryption-facebook-apple-us-europe-law-enforcement.

budzą w ostatnim czasie narzędzia sztucznej inteligencji służące do rozpoznawania twarzy i głosu, stale doskonalone i stosowane na coraz większą skalę. Specjaliści zajmujący się ochroną danych osobowych są zgodni co do tego, że właśnie w tym obszarze dochodzi do szczególnie dotkliwych naruszeń prywatności, które w wielu przypadkach są związane z różnymi formami nadzoru[44].

Technologia identyfikacji personalnej na podstawie szablonu elektronicznego stworzonego w ramach biometrycznego obrazu indywidualnych cech fizycznych twarzy pozwala obecnie potwierdzać – za pomocą porównań – tożsamość osób. Administratorami największych zbiorów, liczących kilka miliardów wizerunków osób, są koncerny będące właścicielami mediów społecznościowych. Stale uzupełniane bazy spersonalizowanych zdjęć mają służby specjalne i policyjne oraz różnego rodzaju podmioty ochrony i rejestracji dostępu do określonych miejsc lub usług. Bardzo często w bazach danych następuje integracja wizerunków twarzy, odcisków palców i DNA. Niejednokrotnie na podstawie zebranego materiału zdjęciowego są podejmowane decyzje o kluczowym znaczeniu dla praw poszczególnych osób, i to w sytuacji, gdy – jak pokazują badania – technologia skanowania wizerunków nadal nie pozwala unikać błędów w identyfikacji tożsamości.

Do opinii publicznej napływają liczne sygnały, że kwestie rejestrowania, przechowywania i wykorzystywania danych biometrycznych, w tym głównie wizerunków twarzy, nie są w wystarczający sposób uregulowane, zaś praktyka postępowania w tym zakresie nie gwarantuje poszanowania praw i wolności człowieka, zwłaszcza prawa do prywatności. Przyczyn tego stanu rzeczy należy upatrywać w działaniach globalnych koncernów internetowych, które czują się właścicielami swoich zasobów. Można też wskazywać w tym zakresie na aktywność różnych służb państwowych, w tym przede wszystkim służb działających w dziedzinie bezpieczeństwa i porządku publicznego. Awaria Facebooka w lipcu 2019 r., która utrudniła użytkownikom dostęp do zamieszczonych w serwisie zdjęć, przy okazji ujawniła uprawiany w tym serwisie proceder. Internauci mogli bowiem zobaczyć, że do ich zdjęć są przypisane kody (tagi) wiążące fotografie z konkretnymi, wyraźnie zidentyfikowanymi użytkownikami[45].

Policja i służby bezpieczeństwa na całym świecie, w tym także w państwach Unii Europejskiej, coraz częściej korzystają z systemów rozpoznawania twarzy osób obecnych w przestrzeni publicznej i zaczynają traktować tę technologię jako swoje rutynowe narzędzie działania. W przygotowanym w 2019 r. przez Comparitech rankingu 50 krajów oceniającym przestrzeganie standardów wykorzystywania danych biometrycznych najgorzej wypadły Chiny – jako

[44] https://www.biometricupdate.com/202002/the-rise-of-facial-recognition-technology-where-we-are-and-what-to-expect.

[45] D. Maikowski, *Awaria Facebooka ujawniła, co serwis robi z naszymi zdjęciami*, Gazeta.pl 4.07.2019.

państwo mające najbardziej niepokojące, zagrażające prywatności regulacje. Kolejne niechlubne miejsca zajęły Malezja, Pakistan i Stany Zjednoczone (głównie w związku ze stosowaniem kontroli biometrycznej na lotniskach). Najmniej zastrzeżeń dotyczyło Irlandii i Portugalii[46].

Identyfikowanie obywateli za pomocą wizerunków internetowych ich twarzy i rozpoznawania głosu stało się standardową procedurą w działaniu władz państwowych w Chinach. W 2019 r. wprowadzono zasadę, że przy rejestracji nowego telefonu komórkowego obowiązkowa jest personalna identyfikacja właściciela i zgoda na zainstalowanie aplikacji pozwalającej władzom zeskanować twarz użytkownika telefonu. Rozwiązanie to zostało – jak zwykle w takich sytuacjach – umotywowane dążeniem do ochrony praw i interesów obywateli w cyberprzestrzeni[47]. W Chinach funkcjonuje zamknięty układ milionów kamer połączonych ze stale doskonalonym od 2014 r. państwowym systemem rozpoznawania twarzy. Jak podał w swoim raporcie Hubert Kozieł[48], liczbę takich kamer w Chinach szacowano w 2018 r. na około 200 milionów, zaś prognozy na 2020 r. mówiły już o 626 milionach kamer nadzoru. Z systemem współdziałają też miliony kamer przemysłowych. Państwo monitoruje przy użyciu tych narzędzi i mechanizmów zachowanie obywateli w przestrzeni publicznej. Kamery wchodzą w skład stale usprawnianego systemu „zaufania społecznego", który w praktyce służy totalnej inwigilacji zachowań w sieci internetowej oraz w przestrzeni publicznej. Mieszkańcy Chin podlegają permanentnej ocenie za pomocą punktów przyznawanych za poszczególne zachowania, w tym także punktów ujemnych za zachowania uznane za naganne, a nawet za utrzymywanie nieodpowiednich kontaktów. Od wyników tej oceny może być uzależnione uznanie danej osoby za „jednostkę zdyskredytowaną" i pozbawienie jej różnych praw. W 2019 r. poinformowano też, że w trakcie manifestacji ulicznych w Hongkongu policja stosowała systemy monitoringu pozwalające rozpoznać twarze uczestników zgromadzeń i na tej podstawie dokonywała później zatrzymań osób zidentyfikowanych w ten sposób[49].

Chiny stanowią skrajny przykład państwa stosującego narzędzia cyfrowe do nadzorowania społeczeństwa i pojedynczych osób. Cyfrowa identyfikacji

---

46 https://www.biometricupdate.com/201912/biometric-data-standards-in-50-countries-ranked-with-china-and-u-s-near-bottom.

47 https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users.

48 https://cyfrowa.rp.pl/globalne-interesy/42722-1984-w-2020-roku-rusza-system-totalnej-kontroli-miliarda-ludzi?utm_source=rp&utm_medium=teaser_redirect.

49 https://www.tvn24.pl/hongkong-i-chiny-wykorzystuja-nowoczesne-technologie-podczas-demonstracji,959099,s.html. O tym, że nowe technologie stanowią broń obosieczną, świadczy fakt, iż w czasie tych samych manifestacji ulicznych ich uczestnicy mogli za pomocą specjalnej aplikacji rozpoznać policjantów, którzy w ubraniach cywilnych podejmowali działania w tłumie protestujących.

biometryczna została tam wpisana w system tzw. społecznej i moralnej wiarygodności, który stał się istotnym instrumentem władczego zarządzania państwem. Urzędowe banki danych biometrycznych: wizerunków twarzy, obrazu tęczówki, odcisków palców, grupy krwi, DNA, próbek głosu są nieustannie uzupełniane, bez poinformowania o tym fakcie zainteresowanych ludzi przy ich kontaktach z instytucjami państwa oraz przy okazji korzystania ze świadczeń medycznych. Wraz z monitoringiem wizyjnym, kontrolą komunikacji i zasobów cyfrowych, elektroniczną rejestracją zdarzeń i informacjami pochodzącymi ze źródeł instytucjonalnych i osobowych, dane biometryczne stanowią podstawę zintegrowanej, interaktywnej bazy danych o osobach i zdarzeniach, która jest w Chinach filarem cyfrowego, ogólnopaństwowego panoptykonu. To „oczy oraz miecz partii i państwa".

Chiński system społecznej i moralnej wiarygodności opiera się na permanentnym i powszechnym monitorowaniu oraz rejestrowaniu w czasie rzeczywistym zachowań ludzi i zdarzeń połączonym z ich cyfrową identyfikacją i integracją wszystkich posiadanych przez państwo informacji oraz działań kontrolowanych przez państwo instytucji. System obejmuje zautomatyzowane weryfikowanie, wartościowanie, kwalifikowanie, pozycjonowanie zachowań ludzi i instytucji. Z jednej strony nagradza ludzi stosujących się do narzuconych standardów, z drugiej zaś – ostrzega, upomina i karze, w tym izoluje społecznie i wyklucza z dostępu do zasobów, usług publicznych i życia gospodarczego. Wartościowanie ludzi i kwalifikowanie ich do kategorii zróżnicowanych pod względem przysługujących im praw odbywa się w ramach systemu punktowego nagród i kar. Osoby uznane za niewiarygodne system ten pozbawia np. prawa do zakupu biletu na środki komunikacji, uniemożliwia im posłanie dziecka do lepszych szkół czy też zdobycie zatrudnienia. Karane są również osoby, które mimo ostrzeżenia utrzymują kontakty z ludźmi negatywnie ocenionymi. System skłania do wskazywania tych, którzy „zawiedli", i zakłada wywieranie na takie osoby społecznej presji, m.in. przez upowszechnianie ich wizerunków i danych personalnych oraz za pomocą aplikacji ostrzegających przed kontaktami z nimi. Celem jest zapewnienie autocenzury, samodyscypliny i autoblokady niepożądanych aktywności ludzi i instytucji – zgodnie z zasadą, że człowiek zagrożony i niepewny swojej sytuacji sam się najlepiej pilnuje i cenzuruje. Rozwiązania systemu znajdują się w fazie pilotażowego wdrażania z wykorzystaniem narzędzi cyfrowych i sztucznej inteligencji. Są one powiązane z działaniami propagandowymi i metodami sterowania opinią publiczną. Uzasadnia się je koniecznością ochrony interesów narodowych, tworzeniem silnego i stabilnego państwa oraz zapewnieniem harmonijnego rozwoju społecznego i „spełnianiem marzeń ludzi"[50].

[50] Zob. K. Strittmatter, *Chiny 5.0. Jak powstaje cyfrowa dyktatura*, Warszawa 2020.

Nadużywanie narzędzi cyfrowych do biometrycznej identyfikacji ludzi prowadzi do naruszeń prawa do prywatności także – jak już wspomniałem – w państwach demokratycznych. W połowie 2019 r. poważne naruszenie ochrony danych osobowych wykryto w systemie biometrycznym stosowanym przez banki, brytyjską policję i firmy ochroniarskie. Izraelscy badacze bezpieczeństwa Noam Rotem i Ran Locar bez trudu dotarli do odcisków palców, wizerunków twarzy i innych danych ponad miliona osób. Materiały te były zamieszczone w łatwo dostępnej bazie firmy ochroniarskiej odpowiedzialnej za internetowy system zamków biometrycznych. Badacze mogli ustalić w czasie rzeczywistym aktualną lokalizację tych osób w podlegających systemowi obiektach także poza Wielką Brytanią[51]. Według licznych doniesień Izrael używa metody rozpoznawania twarzy do śledzenia Palestyńczyków na Zachodnim Brzegu.

W Rosji, gdzie powszechnie praktykuje się w dużych miastach skanowanie rysów twarzy w systemie kamer ulicznych, zaplanowano wyposażenie policjantów w podręczne urządzenia służące do tego samego celu[52]. W styczniu 2020 r. uruchomiono w Moskwie system monitorowania biometrii twarzy na żywo za pomocą technologii wideo dostarczonej przez firmę NtechLab. System ten, którego wartość kontraktowa przekroczyła 3 miliony dolarów, może działać jednocześnie w setkach tysięcy kamer. Obecnie funkcjonuje już w nim 175 tysięcy kamer[53].

W niektórych państwach są prowadzone prace zmierzające do stworzenia ogólnokrajowego rejestru wizerunków ludzi zidentyfikowanych w komunikacji internetowej. Przykładem może być Australia, gdzie obowiązują już rozwiązania ustawowe pozwalające agencjom rządowym na dostęp do dokumentów tożsamości i zdjęć paszportowych. Na podstawie tych regulacji tylko w 2017 r. 100 agencji rządowych i 700 innych firm przeprowadziło ponad 30 milionów biometrycznej kontroli tożsamości za pomocą wizerunków elektronicznych[54]. W sytuacji coraz powszechniejszego korzystania z technik identyfikacji biometrycznej, w 2019 r. komisja parlamentarna do spraw egzekwowania prawa zaleciła rządowi ustanowienie organu nadzorczego zajmującego się bezpieczeństwem danych biometrycznych oraz zwiększenie przejrzystości programu rozpoznawania twarzy[55].

---

51 https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

52 https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it.

53 https://www.biometricupdate.com/202001/moscow-launches-live-facial-biometrics-surveillance-network-ntechlab-ceo-calls-worlds-largest.

54 https://www.theguardian.com/technology/2019/sep/29/plan-for-massive-facial-recognition-database-sparks-privacy-concerns.

55 https://www.biometricupdate.com/201904/committee-recommends-australia-set-up-biometric-data-security-oversight-body.

W Indiach, według danych z grudnia 2019 r., w ramach programu Aadhaar stanowiącego element systemu Unique Identity Authority of India (UIDAI), zgromadzone były identyfikatory biometryczne 1,25 miliarda mieszkańców. Codziennie wysyłano do tego systemu 30 milionów żądań uwierzytelnienia i wprowadzano od 300 do 400 tysięcy aktualizacji informacji. Przygotowywane są regulacje, które pozwolą na integrację kont Aadhaar z listą wyborców za pomocą legitymacji wyborczej ze zdjęciem[56].

Odrębnym problemem staje się fakt, że narzędzia gromadzenia i analizy wizerunków twarzy i próbek głosu są wykorzystywane nie tylko do identyfikacji personalnej i rozpoznawania aktywności poszczególnych osób, ale także do wartościowania tych osób pod kątem wybranych cech. Przykładowo, w Chinach opracowano technologię, która skanuje mimikę twarzy i działa jak wykrywacz kłamstw. System rozpoznaje kilkadziesiąt krótkich mimowolnych reakcji mimicznych i na tej podstawie rozstrzyga o prawdomówności osoby obserwowanej za pomocą kamery w smartfonie. Banki w Chinach zaczynają już w tym trybie weryfikować prawdomówność klientów starających się o kredyt. Ewentualne błędy maszynowe – prowadzące do mylnego podważenia wiarygodności poszczególnych osób – negatywnie odbijają się na ich żywotnych interesach[57].

Rośnie świadomość zagrożeń istniejących w sferze danych biometrycznych i pojawiają się próby ograniczenia dowolności działań w tej dziedzinie. W Unii Europejskiej planowano ograniczenie możliwości rozpoznawania tożsamości na podstawie zarejestrowanych rysów twarzy. Podejmowane są działania zmierzające do objęcia tych procedur przepisami unijnego rozporządzenia o ochronie danych osobowych. Krajowe organy ochrony prywatności, przykładowo Paul Wiles, brytyjski komisarz do spraw biometrii, podkreślają, że błędem jest pozostawienie decyzji w tych sprawach organom bezpieczeństwa, i postulują, aby wyraźnie określić w prawie sytuacje, w których korzyści publiczne związane z wykorzystaniem identyfikacji biometrycznej przeważają nad „znacznym naruszeniem prywatności jednostki”[58]. Powstają ruchy społeczne (np. organizacja Fight for the Future), które śledzą zagrożenia związane z rejestrowaniem wizerunków twarzy i rozpoznawaniem na tej podstawie tożsamości. W 2019 r. grupa użytkowników serwisu złożyła w sądzie w San Francisco pozew, w którym zażądano niemal 35 miliardów dolarów

---

56 https://www.biometricupdate.com/202002/indian-government-considers-linking-aadhaar-with-voter-records-as-biometrics-use-expands.

57 P. Szostak, *Chińskie banki skanują twarze klientów. Sprawdzają, czy mówią prawdę*, https://wyborcza.pl/7,156282,24115107,chinskie-banki-skanuja-twarze-klientow-sprawdzaja-czy-mowia.html.

58 https://www.theguardian.com/uk-news/2019/jun/27/watchdog-criticises-chaotic-police-use-of-facial-recognition.

za nielegalne gromadzenie danych biometrycznych w związku z wykorzystywaniem technologii rozpoznawania twarzy przy logowaniu się na konto na Facebooku[59]. Sąd podzielił zastrzeżenia osób skarżących, co otworzyło drogę do postępowań odszkodowawczych. Warto wspomnieć, że już ponad 10 lat temu stan Illinois, jako pierwszy w USA, wprowadził prawo chroniące dane biometryczne swoich obywateli[60].

Łatwość mechanizmów identyfikacji poprzez skanowanie wizerunków twarzy i próbek głosu powoduje, że państwa wykazują dużą wstrzemięźliwość we wprowadzaniu ograniczeń w korzystaniu z tych narzędzi. Janosch Delcker i Cristiano Lima w swoim raporcie w tej sprawie zwracają uwagę na to, że technologia skanowania twarzy, budząca wiele obaw o prywatność, jest traktowana przez rządy jako ważny instrument wykonywania zadań związanych z bezpieczeństwem. Prowadzi to do blokowania przepisów reglamentujących wykorzystywanie technologii rozpoznawania twarzy i w praktyce pozostawia kontrolę w tej dziedzinie firmom technologicznym i służbom specjalnym. Więcej sygnałów wskazujących na ewentualne zmiany sytuacji pochodzi z Unii Europejskiej niż z USA, chociaż i w Unii praktyka pozostaje w zgodzie z poglądem, że przy tworzeniu ewentualnych ograniczeń rozpoznawania twarzy należy wykazać znaczną ostrożność. Takie podejście rekomendowały m.in. organy nadzoru prywatności w Szwecji, we Francji i w Wielkiej Brytanii. W 2019 r. brytyjski sąd odrzucił „pierwszą poważną próbę ograniczenia policyjnego korzystania z rozpoznawania twarzy, twierdząc, że korzyści w zakresie bezpieczeństwa przeważają nad ryzykiem dla prywatności i wolności indywidualnych”[61]. Na początku 2020 r. okazało się, że Unia Europejska wycofuje się z wcześniejszych zapowiedzi wprowadzenia na okres przejściowy zakazu rozpoznawania twarzy osób przebywających w przestrzeni publicznej i zamierza tylko wypracować w tych sprawach bardziej klarowne zasady i standardy[62].

W praktyce najdalej idącą regulację odnośnie do stosowania metody identyfikacji na podstawie wizerunku twarzy wprowadzono w San Francisco – pierwszym mieście na świecie, które zakazało lokalnym agencjom korzystania z tej technologii. Ochronę elektronicznych danych osobowych zagwarantowało też prawo stanowe w Kalifornii, które weszło w życie 1 stycznia 2020 r. Mieszkańcy stanu otrzymali na mocy ustawy o prywatności duże możliwości ochrony swoich danych i informacji osobistych w internecie. Wprowadzono

[59] https://tvn24bis.pl/ze-swiata,75/facebook-nagrywal-i-udostepnial-probki-rozmow-z-messengera,961131.html.

[60] https://tvn24bis.pl/ze-swiata,75/facebook-serwis-moze-zaplacic-nawet-35-mld-dolarow-kary-sad-w-san-francisco-odrzucil-apelacje,961001.html.

[61] https://www.politico.eu/article/fight-against-facial-recognition-hits-wall-across-the-west.

[62] https://www.politico.eu/article/eu-considers-temporary-ban-on-facial-recognition-in-public-spaces; https://www.biometricupdate.com/202001/eu-no-longer-considering-facial-recognition-ban-in-public-spaces.

odpowiedzialność finansową za łamanie przyjętych zasad przez podmioty, których przychody brutto przekraczają w roku 25 milionów USD, a mają ponad 50 000 klientów, lub które uzyskają 50% albo więcej swoich rocznych przychodów ze sprzedaży danych osobowych konsumentów[63]. Dziś trudno wyrokować, jak te regulacje będą egzekwowane. Wielu komentatorów podkreśla, że regulacje chroniące dane osobowe przyjęte dwa lata temu w Unii Europejskiej są – jak dotychczas – słabo egzekwowane, gdyż podlegają bardzo różnym interpretacjom w państwach członkowskich, zaś prowadzone na ich podstawie dochodzenia znacznie się przeciągają[64].

[63] https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do.

[64] https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605.

Rozdział szósty

Cyfrowy wymiar suwerenności. Globalna rywalizacja w dziedzinie nowych technologii komunikacyjnych i cyfrowych

6.1. Sztuczna inteligencja jako fundament kształtującego się porządku technologiczno-informacyjnego świata

Nowe możliwości technologii informatycznych przesłanką rewizji zasad, zakresu przedmiotowego i procedur decydowania publicznego • Stały postęp badań w dziedzinie biotechnologii i fizjologii człowieka • Zwiększanie się zdolności algorytmów i mechanizmów uczenia maszynowego • Urealnianie wizji zintegrowanego inteligentnego świata cyfrowego • Jakościowy rozwój multimedialnych technologii telekomunikacyjnych • Ekspansja internetu rzeczy • Zaawansowane prace nad rozwiązaniami internetu ciał • Społeczny wymiar rozwoju sztucznej inteligencji

W świetle tego, co wiemy o relacjach między polityką i rządzeniem a ich otoczeniem, słuszne wydaje się założenie, że pojawianie się nowych możliwości technologii informatycznych i transformacja cyfrowa dokonująca się z wielką szybkością we wszystkich dziedzinach życia muszą prowadzić do rewizji zasad, zakresu przedmiotowego i procedur decydowania publicznego. Nie miejsce tu na referowanie trwającej już od połowy poprzedniego wieku historii programów i urządzeń sztucznej inteligencji[1], niezbędne jest jednak zasygnalizowanie głównych kierunków zmian w tej dziedzinie, które mają wpływ na decydowanie publiczne.

Na skutek rozwoju cywilizacji internetowej i inteligentnych technologii elektronicznych to, co jeszcze niedawno było wyłącznie treścią książek i filmów o tematyce fantastycznonaukowej, przenika do świata rzeczywistego. Od

[1] Na ten temat zob. J. Kaplan, *Sztuczna inteligencja…*, s. 29 i nast. Zob. też: T. Zalewski, *Definicja sztucznej inteligencji*, w: M. Świerczyński, L. Lai (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, s. 1 i nast.; A. Krasuski, *Status prawny sztucznego agenta. Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2021.

zbudowania w latach 1943–1945 na Uniwersytecie Pensylwanii w Filadelfii na potrzeby armii USA pierwszego urządzenia, które jest uznawane za komputer (ENIAC – Electronic Numerical Integrator and Computer), jakościowe i coraz szybsze zmiany są stałym elementem obrazu świata technologii. W okresie między powstaniem tego ważącego 30 ton urządzenia zasilanego ponad 17 tysiącami lamp[2] a chwilą obecną zbudowano mikrokomputer, utworzono sieci komputerowe, narodził się i upowszechnił internet, pojawiły się telefony komórkowe, rozbudowano nowe technologie łączy szerokopasmowych, stworzono systemy chmur z danymi przechowywanymi w nich przez miliony użytkowników, opracowano i wdrożono liczne aplikacje otwierające nowe możliwości działania człowieka. Korzystanie z tych urządzeń jest współcześnie dla ogromnej – i szybko rosnącej – rzeszy ludzi niezbędnym i oczywistym elementem ich życia. Stale zwiększa się liczba urządzeń i systemów nabywających zdolności autonomicznego funkcjonowania oraz doskonalenia swoich możliwości w ramach uczenia maszynowego[3]. Kierunek poszukiwań modelu integracji człowieka z komputerem wskazuje zaprezentowany już przez Neuralink (firmę założoną przez miliardera Elona Muska) projekt połączenia ludzkiego mózgu z interfejsem komputera. Projekt ten zakłada, że dzięki cybernetycznemu wszczepowi będzie można kontrolować elektroniczne urządzenia za pomocą myśli[4]. Naukowcy z Korean Advanced Institute of Science and Technology (Korea Południowa) i Uniwersytetu Kolorado w Boulder (USA) skonstruowali urządzenie, które jest w stanie kontrolować obwody nerwowe za pomocą niedużego implantu mózgowego zarządzanego smartfonem. Urządzenie to pozwala podawać leki magazynowane w wymiennych wkładach, a także stosować terapię światłem skierowaną do konkretnych neuronów. Może pomóc w leczeniu chorób Parkinsona, Alzheimera, uzależnień, depresji i bólu. Rozwiązanie zostało z powodzeniem przetestowane na myszach i przechodzi w fazę zastosowań klinicznych[5].

Postęp widoczny w kolejnych projektach sztucznej inteligencji pozwala z dużym prawdopodobieństwem oczekiwać ziszczenia się towarzyszącej człowiekowi od dawna idei inteligentnych maszyn. Zaawansowane są badania w zakresie biotechnologii i fizjologii człowieka, w których dogłębnie analizuje się i opisuje mechanizmy myślenia i inteligencji, dzięki czemu wiadomo o nich coraz więcej. Prowadzone są intensywne prace zmierzające do zrozumienia i wykorzystania mechanizmów układu nerwowego w funkcjonowaniu inteli-

---

2 M. Juza, *Między wolnością a nadzorem…*, s. 11.

3 M. Pudełko, *Prawdziwa historia internetu na świecie*, Piekary Śląskie 2020.

4 https://www.polsatnews.pl/wiadomosc/2019-07-17/komputer-sterowany-za-pomoca-mysli-elon-musk-chce-rozpoczac-testy-na-ludziach/?ref=kafle.

5 https://www.rp.pl/Nowe-technologie/190809554-Powstalo-urzadzenie-do-kontrolowania-mozgu-smartfonem.html.

gencji człowieka, pamięci skojarzeniowej oraz do kształtowania modeli, które potrafią za pomocą numerycznej algorytmizacji odtwarzać i powielać w świecie informatyki relacje charakterystyczne dla sieci neuronów w organizmach żywych. Trwają prace nad stworzeniem scalonych systemów neuromorficznych wzorowanych na działaniu ludzkiego mózgu, które mają być zdolne do uczenia się na doświadczeniach. Intensywne badania mają m.in. rozwikłać jedną z największych ludzkich zagadek, jaką jest pamięć. Neurobiolodzy badają już możliwości „zhakowania" naszej pamięci.

Poszukiwania w dziedzinie sztucznej inteligencji zmierzają już nie tylko do odtworzenia możliwości człowieka, ale także do przekroczenia tych możliwości w różnych obszarach, tam gdzie ujawniają się deficyty – np. mentalnego „uposażenia" czy funkcjonowania – istoty ludzkiej. Dziś to jeszcze „pieśń przyszłości", zbyt wiele zdolności człowieka, w tym zwłaszcza w sferze myślenia oraz inteligencji emocjonalnej, jest barierą, której nie są w stanie przekroczyć współczesne maszyny – roboty. Warto jednak pamiętać, że zmiany w tej dziedzinie zachodzą szybko, choć mogłoby się wydawać, iż od pierwszych prób i eksperymentów dzielą nas lata świetlne (a przecież, od czasu, kiedy za pomocą połączenia między pierwszymi komputerami udało się 29 października 1969 r. przesłać pierwszą wiadomość elektroniczną, minęło niewiele ponad 50 lat). Idea symulowania inteligentnego działania człowieka przez maszyny, która została w 1956 r. przedstawiona przez Johna McCarthy'ego, informatyka z Uniwersytetu Stanforda, twórcę terminu „sztuczna inteligencja", w kolejnych latach owocuje już praktycznymi projektami.

Zdaniem coraz większego grona badaczy, droga dalszego rozwoju sztucznej inteligencji nie musi się sprowadzać do poszukiwania sposobów sztucznego powielania zdolności człowieka. Przykład samochodów autonomicznych Google'a i Tesli pokazuje, że doskonalenie programów komputerowych może pójść inną drogą, na której można uzyskać podobne wyniki. Jak zauważa Yuval N. Harari, takie pojazdy wykonują bez problemu wszystkie czynności związane z techniką i bezpieczeństwem jazdy, „nie czując przy tym ani odrobiny strachu", „bez żadnej świadomości"[6].

Algorytmy są stale doskonalone. Już w 1996 r. komputer Deep Blue zwyciężył szachowego mistrza świata Garriego Kasparowa. W lutym 2015 r. program DeepMind opracowany przez Google'a sam nauczył się grać w 49 gier na Atari. W następnych latach oprogramowanie (AlphaGo) nauczyło się grać w skomplikowaną chińską grę planszową *go*, a drużyna baseballu Oakland Athletics, ukształtowana za pomocą algorytmów, jako pierwsza w ponadstuletniej historii ligi wygrała 20 meczów z rzędu. Algorytmy zaczęły zarządzać – bez ludzkiego nadzoru – milionami taksówkarzy w korporacji Uber. Program

[6] Y.N. Harari, *Homo deus. Krótka historia jutra*, Kraków 2018, s. 148.

komputerowy EMI (Experiments in Musical Intelligence), stworzony przez Davida Cope'a z University of California w Santa Cruz, został przez niego użyty do komponowania utworów naśladujących styl największych twórców w dziejach muzyki – m.in. J.S. Bacha, Beethovena i Chopina; produkcje te spotkały się z krytycznym odbiorem specjalistów, ale publiczność ulegała złudzeniu, że słucha autentycznych dzieł Bacha…[7]. Wreszcie – warto wspomnieć, że badania przeprowadzone na zlecenie Google'a i Facebooka na ponad 80 tysiącach ochotników, którzy mają konto na Facebooku i wypełnili stupunktowy kwestionariusz osobowościowy, wykazały, że algorytm Facebooka był „lepszym znawcą ich osobowości i skłonności niż (…) znajomi, rodzice czy małżonkowie"[8].

Zaawansowane prace nad stworzeniem zintegrowanego inteligentnego świata cyfrowego przy wykorzystaniu multimedialnych technologii telekomunikacyjnych kolejnej generacji mają już wymiar praktyczny. Chińska firma Huawei, działająca w ponad 170 krajach i zatrudniająca ponad 180 tysięcy pracowników, ogłosiła w kwietniu 2019 r. debiut platformy sztucznej inteligencji Atlas przygotowanej do zastosowania komercyjnego[9]. Zaoferowano liczne rozwiązania, które mogą być wykorzystane w realizacji różnych procesów logistycznych, koncepcji inteligentnych miast oraz w systemach komunikacyjnych, energetycznych i bankowych. Podstawą tych rozwiązań jest ogromna moc obliczeniowa architektury Da Vinci 3D Cube. Moduł akceleracji systemu Atlas 200 mieści się w przestrzeni o wielkości zaledwie połowy karty kredytowej. Umożliwia analitykę wideo HB w czasie rzeczywistym w 16 kanałach. Może być podłączony do zróżnicowanych urządzeń końcowych, w tym aparatów, robotów i dronów. Daje możliwość programowania wieloscenariuszowych projektów. Stacja końcowa systemu Atlas 500 pozwala na przetwarzanie do 16 TOPS INT 8, zużywając mniej niż 1 KWh dziennie. Może działać w środowisku od minus 40 do plus 70 stopni Celsjusza. To ważny etap w tworzeniu sieci powszechnych komputerów inteligentnych z innowacyjnymi chipami. Trwają intensywne prace nad stworzeniem kwantowej łączności satelitarnej wykorzystującej komputery kwantowe, dające niespotykane dotąd możliwości obliczeniowe[10].

Ideę zintegrowanego inteligentnego świata cyfrowego urealniają jakościowe przekształcenia multimedialnych technologii telekomunikacyjnych. Przepustowość obecnych sieci LTE (*long-term evolution*) zaliczanych do telefonii czwartej generacji (4G) wynosi zwykle 1 do 2 Gb/s. Technologia mobilna piątej generacji (5G) to już przepustowość na poziomie minimum 20 Gb/s,

[7] Szerzej na ten temat tamże, s. 406–412.
[8] Tamże, s. 431.
[9] Serwis informacyjny PAP z 19.04.2019.
[10] https://cyfrowa.rp.pl/technologie/43250-to-on-zmienia-chiny-w-kwantowe-supermocarstwo.

co daje możliwość obsługiwania w ramach jednej sieci do miliona urządzeń na jednym kilometrze kwadratowym. Otwiera się droga do tworzenia aplikacji rozszerzonej i wirtualnej rzeczywistości. W raporcie Ericsson Mobility ogłoszonym w 2019 r. prognozowano, że w 2024 r. liczba użytkowników sieci 5G wyniesie 1,9 miliarda i że technologia ta znajdzie się w zasięgu 45% ludności świata. Oznacza to ogromne zmiany w różnych dziedzinach aktywności ludzi, a także instytucji, w których potrzebny jest szybki transfer danych w sieciach mobilnych[11]. Wszystkie te okoliczności powodują, że – jak nadmieniam w innych fragmentach książki – udział w budowie sieci 5G jest przedmiotem ostrego sporu między państwami. Spór ten ma już obecnie charakter geopolityczny. Tymczasem pojawiają się kolejne informacje wskazujące, że trwają prace zmierzające do budowy sieci 6G. Jak poinformował w 2019 r. Wang Xi, chiński wiceminister nauki i technologii, Chiny traktują te prace jako jeden z ważnych priorytetów. O potrzebie takich prac pisał także w lutym 2019 r. na Twitterze prezydent Donald Trump. Z kolejną odsłoną sieci komunikacji internetowej ma się wiązać transfer danych przy wykorzystaniu częstotliwości liczonych w terahercach i fal radiowych krótszych niż 1 mm[12].

W fazie rozwoju znajduje się internet rzeczy (*internet of things*, IoT)[13], którego podstawą są rozwiązania pozwalające gromadzić i przekazywać dane przez poszczególne przedmioty. Powstaje cywilizacja autonomicznych urządzeń. Funkcjonujące w tym obszarze rozwiązania wychodzą poza zakres tzw. inteligentnych domów i znajdują zastosowanie w projektach tzw. inteligentnych miast, m.in. w postaci sterowania infrastrukturą komunikacyjną miasta, oraz inteligentnych systemów przeznaczonych do wykorzystania w różnych dziedzinach życia i działach gospodarki, np. systemów energetycznych. Już teraz sieć internetu rzeczy liczy miliony elementów, a ocenia się, że w trzeciej dekadzie XXI wieku będzie to 20 miliardów przedmiotów. Sieć ta zawiera w rozproszonych systemach przetwarzania oraz zbiorach zintegrowanych w serwerach chmurowych informacje o życiu ludzi i różnych formach ich aktywności.

Jak zauważa Kevin Kelly, „w nadchodzących dekadach niemal każdy wytwarzany przedmiot będzie zawierał niewielki krzemowy chip, który będzie połączony z internetem", co więcej – „34 miliardy urządzeń z dostępem do internetu, które planujemy dodać do chmury w ciągu następnych 5 lat, będą zbudowane tak, żeby strumieniować dane i (…) je przechować", a „wszyst-

---

11 www.ericsson.com/en/press-releases/2019/6/ericsson-mobility-report-5g-uptake-even-faster-than-expected.

12 https://cyfrowa.rp.pl/telekomunikacja/41336-chiny-szykuja-sie-do-lacznosci-6g-to-niewyobrazalne-transfery-danych?utm_source=rp&utm_medium=teaser_redirect.

13 Zob.: M. Sikorski, A. Roman (red.), *Internet rzeczy*, Warszawa 2020; M. Miller, *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa, 2016.

ko, co będzie miało kontakt z chmurą i będzie mogło być monitorowane, na pewno będzie monitorowane”[14]. Uzyskanie dostępu do tej sieci ma nie tylko wymiar informacyjny, może bowiem prowadzić do zdalnego sterowania przez operatora, który włamał się do systemu, urządzeniami o podstawowym znaczeniu dla bezpieczeństwa i życia ludzi[15]. Możliwe problemy dobrze ilustruje dość epizodyczny przypadek inteligentnego odkurzacza firmy iRobot, który zbierał dane i przetwarzał je w plan pomieszczenia, gdzie był używany, a następnie przekazywał te informacje do producenta sprzętu[16].

W szybkim tempie rozwija się internet ciał (*internet of bodies*, IoB), w ramach którego człowiek podłączony bezpośrednio do sieci permanentnie generuje i przekazuje do adresatów w sieci informacje i sam odbiera sygnały z tej sieci. W systemie internetu ciała ogniwem sieci zostaje tzw. człowiek biocyfrowy, który np. na bieżąco przesyła dane o stanie swojego zdrowia lub swoim zachowaniu i automatycznie odbiera sygnały elektroniczne, w tym sygnały motywujące do określonych działań lub wręcz te działania stymulujące[17]. Jednak perspektywa powszechnego stawania się ludzi elementami sieci internetowej wydaje się, z powodu zróżnicowania poziomu rozwoju cywilizacyjnego, jeszcze mało realna. Nadal blisko jeden miliard mieszkańców Ziemi nie ma dostępu do energii elektrycznej, wielu ludzi nie ma dostępu do internetu, w tym internetu szerokopasmowego, albo korzysta z łączy internetowych sporadycznie. Za to w wymiarze technologicznym perspektywa internetu ciał jest już jak najbardziej wyobrażalna. Co więcej, jeśli postęp w poznaniu mechanizmów świadomościowych człowieka będzie się dokonywał w takim tempie, jak w ostatnich latach, realne staje się pozyskiwanie za pomocą rozwiązań internetu ciała wiedzy o zamiarach poszczególnych ludzi. Nie trzeba dodawać, jakie to może mieć znaczenie dla sprawowania nadzoru nad życiem ludzi w przyszłości, także w kwestiach dotyczących bezpośrednio polityki.

Sygnały o próbach wdrażania rozwiązań integrujących mechanizmy internetu rzeczy i internetu ciała coraz liczniej napływają z aglomeracji miejskich w Chinach, Korei Południowej, Wielkiej Brytanii, USA i z Dubaju. Realną wizję „przywiązania ludzi do sieci” przedstawił w lutym 2020 r. Norbert Biedrzycki, opisując trwające już przygotowania do przyjęcia nowych zasad funkcjono-

---

14 K. Kelly, *Nieuniknione…*, s. 350–351.

15 J. Krawiec, *Internet rzeczy (IoT). Problemy cyberbezpieczeństwa*, Warszawa 2020.

16 https://cyfrowa.rp.pl/globalne-interesy/36935-odkurzacz-ktory-zbiera-nasze-dane?utm_source=rp&utm_medium=teaser_redirect. Zob.: G. Szpor (red.), *Internet rzeczy. Bezpieczeństwo w Smart city*, Warszawa 2015; J. Surma (red.), *Hakowanie sztucznej inteligencji*, Warszawa 2020.

17 Zob. A. Olsztyński, T. Sroczyński, M. Frąk, R. Kozielski, *Internet ludzi. Organizacja jutra*, Warszawa 2018.

wania jednej z dzielnic Toronto[18]. Według tego samego źródła, w Quayside, w ramach prowadzonego wraz z koncernem Google eksperymentu, planuje się pełne zintegrowanie życia ludzi z technologiami komputerowymi i internetowymi. Ma to być nowa jakość w ucyfrowieniu przestrzeni publicznej, która „będzie mocno nasycona wszelkimi urządzeniami, które będą tworzyły globalną sieć informacyjną, a jej ogniwami będą kamery, stacje WiFi, autonomiczne pojazdy, smartfony, komputery użytkowników, czujniki i wszelkie urządzenia elektroniczne, które można do takiej sieci podłączyć i zintegrować ich działanie”[19]. Na podstawie danych zbieranych od mieszkańców „inteligentne urządzenia będą sortować odpady, regulować temperaturę chodnika i temperaturę w budynkach użyteczności publicznej, a także dbać o to, by ruch drogowy cechował się idealną płynnością”. Warto dodać, że „odpowiednikiem dowodu osobistego będzie specjalne konto elektroniczne czy elektroniczna portmonetka, dzięki której jej użytkownik będzie mógł ‘podłączać’ się do miejskiej sieci urządzeń i korzystać z wszelkich udogodnień, takich jak np. rezerwacja miejsca w restauracji, leżaka na nabrzeżu, samochodu w wypożyczalni czy zakup biletu na samolot”[20]. Autor cytowanej publikacji zwraca uwagę na problemy i zagrożenia związane z omawianym eksperymentem. Słusznie stawia pytanie, czy nie jest to pomysł na „dobrowolne więzienie”, i sygnalizuje, że już na wstępnym etapie projektu pojawia się kwestia zarządzania danymi, które będą się odnosić do cyfrowych śladów zachowań ludzi. Dla jednych jest to przerażająca perspektywa, dla innych – przejaw nieograniczonej przedsiębiorczości i innowacyjności pozwalającej zwiększyć efektywność wykorzystania zasobów materialnych i finansowych. Trzeba się zgodzić z opinią zawartą w referowanej tu publikacji, zgodnie z którą eksperyment z Toronto stanowi sygnał starcia dwóch różnych cywilizacji.

Zmiany składające się na szybki rozwój sztucznej inteligencji oraz budowę zintegrowanej, globalnej sieci internetowych połączeń ludzi i przedmiotów mają tylko pozornie charakter ściśle technologiczny. Postęp dokonujący się w tej dziedzinie modyfikuje stan i zasady funkcjonowania społeczeństwa. Przeobrażenia, które obecnie zachodzą, wykraczają poza stosunki gospodarcze, ekonomiczne, handlowe. Mają wymiar polityczny. Wyznaczają nową perspektywę rywalizacji – ubieganie się o przywództwo technologiczne na świecie. Powodują, że od własności (w znaczeniu posiadania dóbr materialnych) ważniejsze staje się zagwarantowanie sobie dostępu do zbioru danych.

---

18 https://businessinsider.com.pl/technologie/nowe-technologie/inteligentne-miasta-odwazny-eksperyment-w-kanadyjskim-toronto/750bz68.

19 Tamże.

20 Tamże.

6.2. Cyberprzestrzeń jako obszar nasilającej się konkurencji i konfrontacji między państwami

Uzależnianie pozycji państwa od poziomu rozwoju sztucznej inteligencji • Skokowy wzrost zaangażowania państw i grup państw w rozwój inteligentnych technologii • Nasilanie się walki konkurencyjnej o prymat w projektach dotyczących sztucznej inteligencji • Otwarty konflikt na tle nowych technologii cyfrowych między USA i Chinami • Poszukiwanie własnej strategii w sprawach nowych technologii telekomunikacyjnych w Unii Europejskiej i w poszczególnych państwach

Dostęp do nowych technologii, w tym przede wszystkim technologii, które można wykorzystać w konflikcie militarnym, zawsze stanowił istotne uwarunkowanie prestiżu i roli państwa na arenie międzynarodowej. Współcześnie jednak mamy do czynienia z sytuacją z gruntu odmienną od dotychczasowych doświadczeń, oto bowiem inteligentne technologie cyfrowe zyskują rangę kluczowego czynnika, który współkształtuje ład geopolityczny. Zdobycie przez państwo dominującej pozycji w sferze technologii cyfrowych w drugiej dekadzie XXI wieku zapewnia mu – być może na długie lata – przewagę w układzie międzynarodowym. Dlatego jesteśmy świadkami wyścigu technologicznego, a nawet – nowej odsłony technologicznej zimnej wojny. Ale to tylko jeden – budzący uzasadniony lęk – aspekt rozwoju technologicznego.

Ludzie uświadamiają już sobie, że sztuczna inteligencja to „przemysł przyszłości", który będzie odgrywał ważną – w niektórych przypadkach być może decydującą – rolę w wielu dziedzinach życia. Sztuczna inteligencja może stanowić narzędzie wspomagające produkcję i zarządzanie w licznych gałęziach gospodarki, może być używana w programach z zakresu obronności, w medycynie, usługach publicznych i w rozwiązaniach usprawniających życie codzienne ludzi, może się przyczyniać do przyspieszenia wzrostu gospodarczego i być wykorzystywana w działaniach na rzecz ochrony środowiska. Nic więc dziwnego, że trwa zaciekła rywalizacja w doskonaleniu technologii i narzędzi cyfrowych, w tym sztucznej inteligencji.

Poszczególne państwa i grupy państw angażują się coraz bardziej w rozwój prac nad inteligentnymi technologiami. Według danych z 2019 r., już prawie 40 państw opracowało krajowe strategie sztucznej inteligencji[21]. Zwykle są to polityczne dokumenty programowe o zróżnicowanym stopniu szczegółowości. Poza zagadnieniami regulacyjnymi obejmującymi różne aspekty bezpieczeństwa, które przedstawiam w dalszej części książki, elementami wspólnymi tych

[21] https://www.oecd-opsi.org/projects/ai/strategies/. Tam też można znaleźć syntetyczne omówienie strategii państw OECD, do którego odwołuję się w dalszym fragmencie książki, oraz linki do wybranych dokumentów prezentujących te strategie.

dokumentów są kwestie preferowanych kierunków, sposobów prowadzenia i mechanizmów finansowania badań oraz prac wdrożeniowych i edukacyjnych w dziedzinie sztucznej inteligencji. Co ważne, w państwowych dokumentach programowych problematyka sztucznej inteligencji zyskuje charakter ponadsektorowy, a działania w tej dziedzinie są uważane za warunek dalszego postępu cywilizacyjnego i wzrostu gospodarczego.

Centralne miejsce w rozwoju inteligentnych technologii przypisuje się w dokumentach strategicznych władzom państwowym. Niejednokrotnie przewiduje się tworzenie specjalnych rozwiązań instytucjonalnych wspomagających działania programowe. We wszystkich strategiach dużo miejsca poświęca się promowaniu digitalizacji i otwartości w dysponowaniu danymi publicznymi. Bardzo często jako mechanizm rozwoju sztucznej inteligencji wskazuje się partnerstwo publiczno-prywatne. Państwa aspirujące do przewodzenia w rozwoju sztucznej inteligencji traktują osiągnięcie tego celu jako ogólnonarodowe wyzwanie, a w patronowanie poszczególnym projektom angażują się przedstawiciele najwyższych szczebli władzy.

W USA rozwój sztucznej inteligencji określono jako zadanie strategiczne o zasadniczym znaczeniu dla pozycji i bezpieczeństwa państwa. Wspomaganie inwestycji w innowacyjne technologie, które służą rozwojowi narzędzi sztucznej inteligencji i robotyki, odbywa się przede wszystkim poprzez finansowe wsparcie prac prowadzonych przez podmioty prywatne. Pierwotny plan strategiczny w tej dziedzinie został opracowany przez administrację Baracka Obamy w 2016 r. Dofinansowanie państwowe z lat 2017–2018 wyniosło ponad 4 miliardy dolarów. W lutym 2019 r. ogłoszono nową inicjatywę zmierzającą do włączenia w prace rozwojowe wszystkich struktur rządowych, nadając tym pracom status narodowego planu strategicznego[22]. Jako priorytety wskazano inwestowanie w badania dotyczące sfery gospodarczej, wzmocnienie zasobów otwartego rządu oraz przygotowanie kadr dla prac nad sztuczną inteligencją. W ramach nowelizacji programu (*The AI Initiative*) podkreślono znaczenie partnerstwa publiczno-prywatnego. Prezydent Donald Trump powiązał utrzymanie przez USA pozycji światowego lidera technologii z bezpieczeństwem gospodarczym kraju. Aby poprawić aktywność wszystkich urzędów federalnych w obszarze prac rozwojowych nad sztuczną inteligencją, powołano specjalne struktury o charakterze koordynacyjnym[23]. W sprawach rozwoju nowych technologii panuje w USA zgoda między wszystkimi siłami politycznymi. W czasie kampanii wyborczej w 2020 r. kandydujący na urząd prezydenta z ramienia Demokratów Joe Biden zapowiedział, że „kamieniem węgielnym" jego prezydentury będą inwestycje w badania i rozwój, pozwalające Stanom

[22] https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf.

[23] https://www.politico.com/story/2019/02/13/trump-executive-order-artificial-intelligence-1160345.

Zjednoczonym „przewodzić w dziedzinie innowacji", i stanowczo stwierdził, że nie ma żadnych powodów, aby USA pozostawały pod względem zaawansowania technologii 5G i sztucznej inteligencji w tyle za Chinami lub innym państwem[24].

W Chinach działania związane z rozwojem sztucznej inteligencji mają status całościowego programu narodowego. Wpisano je w ogólny plan zdobycia przez państwo rangi mocarstwa informatycznego i jednoznacznie powiązano z działaniami na rzecz zagwarantowania bezpieczeństwa wewnętrznego i zewnętrznego Chin. Kierunki myślenia władz politycznych o tych sprawach wskazują już dokumenty z 2014 r. Przykładem może być wystąpienie Xi Jinpinga 27 lutego 2014 r. na pierwszym posiedzeniu Centralnej Grupy Kierowniczej do spraw Problematyki Informatycznej, w którym przywódca Chin stwierdził m.in., że „Bezpieczeństwo informatyczne i zastosowanie technologii informacyjnych stanowią jedno z najważniejszych zagadnień strategicznych, dotyczących bezpieczeństwa i rozwoju kraju oraz pracy i życia obywateli. Powinniśmy zatem w oparciu o sytuację międzynarodową i wewnętrzną nakreślić kompleksowe plany, koordynować poczynania wszystkich zainteresowanych stron, stymulować innowacyjny rozwój oraz pracować wytrwale, celem przekształcenia Chin w mocarstwo informatyczne. (…) Zadaniem długofalowym jest też dążenie do tego, aby opinia publiczna korzystająca z systemów informatycznych była zdrowa. Powinniśmy doprowadzić do innowacji i do propagandy informatycznej, informacji podawanej za pomocą środków informatycznych i wykorzystywać zasady łączności internetowej, aby promować zagadnienia całościowe i pozytywne, a także upowszechniać i stosować w praktyce podstawowe wartości socjalistyczne. (…) Bez zapewnienia bezpieczeństwa informatycznego nie możemy też zagwarantować bezpieczeństwa narodowego"[25].

W przyjętym w Chinach w 2017 r. obszernym dokumencie zatytułowanym *Plan rozwoju nowej generacji sztucznej inteligencji*[26] wyrażono opinię, że szybki rozwój sztucznej inteligencji głęboko zmieni życie ludzkie, zasady funkcjonowania społeczeństw i relacje między państwami na świecie oraz stanie się przedmiotem międzynarodowej konkurencji i podstawowym narzędziem rozwoju gospodarczego. Jasno wyznaczony cel to zapewnienie Chinom do 2030 r. dominującej pozycji w obszarze sztucznej inteligencji. W tzw. mapie drogowej, czyli harmonogramie działań prowadzących do tego celu przyjęto, że do 2020 r. nastąpi w Chinach zsynchronizowanie ogólnej technologii i zastosowania sztucznej inteligencji na światowym poziomie, do 2025 r. sztuczna inteligencja stanie się główną siłą napędową modernizacji przemy-

[24] Zob. manifest programowy J. Bidena opublikowany w „Foreign Affairs". Cyt. za przekładem opublikowanym w „Magazynie Świątecznym" „Gazety Wyborczej" z 1 sierpnia 2020 r.

[25] Xi Jinping, *Innowacyjne Chiny*, Warszawa 2015, s. 214–216.

[26] http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

słowej i transformacji gospodarczej Chin, zaś do 2030 r. teoria, technologia i zastosowanie sztucznej inteligencji osiągną w Chinach najwyższy światowy poziom i państwo stanie się największym na świecie centrum innowacji w tym zakresie.

W dokumencie z 2017 r. omówiono kierunki działań w poszczególnych obszarach związanych z cyfryzacją. Przedstawiono m.in. koncepcję „inteligentnego rządu" i systemu usług cyfrowych oraz plan wykorzystania narzędzi sztucznej inteligencji do podejmowania przez podmioty publiczne decyzji, w tym opracowywania programów i strategii oraz dokonywania ocen polityki, reagowania w sytuacjach kryzysowych, wzmacniania bezpieczeństwa publicznego, prognozowania potrzeb publicznych oraz interakcji między rządem a społeczeństwem. Elementem programu stała się integracja danych rządowych.

W opracowanym w 2018 r. rządowym planie działania obejmującym lata 2018–2020 zarysowano jego rozwiązania instytucjonalne, funkcjonalne i finansowe. Jako naczelną zasadę przyjęto synergiczne współdziałanie rządu, stanowiącego centrum aktywności w sprawach rozwoju inteligentnych technologii, z podmiotami władzy i administracji na wszystkich poziomach podziału terytorialnego państwa. Zapowiedziano długoterminowe wsparcie projektu przy wykorzystaniu wszystkich dostępnych zasobów i szczegółowe monitorowanie uzyskiwanych wyników, w tym zwłaszcza w zakresie tworzenia rozwiązań nowej generacji oraz osiągania synergii między działalnością naukową, edukacyjną i przemysłową. Jako jeden z kierunków wskazano promowanie pełnego, wielozadaniowego i wysokowydajnego integrowania działania w sferze wojskowej i cywilnej.

Założenia, na których opiera się plan cyfryzacji, są w Chinach konsekwentnie spełniane. Tylko w 2017 r. wydano w tym kraju w ramach programu rozwoju sztucznej inteligencji 28 miliardów dolarów. Jest rzeczą znamienną, że w realizacji programu inwestycji w dziedzinie sztucznej inteligencji uczestniczą bardzo aktywnie podmioty regionalne i lokalne. Jak poinformowano w 2019 r., programy i wydatki dotyczące sztucznej inteligencji zostały zaplanowane w 19 prowincjach i regionach Chin[27].

Chiny zabiegają o to, aby uzyskać maksymalny wpływ na systemy koordynacji sztucznej inteligencji w jak największej liczbie państw. W ofercie firm chińskich znajduje się cała infrastruktura niezbędna do utworzenia i rozwijania systemów AI. Dotyczy to m.in. kamer, algorytmów rozpoznawania twarzy i narzędzi eksploracji danych. O tym, jak wielkie są chińskie wpływy w dziedzinie systemów AI, świadczy fakt, że – według raportu FutureGrasp – we wrześniu 2019 r. w aż 64 państwach działały pochodzące z Chin syste-

[27] https://www.politico.com/story/2019/07/18/global-translations-ai-china-1598442.

my nadzoru AI. Były to w większości państwa, które po dopuszczeniu takich systemów zrezygnowały z alternatywnych źródeł technologii w tym zakresie[28].

Kwestiom związanym z rozwojem sztucznej inteligencji nadaje się priorytet także w niektórych innych państwach pozaeuropejskich. Przykładem mogą być Indie i Korea Południowa. W narodowej strategii Indii na rzecz sztucznej inteligencji z czerwca 2018 r. za cel przyjęto zbudowanie całościowego ekosystemu sztucznej inteligencji, widząc w nim motor wzrostu gospodarczego, czynnik sprzyjający wyzwalaniu aktywności społecznej, ograniczaniu zjawiska wykluczenia społecznego oraz umacnianiu pozycji państwa na arenie międzynarodowej. Wskazano na odpowiedzialność rządu za stworzenie podstaw informacyjnych, koordynację i finansowe wspomaganie projektu oraz za innowacyjną i proaktywną transformację sektora publicznego. W Korei Południowej w ramach realizowanej obecnie pięcioletniej strategii nowych technologii zapowiedziano inwestycje w badania i rozwój na łączną kwotę 1,7 miliarda euro. Wyraźnie określono cel, którym jest ugruntowanie pozycji Korei Południowej jako lidera w dziedzinie sztucznej inteligencji. Strategia koncentruje się na zadaniach związanych z kształceniem kadr, opracowaniem i finansowaniem dużych projektów w obszarze zdrowia, bezpieczeństwa publicznego i obrony, inwestowaniem w infrastrukturę oraz rozwojem gospodarczym w sektorze prywatnym[29].

W Unii Europejskiej udział państw członkowskich w rozwijaniu sztucznej inteligencji uznano za nadrzędne zadanie o strategicznym znaczeniu. W wydanym w kwietniu 2018 r. komunikacie Komisji Europejskiej („Sztuczna inteligencja dla Europy") wskazano na potrzebę wspólnych działań służących zwiększeniu zdolności i stopnia wykorzystania narzędzi sztucznej inteligencji w sektorze prywatnym i publicznym. Podkreślono znaczenie zasadniczego zwiększenia poziomu inwestycji w inteligentne technologie oraz partnerstwo publiczno-prywatne na szczeblu krajowym i międzynarodowym. Zapowiedziano utworzenie centrum wsparcia prawnego i technicznego, promowanie udostępniania danych i wyników badań, ułatwienia dla specjalistów i podmiotów instytucjonalnych rozpoczynających działalność w sferze sztucznej inteligencji oraz podkreślono znaczenie opracowania i przestrzegania w tej dziedzinie standardów etycznych i prawnych. W komunikacie Komisji Europejskiej uznano, że europejskie podejście do sztucznej inteligencji powinno mieć na uwadze trzy cele: po pierwsze – zwiększenie potencjału technologicznego i przemysłowego UE oraz wdrożenie sztucznej inteligencji w całej gospodarce, zarówno w sektorze prywatnym, jak i publicznym; po drugie – przygotowywanie się na zmiany społeczno-gospodarcze wywołane przez sztuczną inteligencję; po

[28] https://www.atlanticcouncil.org/blogs/new-atlanticist/toward-digital-power-over-states.
[29] https://www.oecd-opsi.org/projects/ai/strategies.

trzecie – zapewnienie odpowiednich ram etycznych i prawnych. Wśród zadań z drugiego obszaru wskazano na „sprzyjanie modernizacji systemów kształcenia i szkolenia, wspieranie talentów", a także „antycypowanie i wspieranie zmian na rynku pracy oraz przystosowanie systemów ochrony socjalnej"[30].

W końcu 2018 r. ogólna strategia na rzecz rozwoju sztucznej inteligencji znalazła w Unii Europejskiej konkretyzację w planie skoordynowanych działań państw członkowskich oraz Norwegii i Szwajcarii w obszarze zwiększenia inwestycji, udostępnienia danych, wspierania najlepszych inicjatyw i zapewnienia zaufania. Jednoznacznie potwierdzono dążenia, by Europa odrobiła straty i stała się światowym liderem w zakresie „rozwoju i wdrażania najnowocześniejszej, etycznej i bezpiecznej sztucznej inteligencji"[31].

W budżecie Unii Europejskiej, w programie Horyzont 2020 przeznaczono na wsparcie rozwoju sztucznej inteligencji 1,5 miliarda euro. W programie „Cyfrowa Europa" w perspektywie finansowej na lata 2021–2027 na wsparcie inwestycji w tej dziedzinie planuje się wydatkować co najmniej 7 miliardów euro. Założonym celem jest przeznaczenie w Europie do końca 2020 r. co najmniej 20 miliardów euro na inwestycje prywatne i publiczne w sztuczną inteligencję i zapewnienie w kolejnych latach inwestycji na poziomie ponad 20 miliardów euro rocznie[32].

Po ukształtowaniu w 2019 r. nowej Komisji Europejskiej, Unia Europejska podjęła inicjatywę w sprawie technologii cyfrowych. W dokumentach programowych dano wyraz dążeniu do uzyskania przez Europę strategicznej pozycji w dziedzinie transformacji cyfrowej i sztucznej inteligencji. Działania z tym związane wpisano do zasadniczych priorytetów na kolejne lata[33]. Przewodnicząca i członkowie Komisji Europejskiej w swych wystąpieniach wyrażają przekonanie, że istnieją przesłanki ku temu, aby Europa stała się liderem świata cyfrowego, zaś wypracowane w niej standardy cyfrowe uzyskały status ogólnoświatowych wzorów do naśladowania[34]. W unijnej linii programowej eksponuje się dążenie do zachowania przez ludzi kontroli nad transformacją cyfrową. W lutym 2020 r. opublikowano białą księgę zamierzeń związanych

---

30 COM(2018) 237 final, https://ec.europa.eu/transparency/regdoc/rep/1/2018/PL/COM-2018-237-F1-PL-MAIN-PART-1.PDF

31 COM(2018) 795 final, https://ec.europa.eu/knowledge4policy/publication/coordinated-plan-artificial-intelligence-com2018-795-final_en.

32 https://ec.europa.eu/poland/news/181207_ai_pl; https://europa.eu/rapid/press-release_MEMO-18-6690_en.htm. Zob. też M. Makowska, *UE wobec rozwoju sztucznej inteligencji*, „Biuletyn PISM" 2019, nr 12 (1760).

33 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en.

34 *Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, Brussels, 19.2.2020, COM(2020) 64 final.

z kształtowaniem cyfrowej przyszłości Europy[35], rozwojem i standaryzacją sztucznej inteligencji oraz odzyskaniem wpływu podmiotów europejskich na gospodarkę danymi internetowymi[36]. Pojawił się motyw technosuwerenności europejskiej. Projekt obejmuje wytężone działania w płaszczyźnie normatywnej, finansowej, technologicznej i edukacyjnej. Postęp w zakresie technologii cyfrowych powiązano z realizacją zadań rozwojowych, poprawą warunków życia i pracy ludzi, zapewnieniem bezpieczeństwa oraz ochroną środowiska naturalnego[37]. Celem kształtowania cyfrowej przyszłości Europy ma być wspieranie otwartego i demokratycznego społeczeństwa oraz dynamicznej i zrównoważonej gospodarki.

W stanowisku ogłoszonym przez Komisję Europejską w lutym 2020 r. pojawiają się informacje na temat kalendarza działań i podstawowych wskaźników. Są to jednak tylko ogólne zapowiedzi, mające charakter wezwania programowego. Świadczy to o tym, że władze unijne zdają sobie sprawę z wagi problemu zapóźnienia technologicznego Unii Europejskiej. Wciąż brakuje rozwiązań wypracowanych na poziomie operacyjnym, jednak sam fakt, że w Unii wzrosło zrozumienie tego, iż nie da się zagwarantować silnej pozycji Europy w układzie globalnym bez istotnego postępu w dziedzinie technologii cyfrowych, należy ocenić pozytywnie. W ramach powiązania technologii cyfrowych z warunkami życia ludzi zapowiedziano w ogłoszonych dokumentach w szczególności następujące zadania: inwestowanie w kompetencje cyfrowe Europejczyków; stworzenie ochrony ludzi przed zagrożeniami cybernetycznymi (takimi jak hakowanie, *ransomware* i kradzież tożsamości); zagwarantowanie, że w rozwoju sztucznej inteligencji będą szanowane prawa ludzi; przyspieszenie wdrażania ultraszybkiego internetu szerokopasmowego w domach, szkołach i szpitalach; zwiększenie wykorzystania komputerów nowej generacji na rzecz innowacyjnych rozwiązań dla medycyny, transportu i środowiska. W ramach kształtowania uczciwej i konkurencyjnej gospodarki cyfrowej zapowiedziano: promowanie innowacyjnych przedsiębiorstw typu start-up; przygotowanie ustawy o usługach cyfrowych w celu zwiększenia odpowiedzialności za platformy internetowe i wyjaśnienia zasad dotyczących usług online; dostosowanie

---

35 *White Paper. On Artificial Intelligence – a European approach to excellence and trust*, Brussels, 19.2.2020, COM(2020) 65 final.

36 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future, Brussels, 19.2.2020, COM(2020) 67 final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions: A European strategy for data, Brussels, 19.2.2020, COM(2020) 66 final. Zob. też ec.europa.eu/commission/presscorner/detail/en/ip_20_273, komunikat prasowy z 19 lutego 2020 r.

37 Digital technologies are crucial for the EU to become climate neutral by 2050, the goal set in the European Green Deal, European Union, 2020.

przepisów UE do wymagań gospodarki cyfrowej; stworzenie w gospodarce warunków uczciwej konkurencji; zwiększenie dostępu do danych wysokiej jakości, z równoczesnym zapewnieniem ochrony danych osobowych i wrażliwych. Z dążeniem do kształtowania otwartego, demokratycznego i zrównoważonego społeczeństwa powiązano: wykorzystanie technologii do osiągnięcia w Europie do 2050 r. neutralności klimatycznej; zmniejszenie emisji dwutlenku węgla w sektorze cyfrowym; zagwarantowanie obywatelom lepszej kontroli i ochrony ich danych; stworzenie europejskiej przestrzeni danych na temat zdrowia, w celu wspomagania badań, diagnostyki i leczenia; zwalczanie dezinformacji online i wspieranie wiarygodnych treści medialnych. Propozycje wskazanych kierunków działań zostały przesłane do konsultacji. Zapowiedziano, że projektów legislacyjnych i organizacyjnych można się spodziewać w końcu 2020 r.

W projekcie strategicznym UE z początku 2020 r. zapowiedziano: stworzenie europejskiej przestrzeni danych i jednolitego rynku danych; wykorzystanie danych do unowocześnienia usług publicznych; ustanowienie jasnych i uczciwych zasad dostępu do danych i ich ponownego wykorzystania; inwestowanie w standardy, narzędzia i infrastrukturę nowej generacji do przechowywania i przetwarzania danych; łączenie sił w sprawach europejskiej zdolności przetwarzania w chmurze; danie użytkownikom prawa, narzędzi i umiejętności umożliwiających pełną kontrolę nad ich danymi. W prognozie na 2025 r. założono wzrost globalnej wielkości danych o 530% w stosunku do 2018 r. (z 33 do 175 zettabajtów). Zgodnie z tą prognozą, w 27 państwach UE wartość gospodarki opartej na danych wzrośnie do 829 miliardów euro (z 301 miliardów euro, tj. 2,4% PKB UE, w 2018 r.), liczba specjalistów do spraw danych zwiększy się do 10,9 miliona osób (z 5,7 miliona w 2018 r.), a odsetek ludności z podstawowymi umiejętnościami cyfrowymi wzrośnie do 65% (z 57% w 2018 r.)[38].

Należy zauważyć, że wśród państw członkowskich Unii Europejskiej, obok współpracy, nasila się wewnętrzna rywalizacja na polu projektów sztucznej inteligencji. O pierwsze miejsce w Unii Europejskiej zabiega Francja, która planuje wydatki na badania naukowe, inwestycje i działania edukacyjne w tej dziedzinie w latach 2018–2022 na poziomie 1,5 miliarda euro. W marcu 2018 r. prezydent Emmanuel Macron zapowiedział, że jego kraj zamierza zostać europejskim centrum rozwoju sztucznej inteligencji i wejść do grona światowych liderów nowych technologii[39]. Preferencjami mają być objęte prace nad sztuczną inteligencją nakierowane na potrzeby opieki zdrowotnej, transportu, ochrony środowiska i obrony. Władze publiczne zostały wskazane jako

[38] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en.

[39] https://www.sztucznainteligencja.org.pl/francja-mocarstwowe-ambicje/; https://www.oecd-opsi.org/projects/ai/strategies.

centralne ogniwo w tworzeniu warunków do rozwoju sztucznej inteligencji. Kluczowe znaczenie przypisano kształceniu zasobów ludzkich niezbędnych w realizacji projektów technologicznych nowej generacji oraz koordynacji współpracy rządu i podmiotów prywatnych.

Swoje całościowe programy w dziedzinie sztucznej inteligencji – jako integralnej części projektów rozwojowych – mają też inne państwa europejskie. Przykładowo, w Wielkiej Brytanii w dokumencie programowym z 2018 r. (zaktualizowanym w maju 2019 r.) zadeklarowano, że kraj ten ma potencjał, by w tej dziedzinie przewodzić światu. Wskazano na możliwości stosowania innowacji technologicznych do zaspokajania potrzeb starzejącego się społeczeństwa. Zapowiedziano inwestowanie w nowe technologie do poprawy wydajności, w tym w świadczenie usług cyfrowych w sektorze publicznym, oraz utworzenie funduszu GovTech o wartości 22,4 miliona euro, dla wspierania innowacyjnych rozwiązań w zakresie usług publicznych. Przewidziano zwiększenie ogólnych wydatków związanych ze sztuczną inteligencją z 1,7% do 2,4% w 2027 r. Zapowiedziano wspomaganie, w tym także na poziomie akademickim, rozwoju wysokokwalifikowanych kadr zdolnych do tworzenia nowych projektów technologicznych, a także usuwanie barier w udostępnianiu danych z sektora publicznego i prywatnego oraz zbudowanie infrastruktury rządowej warunkującej postęp w dziedzinie sztucznej inteligencji[40]. Z kolei, w opublikowanej w Niemczech w 2018 r. strategii rozwoju sztucznej inteligencji („AI made in Germany")[41] położono akcent na umacnianie i uregulowanie pozycji państwa jako centrum badań nad nowymi technologiami. Za zasadnicze cele przyjęto promowanie wzrostu gospodarczego, wykorzystanie sztucznej inteligencji w sektorze publicznym, szczególnie w sferze informacji i usług, zarządzania kryzysowego oraz bezpieczeństwa wewnętrznego i zewnętrznego.

Konkurencja w obszarze nowych technologii cyfrowych między USA i Chinami przerodziła się w otwarty konflikt. Kluczowym elementem amerykańsko-chińskiego sporu, który w 2019 r. przybrał charakter swoistej (zimnej) wojny technologicznej, stały się kwestie związane z osiągnięciem supremacji w sprawach technologii sieci telekomunikacyjnej 5G. W tym przypadku nakładają się na siebie względy bezpieczeństwa państw i konkurencyjne interesy finansowe, ale ponad tymi czynnikami trzeba widzieć coś więcej: walkę o przywództwo technologiczne we współczesnym świecie. Stawką w tej grze jest zdobycie dominującej pozycji w dostarczaniu technologii decydującej o sposobie działania internetu rzeczy. Dalszy rozwój społeczeństwa informacyjnego i sztucznej inteligencji doprowadzi do gwałtownego wzrostu ilości danych magazynowanych w chmurach elektronicznych, które będą wymagać przesyłania, integrowania

[40] https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal.
[41] https://www.oecd-opsi.org/projects/ai/strategies.

i analizowania w czasie rzeczywistym. Już w 2019 r. sieć 5G była wdrażana w Stanach Zjednoczonych, Korei Południowej, Szwajcarii i Australii. W niedalekiej przyszłości sieć łączności 5G stanie się centralnym elementem systemu, w którym będzie można przesyłać dane tysiąckrotnie szybciej niż obecnie. Zostanie bazą wielu miliardów urządzeń, w tym elementów infrastruktury krytycznej, spiętych w globalną sieć. W tej sytuacji jest sprawą oczywistą, że cele wyścigu największych światowych potęg, Stanów Zjednoczonych i Chin, wykraczają poza sferę technologicznych innowacji, dotyczą mechanizmów decydowania politycznego, umożliwiających wywieranie globalnego wpływu.

Według USA, produkty koncernu Huawei oferowane w sieci internetowej 5G mają zdolność przechwytywania danych użytkowników i przekazywania tych informacji chińskim służbom specjalnym. Producent infrastruktury nowej generacji łączności internetowej uzyska też, zdaniem ekspertów od bezpieczeństwa sieci, możliwość nietransparentnego ingerowania w działanie jej urządzeń. Przedstawiciele Huawei zaprzeczają oczywiście istnieniu zagrożeń bezpieczeństwa związanych z używaniem ich produktów. Co więcej, Ren Zhengfei, założyciel Huawei, w wywiadzie dla dziennika „La Repubblica" tak ujął sedno sporu: „Amerykanie mieli tajny dostęp do sieci 3G i 4G i wykorzystywali go w celach wywiadowczych, a teraz już nie mogą tego robić"[42].

Stany Zjednoczone nie są osamotnione w dostrzeganiu zagrożeń wynikających z uzależnienia od chińskich produktów sieci 5G. Istotną rolę w uświadomieniu ryzyka związanego z przyjęciem oferty chińskich producentów odegrała Australia. Już w 2018 r. australijskie służby specjalne przeprowadziły symulacyjną analizę możliwości wykorzystania systemu sieci 5G do szpiegowania i blokowania infrastruktury krytycznej. W lutym 2018 r. Malcolm Turnbull, ówczesny premier Australii, przedstawił swoje zastrzeżenia wobec chińskiej oferty teleinformatycznej w trakcie wizyty w Waszyngtonie. W połowie 2018 r. na zagrożenia związane z używaniem chińskiego sprzętu wskazali analitycy badający te kwestie w Wielkiej Brytanii. W maju 2019 r. o podejrzeniach holenderskiej agencji kontrwywiadowczej AIVD dotyczące instalowania przez Huawei „bocznej furtki" w sprzęcie zakupionym przez jednego z holenderskich operatorów telekomunikacyjnych poinformował dziennik „De Volkskrant"[43]. Autorzy raportu opublikowanego w maju 2019 r. przez agencję Reuters[44] przypomnieli, że operacje cybernetyczne już od 2012 r. stanowią kluczowy element polityki prezydenta Xi Jinpinga, co przekłada się na popieranie przez państwo akcji hakowania systemów informatycznych w celu osiągnięcia przez Chiny korzyści strategicznych i handlowych. Władze

[42] Wywiad zamieszczony w „Gazecie Wyborczej" z 25 lipca 2019 r., s. 16–17.

[43] https://cyfrowa.rp.pl/globalne-interesy/36275-kto-wspiera-huawei-a-kto-z-nim-walczy.

[44] https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-u-s-war-on-chinas-tech-giant-idUSKCN1SR1EU.

Chin stanowczo sprzeciwiają się takim opiniom i podkreślają, m.in. w dokumencie z 2015 r. przedstawiającym strategię wojskową, że same były ofiarą szpiegostwa cybernetycznego.

Departament Handlu USA podjął w 2019 r. decyzję o wpisaniu Huawei Technologies i siedemdziesięciu związanych z tą korporacją firm na listę podmiotów, które muszą uzyskiwać zgodę rządu w Waszyngtonie na kupowanie amerykańskich komponentów i technologii. Prezydent Donald Trump zakazał amerykańskim firmom używania sprzętu telekomunikacyjnego wyprodukowanego przez podmioty uznane za zagrożenie dla bezpieczeństwa narodowego USA. W czasie rozmów przywódców USA i Chin w połowie 2019 r. prezydent USA zapowiedział złagodzenie ograniczeń w sprawie korzystania przez firmy amerykańskie z chińskich produktów, co nie znalazło jednak potwierdzenia w rzeczywistości. Trzeba zaznaczyć, że w USA eliminuje się produkty elektroniczne nie tylko chińskich firm podejrzanych o powiązania ze służbami specjalnymi. W 2007 r. Departament Bezpieczeństwa Wewnętrznego zakazał wszystkim agencjom federalnym sięgania po oprogramowanie rosyjskiej firmy Kaspersky Lab zajmującej się tworzeniem rozwiązań z zakresu cyberbezpieczeństwa. Decyzję uzasadniono obawami o to, że produkty tej firmy umożliwiają rosyjskim służbom specjalnym penetrację systemów elektronicznych[45].

W związku z wydanym przez władze USA zakazem kooperacji z chińskimi firmami spór przeniósł się na płaszczyznę oprogramowania urządzeń telekomunikacji internetowej, które jest produkowane przede wszystkim przez koncerny amerykańskie. W maju 2019 r. holding Alphabet Inc. powołany do życia przez spółkę Google zapowiedział zakończenie współpracy z Huawei. Chiński koncern stracił stabilny dostęp do aktualizacji mobilnego systemu operacyjnego Android oraz niektórych aplikacji Google. Zagroziło to w poważnym stopniu funkcjonowaniu Huawei na rynkach światowych. Na całym świecie jest około 2,5 miliarda urządzeń działających pod kontrolą systemu Android, takich jak telefony komórkowe, smartfony, tablety czy notebooki. W połowie 2019 r. obroty Huawei spadły ze 135 do 100 miliardów dolarów. Chińczycy podjęli intensywne wysiłki, aby wyzwolić się z uzależnienia od komponentów objętych embargiem amerykańskim. W przywołanym wyżej wywiadzie Ren Zhengfei poinformował, że jego firma usunie do końca 2019 r. swoje braki technologiczne w 93%. Elementem realizacji tego planu stało się opracowanie przez Huawei Technologies w sierpniu 2019 r. własnego system operacyjnego dla smartfonów i innych urządzeń. System Harmony OS (chińska nazwa: Hongmeng) został zaprezentowany jako alternatywny wobec amerykańskiej technologii Android i ma być stopniowo wdrażany do 2022 r. do obsługi

[45] https://www.politico.com/story/2017/09/13/kaspersky-software-banned-242664.

urządzeń wirtualnej rzeczywistości – w pierwszej kolejności na rynku chińskim. System ma być nadal ulepszany, a na potrzeby Huawei pracuje nad tym już ponad 4000 programistów[46]. Biorąc pod uwagę wielkość chińskiego rynku zbytu na urządzenia elektroniczne, należy liczyć się z tym, że ograniczenia w wymianie handlowej w tej dziedzinie mogą w istotnym stopniu wpłynąć na wyniki firm amerykańskich. Już obecnie perspektywa utraty ważnego kierunku eksportu swoich produktów jest przedmiotem rozmów między tymi firmami i władzami USA. Problem jest poważny, tym bardziej że w 2019 r. władze Chin wydały dyrektywę, zgodnie z którą instytucje publiczne w tym państwie mają zaprzestać do 2022 r. używania sprzętu i oprogramowania komputerowego produkowanego za granicą. Eksperci szacują, że dyrektywa władz chińskich spowoduje konieczność wymiany na krajowe odpowiedniki 20 do 30 milionów elementów sprzętu i oprogramowania. Prace miały się rozpocząć w 2020 r. (planowano dokonać wówczas 30% zamian), zintensyfikować w 2021 r. (50% zamian) i zakończyć w 2022 r.[47].

Amerykańsko-chiński spór o udział firmy Huawei w budowie sieci 5G wykracza – jak już sygnalizowałem – poza rywalizację w dziedzinie inteligentnych technologii między tymi państwami. Sprawa zatacza coraz szersze kręgi i budzi wiele emocji, a zainteresowane nią państwa stają przed podjęciem decyzji, po której stronie tego sporu mają się opowiedzieć. Jego przedmiot stał się elementem światowej gry i konkurencji politycznej, prowadzącej być może do ukształtowania się nowego układu sił w świecie. USA podjęły w 2019 r. intensywne wysiłki dyplomatyczne, aby stanowczo zachęcić sojuszników do wykluczenia oferty Huawei z ich planów inwestycyjnych. Niektóre państwa podjęły już decyzję o blokadzie współdziałania z producentami chińskimi w rozwijaniu sieci 5G. Inne państwa przyjmują pozycję wyczekującą lub też poszukują rozwiązań kompromisowych. W lipcu 2019 r. koncern Huawei ogłosił, że udało mu się już zawrzeć na całym świecie 50 kontraktów na dostawy sprzętu i technologii na potrzeby budowy sieci 5G. Prawie dwie trzecie z nich przypadło na Europę[48].

Jak pokazują dane z grudnia 2019 r. opublikowane w lutym 2020 r. przy okazji konferencji na temat bezpieczeństwa w Monachium, na świecie nie ma jednomyślności w kwestii dopuszczenia technologii chińskiej do tworzenia sieci 5G. Spośród państw OECD całkowicie wykluczały sięgnięcie po tę technologię Australia, Japonia, Izrael, Nowa Zelandia i USA. Jej częściowe lub pełne wyłączenie było rozważane lub wyraźnie już zapowiedziane m.in. w Danii,

---

46 https://www.reuters.com/article/us-huawei-tech-developer/huawei-unveils-harmony-operating-system-but-wont-ditch-android-for-smartphones-idUSKCN1UZ0MH.

47 https://www.theguardian.com/world/2019/dec/09/china-tells-government-offices-to-remove-all-foreign-computer-equipment.

48 https://cyfrowa.rp.pl/globalne-interesy/36275-kto-wspiera-huawei-a-kto-z-nim-walczy.

Estonii, we Francji, w Irlandii, Kanadzie, Litwie, Łotwie, Niemczech, Niderlandach, Norwegii, Polsce, Republice Czeskiej, Szwecji, Wielkiej Brytanii i we Włoszech. Nic natomiast nie wiadomo – powszechnie dostępne materiały nie zawierają informacji na ten temat – o możliwym ograniczeniu lub akceptowaniu współpracy z Huawei w tworzeniu sieci 5G w Austrii, Belgii, Chile, Finlandii, Grecji, Hiszpanii, Islandii, Luksemburgu, Portugalii, Słowacji, Słowenii, Szwajcarii, Turcji i na Węgrzech[49].

Amerykanie otwarcie ostrzegają swoich partnerów w Europie, że dopuszczenie chińskiego sprzętu do użytku będzie się wiązać z wykluczeniem danego państwa z obiegu informacji tajnych dotyczących obronności i walki z terroryzmem. Takie ostrzeżenie skierowano m.in. pod adresem Niemiec i Wielkiej Brytanii. Także Georgette Mosbacher, ambasador USA w Polsce, przypomniała w wywiadzie prasowym, że Stany Zjednoczone muszą mieć pewność, iż wszystkie operacje, które prowadzą z sojusznikami, nie są narażone na ryzyko przechwycenia, zaś chińskie urządzenia umożliwiające wprowadzenie nowej technologii internetowej w naszym kraju nie dają takiej pewności[50].

W 2018 r. Departament Sprawiedliwości Stanów Zjednoczonych oskarżył członków hakerskiej grupy APT10 o atak na dziesiątki europejskich i amerykańskich firm w celu kradzieży własności intelektualnej i poufnych danych osobowych. Ogłoszono, że grupa ta działała we współpracy z chińskim Ministerstwem Bezpieczeństwa Państwowego. Władze amerykańskie zwracały też wielokrotnie uwagę, że w Chinach wykorzystuje się technologię cyfrową do stosowania masowych represji.

W grudniu 2019 r. sekretarz stanu USA Mike Pompeo zwrócił się do władz państw europejskich ze stanowczym wezwaniem, by stawiały przy wyborze technologii 5G na pierwszym miejscu względy bezpieczeństwa i zrezygnowały w związku z tym z kooperacji z firmami chińskimi[51]. W jego opinii, sięgnięcie po produkty z Chin będzie równoznaczne z oddaniem kontroli nad swoją infrastrukturą krytyczną chińskim gigantom technologicznym powiązanym ze służbami specjalnymi. Zdaniem polityków amerykańskich, dzięki możliwościom 5G chińskie służby specjalne mogą wykorzystać Huawei lub ZTE (inną chińską firmę telekomunikacyjną) do kradzieży prywatnych lub zastrzeżonych informacji. W lutym 2020 r. stanowisko takie zaprezentował na konferencji w sprawie bezpieczeństwa w Monachium Mark Esper, sekretarz obrony USA. Ostrzegł przy tym, że amerykańskie sojusze, w tym przyszłość NATO, a także

---

[49] *Munich Security Report 2020*, www.securityconference.org/en/publications/munich-security-report, s. 32.

[50] Serwis informacyjny PAP z 21 kwietnia 2019 r.

[51] https://www.politico.eu/article/europe-must-put-security-first-with-5g-mike-pompeo-eu-us-china.

współpraca wywiadowcza będą zagrożone, jeśli kraje europejskie zaczną stosować technologię Huawei w swoich sieciach 5G[52].

Konflikt amerykańsko-chiński postawił w trudnej sytuacji państwa Unii Europejskiej podejmujące decyzję o wyborze inwestora sieci 5G. Stoją one przed dylematem: dopuścić na swoim terytorium urządzenia chińskie czy zachować sojusznicze relacje z USA. Huawei jest, obok Ericssona i Nokii, jedną z trzech największych globalnych firm, które według analityków mogą dostarczać szeroki asortyment zaawansowanego technologicznie sprzętu mobilnego na dużą skalę. Jest to koncern bardzo intensywnie inwestujący w rozwój swoich technologii. Nie bez znaczenia jest też fakt, że oferuje sprzęt po atrakcyjnych, konkurencyjnych cenach. Jednak podjęcie decyzji w tej sprawie nie jest rzeczą prostą, bowiem „europejskie łańcuchy handlowe, gospodarcze i produkcyjne są nierozerwalnie związane zarówno z technologiami chińskimi, jak i amerykańskimi”[53].

Unia Europejska rekomendowała państwom członkowskim przyjęcie zasady wspólnej, europejskiej certyfikacji bezpieczeństwa cybernetycznego dla produktów, procesów i usług w cyberprzestrzeni. W marcu 2019 r. uchwałę w tej sprawie przyjął Parlament Europejski. Podstawowe znaczenie nadano certyfikacji w obszarze infrastruktury krytycznej. Rozwiązania te mają dotyczyć systemów sieci 5G. W okresie przejściowym, do 2023 r., certyfikacja ma być dobrowolna i uzależniona od decyzji władz państw członkowskich UE. Postanowiono zwiększyć uprawnienia unijnej agencji ds. bezpieczeństwa cybernetycznego (ENISA). W 2019 r. Komisja Europejska wezwała państwa członkowskie do skoordynowanego podejścia do bezpieczeństwa sieci 5G oraz przeprowadzenia krajowych ocen ryzyka związanego z technologią 5G i podjęcia środków zaradczych ograniczających ryzyko w tej dziedzinie. Za rzecz niezwykle ważną uznano ustalenie stopnia wrażliwości elementów i funkcji sieci 5G oraz różnych rodzajów podatności na zagrożenia, w tym zagrożenia związane z łańcuchem dostaw 5G. Podjęto prace zmierzające do opracowania ogólnounijnej oceny i planu działań w tej dziedzinie przy uwzględnieniu faktu, że sieci piątej generacji będą stanowić w przyszłości podstawową infrastrukturę, łącząc miliardy przedmiotów i systemów, w tym w kluczowych sektorach, takich jak energetyka, transport, bankowość i opieka zdrowotna, a także w systemach zawierających wrażliwe informacje przemysłowe i dotyczące bezpieczeństwa[54].

---

52 https://www.theguardian.com/us-news/2020/feb/15/us-defence-secretary-warns-us-alliances-at-risk-from-huawei-5g.

53 http://www.ipsnews.net/2019/07/age-digital-geopolitics-proxy-war-us-china/#.

54 https://ec.europa.eu/poland/news/190719_5G_pl; https://cyfrowa.rp.pl/globalne-interesy/32358-unia-chce-ochrony-sieci-5g-to-reakcja-na-tzw-sprawe-huawei.

Strategię poszczególnych państw UE w sprawie wyboru inwestora budującego sieci 5G wyznacza otwarcie na wszystkie oferty – przy wyraźnym akcentowaniu konieczności zagwarantowania ze strony dostawcy infrastruktury sieci wysokich standardów bezpieczeństwa, oraz preferowanie rozwiązań, w których realizacji nie uczestniczy tylko jeden, mający pozycję monopolistyczną dostawca technologii. Ze względu na stan zaawansowania projektów 5G, wśród rodzimych oferentów europejskich obecnie mogą być jednak brani pod uwagę wyłącznie producenci skandynawscy (Ericsson i Nokia). W 2020 r. w Unii Europejskiej nasiliły się próby zmniejszenia uzależnienia rozwiązań z zakresu technologii 5G od sprzętu chińskiej firmy Huawei.

Wraz z rozpoczęciem w Europie budowy sieci 5G, mimo ogólnych deklaracji o potrzebie zachowania jednolitego stanowiska, widać różnicowanie się państw członkowskich UE w kwestii granic współpracy z chińskimi dostawcami infrastruktury komunikacji internetowej nowej generacji. Jako przykład można podać podpisanie w marcu 2019 r. przez Włochy i Chiny protokołu o przystąpieniu Włoch do chińskiego projektu Pasa i Szlaku (Belt and Road Initiative), zwanego też Nowym Jedwabnym Szlakiem. W 2019 r. w niektórych państwach UE, po etapie opracowania strategii rozwoju sztucznej inteligencji oraz testów i pilotaży technologii 5G, rozpoczęło się już przydzielanie częstotliwości na potrzeby nowej sieci i ruszył proces wyboru inwestora systemowego tej sieci. Najbardziej zaawansowane w tych działaniach są Francja, Finlandia, Austria, Niemcy, Luksemburg, Holandia, Hiszpania, Szwecja i Wielka Brytania. Częstotliwości operatorom przydzieliły m.in. Austria, Dania i Niemcy, a z państw spoza UE także Szwajcaria. Tym bardzo kosztownym, pochłaniającym już miliardy euro działaniom towarzyszy niepewność co do możliwości perspektywicznej współpracy z partnerami chińskimi[55].

Świadomość politycznego znaczenia nowych technologii telekomunikacyjnych może prowadzić do decyzji o budowie własnych systemów sieci 5G. Taką decyzję podjęto w Rosji, gdzie zadanie to ma być zrealizowane do 2024 r., a powierzono je państwowej korporacji zbrojeniowej Rostech. Podstawą mają być rozwiązania przygotowane przez firmę Sozvezdie pracującą m.in. nad projektami sztucznej inteligencji, w tym internetem rzeczy[56]. Tworzenie własnych rozwiązań systemowych i operacyjnych w internetowej telekomunikacji wymaga ogromnych nakładów oraz zaplecza informatycznego, co rodzi trudne do pokonania bariery nawet dla firm silnych na rynku. Tytułem przykładu wskazać można próby opracowania własnego oprogramowania operacyjnego o nazwie Tizen przez południowokoreańską firmę Samsung Electronics, które nie zostały przeniesione na poziom konkurencji z systemem Android z powodu

[55] https://cyfrowa.rp.pl/telekomunikacja/32961-europa-przygotowuje-sie-na-ere-sieci-5g.
[56] https://cyfrowa.rp.pl/globalne-interesy/35690-rosjanie-tez-chca-miec-swoje-5g.

niedostatecznego zaplecza informatycznego. Własne rozwiązania dotyczące sieci 5G uruchomiła w 2019 r. Korea Południowa w ramach komercyjnej oferty przygotowanej przez SK Telecom, LG Ulus i KT. W ciągu roku 15 tysięcy stacji bazowych zdolnych do obsługi tej technologii ma być wzmocnionych przez kolejne tysiące nadajników[57].

Walka o prymat w dziedzinie technologii komunikacyjnej 5G to tylko jeden z przykładów rywalizacji między państwami w kreowaniu nowych rozwiązań telekomunikacyjnych. Innym przykładem jest obszar usług komputerowych oraz chmur elektronicznych, w których mają być przechowywane dane pochodzące od wielu podmiotów. Jak już sygnalizowałem, państwa i korporacje doskonale zdają sobie sprawę z tego, że administrowanie chmurami elektronicznymi może wpływać na ich pozycję we współczesnym świecie. W tej dziedzinie trwa już wojna cenowa, która ma istotne aspekty polityczne. Widać też tendencję do budowania silnych podmiotów zdolnych do sfinansowania inwestycji w systemy przechowywania danych, te inwestycje pochłaniają bowiem miliardy dolarów. W 2019 r. spółka Reliance Industries Ltd z Indii ogłosiła partnerstwo z platformą chmurową Microsoft Azure, co stanowi wyzwanie dla konkurencyjnych dostawców usług w chmurze, takich jak Amazon.com i Alphabet's Google[58]. W tym samym roku amerykański dostawca usług chmurowych Salesforce zakupił za 1,35 miliarda dolarów amerykańsko-izraelskie produkty służące przyspieszeniu rozwoju usług w chmurze. Firma ta zakupiła też za ponad 15 miliardów dolarów oprogramowanie od firmy analitycznej Tableau[59]. O jak najlepszy udział w rynku zabiega także koncern Oracle, który ma mieć do końca 2020 r. 36 lokalizacji centrów danych w chmurze. Celem Oracle jest posiadanie co najmniej dwóch centrów w każdym kraju, w którym działa, tak aby klienci mogli mieć obok bazy głównej także mechanizm zapasowy na wypadek awarii[60].

Cyfrowe technologie komputerowe i komunikacyjne stają się coraz częściej polem konfrontacji, w tym walki politycznej między państwami oraz między różnymi siłami politycznymi wewnątrz poszczególnych państw. Przykładowo, różnica zdań na temat granic regulacji technologii komputerowych i komunikacyjnych znalazła wyraz w sporze o prawa autorskie w cyberprzestrzeni. Projekt rozwiązań w zakresie reglamentacji mającej na celu obronę interesów twórców został potraktowany przez wielu aktorów sceny publicznej jako atak

---

57 https://www.geekweek.pl/news/2019-04-05/korea-poludniowa-pierwszym-krajem-na-swiecie-ktory-uruchomil-siec-5g.

58 https://www.reuters.com/article/us-reliance-agm-microsoft-analysis/reliance-microsoft-cloud-tie-up-poses-threat-to-amazon-google-in-india-idUSKCN1V21DW.

59 https://www.reuters.com/journalists/steven-scheer.

60 https://www.reuters.com/article/us-oracle-cloud/oracle-adds-cloud-data-centers-in-five-countries-sets-new-2020-target-idUSKBN1ZX1DG.

na wolność i próba wprowadzenia cenzury w komunikacji elektronicznej. Miało to miejsce w 2019 r., przy okazji prac nad unijną dyrektywą o prawie autorskim na jednolitym rynku cyfrowym, która nakłada na platformy internetowe obowiązek filtrowania treści pod kątem praw autorskich i praw pokrewnych dla wydawców prasowych oraz ustanawia mechanizmy licencjonowania treści chronionych prawem autorskim. Mimo że przyjęte regulacje dotyczą tylko największych platform, których właścicielami są Google czy Facebook, ich przeciwnicy uważają, iż mogą one prowadzić do cenzury w sieci. Regulacje nakazują, by platformy płaciły posiadaczom praw autorskich za treści publikowane przez użytkowników albo kasowały takie materiały. O tym, jak duże kontrowersje budzi ten projekt, świadczy już sam wynik głosowania w Parlamencie Europejskim: 348 europosłów było za, 274 przeciw, a 36 wstrzymało się od głosu. Wejście w życie dyrektywy jest uzależnione od zatwierdzenia przez państwa członkowskie UE, a jej wdrożenie ma nastąpić w ciągu dwóch lat. Już obecnie wiadomo, że będzie to trudne, gdyż Polska, Holandia, Włochy, Finlandia i Luksemburg nie poparły porozumienia w tej sprawie wypracowanego w Radzie UE.

Przedmiotem sporów jest też kwestia opodatkowania zysków, jakie globalne firmy czerpią ze swoich usług cyfrowych. Jak na razie nie ma porozumienia między państwami UE w tej kwestii. We Francji taki podatek został już wprowadzony w 2019 r. w wysokości 3% dla firm technologicznych osiągających globalne przychody przekraczające 750 milionów euro rocznie i przychody we Francji powyżej 25 milionów euro rocznie (tzw. podatek GAFA – skrót od Google, Amazon, Facebook, Apple). Decyzję o wprowadzeniu wiosną 2020 r. podatku w wysokości 2% za usługi cyfrowe sprzedawane przez firmy o rocznych globalnych przychodach wynoszących co najmniej 500 milionów funtów podjęto również w Wielkiej Brytanii. Także niektóre inne państwa europejskie (m.in. Austria) zapowiadają już opodatkowanie przychodów uzyskiwanych przez takie firmy, jak Google, Amazon czy Facebook.

Problem podatku cyfrowego zaczyna ciążyć na stosunkach europejsko-amerykańskich, gdyż władze USA uznały, że decyzje o opodatkowaniu globalnych korporacji cyfrowych uderzą w działające w Europie amerykańskie firmy technologiczne, i zapowiedziały kroki odwetowe. Francja po wprowadzeniu podatku GAFA, w obliczu zagrożenia wzrostem w USA ceł na główne produkty swojego eksportu (np. na szampana, sery), przystała na porozumienie łagodzące napięcie[61]. Sygnały docierające z Komisji Europejskiej wskazują, że Unia Europejska zamierza wzmacniać działania na rzecz ustanowienia podatku cyfrowego, co może prowadzić do nasilenia się konfliktu europejsko-amery-

[61] https://www.polsatnews.pl/wiadomosc/2019-07-12/google-amazon-facebook-apple-opodatkowane-we-francji-usa-rozpoczyna-sledztwo.

kańskiego na tym tle. Próby porozumienia w tej sprawie są podejmowane w ramach OECD. Koordynujący te prace Pascal Saint-Amans jest optymistą, ale nadal realna wydaje się w tym przypadku perspektywa amerykańsko-europejskiej wojny handlowej, gdyż Austria, Francja, Włochy i Hiszpania zapowiadają, że z końcem 2020 r. przystąpią do realizacji zamrożonych planów wprowadzenia podatku cyfrowego[62].

6.3. Rozwój cywilizacji cyfrowej jako cel inwestycji finansowych i prac badawczo-wdrożeniowych

• *Szybki wzrost liczby firm i podmiotów finansowych angażujących się w projekty rozwoju narzędzi sztucznej inteligencji*

Na świecie przybywa firm, które angażują się w projekty związane z rozwojem narzędzi sztucznej inteligencji, a instytucje finansowe – zwykle ostrożne – wykazują duże zainteresowanie inwestowaniem w tej dziedzinie. Jak wynika z badań Andrzeja Wodeckiego z Wydziału Zarządzania Politechniki Warszawskiej, w 2019 r. takie projekty realizowało ponad 3,2 tysiąca podmiotów na całym świecie. Blisko 2 tysiące firm specjalizowało się w technologii *big data*, a ponad 1,7 tysiąca prowadziło prace w zakresie uczenia maszynowego[63]. W budżetach instytucji finansowych do 2025 r. zarezerwowano na prace badawcze i wdrożeniowe w obszarze sztucznej inteligencji ponad bilion dolarów. Według danych firmy IDC, tylko w 2016 r. w instytucjach bankowych na rozbudowę narzędzi do analizy danych zgromadzonych w zasobie pamięci cyfrowej wydano na świecie ponad 20,8 miliarda dolarów.

Ścieżki finansowania prac badawczych i wdrożeniowych w dziedzinie doskonalenia komunikacji społecznej oraz rozwoju sztucznej inteligencji wypracowują poszczególne państwa, zwłaszcza te, które aspirują do ścisłej światowej czołówki – nie tylko na polu technologii. Prace te są też wpisywane do budżetów największych miast, a podmioty gospodarcze angażują w nie coraz większe środki finansowe.

Tak więc, media społecznościowe i sztuczna inteligencja to współcześnie już nie tylko przedmiot prac naukowców, technologów i specjalistów od komunikacji społecznej. To także – jak staram się pokazać w tej książce – płaszczyzna aktywności polityków i gremiów odpowiedzialnych za bieg spraw w przestrzeni publicznej i rozwój państw oraz decydentów ze świata kapitału i gospodarki.

---

62 https://www.politico.eu/article/digital-tax-oecd-pascal-saint-amans-facebook-google.

63 https://cyfrowa.rp.pl/technologie/34924-juz-wiadomo-kto-na-swiecie-pracuje-nad-ai.

6.4. Groźba powiększania się nierówności i nasilania konfrontacji w związku z kształtującym się cybernetycznym porządkiem w świecie

• Walka o zasady tworzenia nowych technologii oraz udział w kontroli globalnych sieci i węzłów komunikacji elektronicznej jako przedmiot geopolityki cyfrowej • Stany Zjednoczone i Chiny na drodze do zagwarantowania sobie największych zysków z rozwoju gospodarki cyfrowej • Niebezpieczeństwo pogłębiania się nierówności ekonomicznych oraz wykluczenia społecznego na tle różnic w rozwoju cyfrowym

Kształt geopolityki w rzeczywistości cyfrowej jest wypracowywany obecnie przynajmniej na najbliższe kilkanaście lat. Musi to znaleźć odzwierciedlenie w polityce strategicznej każdego rządu podchodzącego odpowiedzialnie do wyzwań przyszłości. Właśnie teraz zapadają decyzje określające stopień ponadnarodowej interoperacyjności, czyli możliwości współpracy między systemami społecznymi i technicznymi, oraz poziom trwałości ekosystemów cyfrowych. Na skutek strategicznej współzależności między poziomem rozwoju technologicznego a pozycją ekonomiczną i polityczną, kształtuje się nowy układ sił w ekonomice światowej. Spór o technologię 5G jest tylko częścią zabiegów o uzyskanie pozycji pozwalającej na osiąganie maksymalnych korzyści z rozwoju gospodarki cyfrowej, częścią zmagań o ustalenie zasad gry politycznej związanej z nowymi technologiami oraz z udziałem w kontroli globalnych sieci i węzłów komunikacji elektronicznej.

Głównymi graczami rywalizującymi o zagwarantowanie sobie największych zysków z rozwoju gospodarki cyfrowej są Stany Zjednoczone i Chiny. Jak wskazano w obszernym, opracowanym w 2019 r. przez UNCTAD (Konferencję Narodów Zjednoczonych do spraw Handlu i Rozwoju, organ pomocniczy ONZ) pierwszym światowym raporcie o gospodarce cyfrowej (*Digital Economy Report*)[64], Stany Zjednoczone i Chiny wytwarzają większość wartości w gospodarce cyfrowej. Z obydwoma tymi krajami jest związanych 75% wszystkich patentów w dziedzinie technologii łańcuchowej infrastruktury sieciowej, 50% globalnych wydatków na internet rzeczy, ponad 75% rynku przetwarzania w chmurze i aż 90% wartości kapitalizacji rynkowej największych światowych platform cyfrowych. Daje to im uprzywilejowaną pozycję w związku z przewagą gospodarki opartej na danych i pozwala przechwytywać zyski z technologii cyfrowej, a zarazem ogranicza możliwości wykorzystywania danych cyfrowych do globalnego rozwoju i do rozwiązywania problemów społecznych. Równocześnie zaś oba kraje dążą do tego, by w jak najmniejszym stopniu musiały dzielić się ze sobą zyskami z inwestycji cyfrowych, co prowadzi do konfliktów, których przykładem jest spór o technologię 5G.

[64] https://news.un.org/en/story/2019/09/1045572.

Wspomniany wyżej raport UNCTAD na temat gospodarki cyfrowej zawiera liczne dane, które wskazują, że w związku z olbrzymimi dysproporcjami w rozwoju cyfrowym poszczególnych regionów i państw światu grozi nasilenie się nierówności ekonomicznych, a w ślad za tym – wzrost nierówności społecznych i wykluczenia społecznego. Autorzy raportu oceniają, że korzyści z rozwoju cyfrowego czerpią dotychczas tylko nieliczne państwa i społeczeństwa – ze Stanami Zjednoczonymi i z Chinami na czele. Przypominają, że ponad połowa świata ma ograniczony dostęp do internetu lub nie ma go wcale. Dotyczy to w szczególności krajów Afryki i Ameryki Łacińskiej.

W opinii autorów raportu dalsza koncentracja danych w ramach siedmiu globalnych marek – tzw. superplatform (Microsoft, Apple, Amazon, Google, Facebook, Tencent, Alibaba) – tworzy nowy układ władzy w świecie. Następuje kumulacja zysków z gospodarki cyfrowej i pogłębiają się nierówności między państwami i wewnątrz nich, przy czym w najgorszej sytuacji są kraje rozwijające się. W raporcie przypomniano, że globalny ruch internetowy wzrósł z około 100 gigabajtów (GB) dziennie w 1992 r. do ponad 45 000 GB na sekundę w 2017 r., zaś w 2022 r. światowy ruch IP ma osiągnąć 150 700 GB na sekundę. Wymienionych wyżej siedem globalnych firm internetowych stanowi dwie trzecie całkowitej wartości rynkowej 70 najsilniejszych platform. Google obsługuje około 90% światowego rynku wyszukiwania w internecie, Facebook jest najsilniejszą platformą mediów społecznościowych w ponad 90% krajów. O koncentracji (czy monopolizacji) można też mówić w odniesieniu do platform transakcyjnych (takich jak Amazon, Alibaba, Facebook, eBay). Dominującą pozycję na rynku mają nieliczne platformy sprzętowe dostarczające systemy operacyjne (np. Android lub Linux) i standardy technologiczne (np. wideo w formacie MPEG).

W raporcie UNCTAD podkreślono, że potrzebne jest wypracowanie na gruncie politycznym zasad wyrównujących na świecie szanse rozwoju instrumentów cyfrowych. Przypomniano, że technologia ma podwójne oblicze: tworzy zarówno szanse, jak i zagrożenia. Wezwano więc do podjęcia działań – w skali globalnej, z udziałem rządów – prowadzących do niwelowania dysproporcji w czerpaniu korzyści płynących z gospodarki cyfrowej.

Jak ostrzegał w 2019 r. Dominic Cummings, doradca strategiczny premiera Borisa Johnsona, jeśli Wielka Brytania nie zintensyfikuje swoich prac nad AI i nie zmusi zagranicznych gigantów technologicznych do płacenia podatków, stanie się amerykańską lub chińską „kolonią AI". Groźba ta może się spełnić zwłaszcza wtedy, gdy rozwój AI doprowadzi do przekroczenia przez roboty poziomu inteligencji ludzi[65].

[65] https://www.politico.eu/article/3-artificial-intelligence-scenarios-that-keep-dominic-cummings-awake-at-night.

Wyraźne sygnały świadczące o chęci odzyskania pozycji gracza w sferze nowych technologii płyną z Unii Europejskiej. Thierry Breton, od 2019 r. komisarz UE do spraw rynku wewnętrznego i usług, stwierdził, że europejska strategia jest pilnie potrzebna przede wszystkim w dziedzinie zarządzania danymi, gdyż „obecnie pięć, sześć firm na świecie zarządza 80 proc. danych całej planety i to nie są firmy europejskie". Komentując w wywiadzie udzielonym korespondentom kilku europejskich dzienników istniejącą sytuację w zakresie danych internetowych, stwierdził on m.in.: „Uważamy, że to musi się zmienić. Bo nasza gospodarka to jedna czwarta gospodarki światowej, generujemy mnóstwo danych i musimy się jakoś organizować. Tak, żebyśmy byli w stanie to prowadzić i kontrolować. Dobra wiadomość jest taka, że na Ziemi podwajamy liczbę danych co 18 miesięcy – mówię o wszystkich danych, tych produkowanych przez osoby prywatne, firmy, instytucje publiczne, służbę zdrowia, transport. Teraz wirtualna wielkość naszej planety to 35 zettabajtów, czyli 35 trylionów gigabajtów. To są wszystkie dane zgromadzone od początku ludzkości. I tą górą danych zawładnęło kilka firm – amerykańskich, ale też chińskich – i używają moich danych, waszych danych, danych całej planety do oferowania swoich usług. Ale, jak wspomniałem, za półtora roku planeta Ziemia to nie będzie już 35, ale 70 zettabajtów danych. I naszym celem jest stworzenie sytuacji, w której to my w Europie z tego skorzystamy"[66].

Dążenie do czerpania jak największych profitów z rozwoju nowych, inteligentnych technologii stoi u podstaw gry, jaką prowadzą Chiny i państwa Unii Europejskiej. Annegret Bendiek, Nadine Godehardt, Jürgen Neyer i David Schulze, badacze zajmujący się problemami wojny handlowej o kontrolę nad technologią 5G, przedstawili na stronie Niemieckiego Instytutu Spraw Międzynarodowych i Bezpieczeństwa (Stiftung Wissenschaft und Politik, SWP) cztery scenariusze dalszych relacji na tej płaszczyźnie między Unią Europejską i Chinami. Podstawą opracowania były wnioski z warsztatów na temat geopolityki cyfrowej zorganizowanych na zaproszenie SWP i Uniwersytetu Europejskiego Viadrina, z udziałem kilkudziesięciu ekspertów z Europy i Chin.

Zdaniem wymienionych wyżej badaczy, w ciągu najbliższych 15 lat pod wpływem transformacji cyfrowej zasadniczo zmienią się ramy działań politycznych w relacjach Europy z Chinami[67]. Najbardziej optymistyczny scenariusz zakłada zwycięstwo koncepcji cyberpokoju (*cyber peace*) na podstawie wspólnie wypracowanych, uznanych i przestrzeganych umów. W takiej sytuacji byłoby możliwe wspólne finansowanie rozwoju technologii cyberbezpie-

---

66 Zob. A. Słojewska, *Thierry Breton: Europejczycy muszą sami decydować o swoich danych*, https://www.rp.pl/Wywiady/301169867-Thierry-Breton-Europejczycy-musza-sami-decydowac-o-swoich-danych.html.

67 https://www.swp-berlin.org/en/point-of-view/2019/preventing-digital-trench-warfare-between-the-eu-and-china.

czeństwa, a konkurencja przebiegałaby w warunkach wzajemnego zaufania. Drugi scenariusz przewiduje pójście w kierunku izolacji zasobów cyfrowych, co doprowadzi do naruszenia zintegrowanych rynków i łańcuchów produkcyjnych oraz do wstrząsów politycznych i społecznych. Trzeci scenariusz rozwoju wydarzeń, opatrzony przez autorów hasłem „zimna wojna 4.0", zawiera zapowiedź radykalizacji politycznej w Europie i nasilenia się ataków cybernetycznych w warunkach umacniania się narodowych tendencji protekcjonistycznych, spadku znaczenia regulacji międzynarodowych oraz całkowitego uzależnienia Europy od stanu relacji amerykańsko-chińskich. Czwarty – najbardziej zdaniem autorów prawdopodobny – scenariusz to wizja „cyfrowej wojny okopowej". Ten wariant scenariusza opiera się na założeniu, że globalne rozdrobnienie społeczno-techniczne doprowadzi do ukształtowania się trzech izolujących się bloków cyfrowych, tworzonych przez Stany Zjednoczone, Chiny i Europę, które będą konkurować ze sobą na całym świecie. Internet w obecnej postaci zniknie i zostanie zastąpiony przez niekompatybilną, podzieloną cyberprzestrzeń funkcjonującą w ramach poszczególnych bloków. Krajowe programy badań cyfrowych i wszystkie aspekty rozwoju technologii zostaną poddane ścisłej regulacji i kontroli ze strony państw. Autorzy omawianej tu prognozy nie mają wątpliwości, że trzy z przedstawionych przez nich scenariuszy kreślą ponurą wizję świata, zaś scenariusz zaprowadzenia cyberpokoju jest mało prawdopodobny, a jego realizacja – bardzo trudna dla polityków, choćby dlatego, że wymaga skupienia się na dialogu o dalszej transformacji cyfrowej, rezygnacji z dążenia do dominacji i wykazania przez Europę zdolności do działań wspólnych.

6.5. Polska na tle globalnej rywalizacji w dziedzinie nowych technologii komunikacyjnych i cyfrowych

• Nowe technologie w Polsce – etap diagnoz, deklaracji politycznych i projektów oraz cząstkowych wdrożeń • Próby wypracowania rozwiązań w warunkach silnego wpływu polityki

W sprawach dotyczących technologii i – szerzej – sztucznej inteligencji Polska znajduje się na etapie diagnoz i projektów oraz cząstkowych wdrożeń, zwłaszcza w sferze administracji, świadczeń zdrowotnych i ubezpieczeń społecznych (tu liderem jest ZUS). Stanowisko władz państwowych w globalnej konkurencji na polu inteligentnych technologii telekomunikacyjnych nowej generacji wynika z ogólnej strategii geopolitycznej rządu, związanej z dążeniem do utrzymania jak najlepszych stosunków z USA. O naszej pozycji w tej rywali-

zacji przesądza również poziom zaawansowania badań naukowych. Wprawdzie mamy tu pewne osiągnięcia, inżynierowie polscy są autorami nowatorskich projektów technologicznych, ale – patrząc ogólnie i ujmując rzecz eufemistycznie – Polska nie jest liderem w pracach nad sztuczną inteligencją. Nic też nie wskazuje, by mogła się stać samodzielnym graczem na międzynarodowym rynku technologii informatycznych. W obecnej sytuacji zdani jesteśmy na kooperację z państwami i firmami przodującymi w tej dziedzinie. Nie ulega wątpliwości, że na decyzje zakupowe podejmowane przez polskie władze wpływają przede wszystkim uwarunkowania polityczne: strategiczne relacje z USA oraz członkostwo w Unii Europejskiej. Równocześnie jednak trudne do pominięcia są uwarunkowania ekonomiczne, związane w szczególności z atrakcyjnymi finansowo ofertami chińskimi.

Biorąc pod uwagę rozbieżne przesłanki stojące u podstaw oczekiwanych decyzji o wyborze partnerów w pracach nad inteligentnymi technologiami, a być może także ryzyko retorsji ze strony odrzuconych oferentów, Polska zajmowała w tej sprawie do drugiej połowy 2019 r. postawę wyczekującą. Pierwsze przetargi na budowę sieci 5G przewidziano w Polsce na 2020 r. W przygotowanym przez rząd w połowie 2019 r. opracowaniu dotyczącym zasad rozwoju sieci 5G zaznaczono, że Polska nie wyklucza nikogo z udziału w budowie tej sieci, ale wszelkie decyzje dopuszczające określone podmioty do współdziałania muszą być uwarunkowane względami bezpieczeństwa. Badaniem ryzyka naruszenia bezpieczeństwa sieci przez poszczególne inwestycje miałyby się zajmować firmy telekomunikacyjne działające zgodnie ze specjalnymi regulacjami prawnymi przygotowywanymi przez rząd. Stanowisko władz polskich było na tym etapie jeszcze dość ogólne i wskazywało na różne warianty działań zmierzających do ograniczenia zagrożeń bezpieczeństwa informatycznego związanych z atakami zewnętrznymi i wewnątrzsystemowymi. Wyznaczono kierunki niezbędnych zmian w prawie krajowym i opowiedziano się za koordynacją rozwiązań systemowych i sprzętowych na poziomie Unii Europejskiej. Przyjęto, że przy rozstrzyganiu przetargów na częstotliwości 5G należy mieć na uwadze dywersyfikację dostawców infrastruktury i wymagania tzw. zaufanego dostawcy (*trusted vendor*), co odpowiada regułom obowiązującym w niektórych innych państwach europejskich, w tym w Wielkiej Brytanii i Niemczech[68].

W drugiej połowie 2019 r. władze polskie podjęły w sprawie sieci 5G decyzję wyraźnie umotywowaną politycznie. W trakcie wizyty wiceprezydenta USA Mike'a Pence'a, który w zastępstwie prezydenta Donalda Trumpa przy-

[68] https://cyfrowa.rp.pl/it/bezpieczenstwo/35835-rzadowa-analiza-o-5g-trafila-do-komisji-europejskiej?utm_source=rp&utm_medium=teaser_redirect. https://www.pap.pl/aktualnosci/news%2C493230%2Cmc-bezpieczenstwo-infrastrukturalne-i-cyfrowe-kluczowe-dla-sieci-5g.html.

był do Warszawy na obchody rocznicy wybuchu II wojny światowej, została podpisana deklaracja polsko-amerykańska o rozwoju sieci 5G. Z dokumentu tego wynika pośrednio, że władze polskie uznały za priorytet dobre stosunki z USA i dla osiągnięcia tego celu są skłonne odrzucić możliwość współpracy z dostawcami technologii z Chin[69]. Jak czytamy w serwisie Cyfrowa.RP.pl, „W powszechnym odbiorze deklaracja skierowana jest przeciwko chińskim dostawcom, w tym głównie Huawei, który zbudował ¾ sieci komórkowych 4G w Polsce, i może oznaczać, że telekomy nie będą mogły stosować rozwiązań tej firmy w sieciach 5G. To z kolei może oznaczać wyższe koszty wprowadzenia 5G przez telekomy, których sieci budował Huawei"[70]. Polska podjęła równocześnie próbę ulokowania na swoim terenie inwestycji, które są związane z rozwojem – konkurencyjnej wobec chińskiej oferty – technologii łączności 5G dostarczonej przez szwedzką firmę Ericsson[71]. Stanowisko rządu ma istotne znaczenie dla polskich firm telekomunikacyjnych. W chwili przygotowywania niniejszej publikacji Play, Orange i T-Mobile, których sieci 4G w dużej mierze budował Huawei, nie ogłosiły jeszcze strategii swojego działania. Cyfrowy Polsat, współpracujący już wcześniej z Nokią i Ericssonem, odstąpił od kontraktu z Huawei.

Kolejne wypowiedzi przedstawicieli rządu oraz informacje na temat polskiego stanowiska w sprawach inwestycji związanych z technologią 5G pokazują, że strategicznym założeniem, na którym mają się opierać działania w tym zakresie, jest zachowanie pełnej zgodności z ocenami i rekomendacjami amerykańskimi w ramach wspólnej polityki bezpieczeństwa. Nie wydaje się, aby to stanowisko miało ulec zmianie po wyborach prezydenckich w USA w 2020 r. Stawiając sobie za cel wyeliminowanie dostawców usług telekomunikacyjnych 5G „wysokiego ryzyka", Polska zamierza wprowadzić zasady bardziej restrykcyjne od tych, które proponuje się w Unii Europejskiej, co wyraźnie zapowiedział na początku 2020 r. ówczesny minister cyfryzacji Marek Zagórski. Polska chce też „uniezależnić się od jednego sprzedawcy". Ostateczne reguły obowiązujące w tym zakresie mają zostać potwierdzone w ustawie o bezpieczeństwie telekomunikacyjnym[72].

---

69 https://cyfrowa.rp.pl/telekomunikacja/37091-premier-i-wiceprezydent-usa-podpisali-deklaracje-o-sieciach-5g?utm_source=rp&utm_medium=teaser_redirect.

70 https://cyfrowa.rp.pl/telekomunikacja/37129-deklaracja-polski-i-usa-w-sprawie-5g-uderzyla-w-telekomy?utm_source=rp&utm_medium=teaser_redirect.

71 https://cyfrowa.rp.pl/telekomunikacja/36979-premier-leci-do-szwecji-po-wielkie-inwestycje-5g?utm_source=rp&utm_medium=teaser_redirect; https://cyfrowa.rp.pl/opinie/37011-wiceprezes-ericssona-polska-moze-jeszcze-zostac-europejskim-pionierem-w-5g?utm_source=rp&utm_medium=teaser_redirect.

72 https://www.politico.eu/article/poland-wants-to-go-beyond-5g-security-toolbox-restrictions.

Polska opowiedziała się na początku 2020 r. za tym, aby Europejski Kodeks Cyfrowy (Digital Services Act), który ma być przygotowany w Unii Europejskiej, zapewnił użytkownikom internetu większy zakres praw, m.in. poprzez regulacje dotyczące własności swoich danych na portalach społecznościowych. Nasz kraj chce też aktywnie uczestniczyć w realizacji unijnego programu „Cyfrowa Europa" (Digital Europe Programme), który z budżetem 8,1 miliarda euro ma być uruchomiony w 2021 r. dla finansowego wsparcia transformacji cyfrowej europejskich społeczeństw i gospodarek[73].

Trwają prace nad stworzeniem w Polsce infrastruktury chmury obliczeniowej administrowanej przez Operatora Chmury Krajowej (OChK), spółki powołanej przez PKO Bank Polski i Polski Fundusz Rozwoju. W 2019 r. przyjęto, że podstawą dostępu do usług w chmurze obliczeniowej stanie się technologia i centrum regionalne Google'a. Ta pierwsza w Europie Środkowej instalacja, dająca możliwość korzystania z rozwiązań chmurowych oferowanych w skali globalnej, ma łączyć wymogi bezpieczeństwa i zaawansowania technologicznego oraz zasadniczo przyspieszyć cyfryzację polskiej gospodarki[74].

W początku 2019 r. premier Mateusz Morawiecki poinformował o zamiarach wprowadzenia podatku cyfrowego w Polsce, wskazując, że wielkie korporacje powinny płacić podatki w miejscu, gdzie prowadzą biznes. Wpływy z tytułu takiego podatku oszacowano wówczas na 1 miliard złotych rocznie[75]. Planowane dochody zostały wpisane do założeń budżetu na 2020 r. W drugiej połowie 2019 r. okazało się jednak, że Polska (jak można sądzić – w imię zachowania dobrych stosunków z USA) zrezygnowała z planów wprowadzenia podatku cyfrowego. Nie udało się przy tym uniknąć konfuzji, bowiem opinia publiczna uzyskała informację na ten temat nie od polskiego rządu, lecz od wiceprezydenta USA Pence'a[76]. Od tego czasu projekty wprowadzenia podatku cyfrowego są w wypowiedziach przedstawicieli rządu wiązane przede wszystkim ze wspólnymi decyzjami, które mają być wypracowane w Unii Europejskiej oraz OECD.

Wpisanie przez Prawo i Sprawiedliwość przed wyborami do Parlamentu Europejskiego do pakietu programowego sprawy ograniczenia ochrony praw autorskich w internecie jednoznacznie pokazuje, że kwestie dotyczące internetu mogą stanowić nie tylko istotne uwarunkowanie polityki, lecz także jej przedmiot. W ten sposób można zinterpretować wypowiedź premiera Mora-

---

73 http://centrumprasowe.pap.pl/cp/pl/news/info/153675,36,mc-minister-cyfryzacji-w-brukseli-rozmowy-o-cyfrowej-przyszlosci-europy-(komunikat).

74 https://www.polska2041.pl/innowacje/news-nad-polske-nadciaga-cyfrowa-chmura,nId,3226619.

75 Serwis informacyjny TVN24 z 18.03.2019.

76 https://biznes.interia.pl/wiadomosci/news/cyfrowi-giganci-nie-zaplaca-podatku-w-polsce,2628004,4199.

wieckiego na konwencji wyborczej w Gdańsku w 2019 r., w której przyrzekał „wszystkim naszym wspaniałym youtuberom, blogerom, influencerom, forumowiczom, wszystkim internautom", że dla PiS wolność słowa w internecie jest „niezbywalnym imperatywem wolności gospodarczej"[77]. Podobnie trzeba traktować zapowiedź skierowania uchwalonych w UE regulacji do Trybunału Sprawiedliwości UE, zawartą w wystąpieniu Jarosława Kaczyńskiego w przededniu wyborów do Parlamentu Europejskiego[78].

[77] Serwis informacyjny Onet.pl z 30.03.2019.
[78] Serwis informacyjny PAP z 21.05.2019.

Rozdział siódmy

Cywilizacja cyfrowa jako przestrzeń gry i manipulacji politycznej

7.1. Internet jako instrument optymalizacji polityki, komunikacji politycznej i rządzenia

Niejednoznaczne oblicze polityczne internetu i cywilizacji cyfrowej • Internet jako narzędzie zindywidualizowanych, interaktywnych kontaktów masowych w czasie rzeczywistym, z pominięciem ograniczeń odległości • Internet jako standardowy instrument komunikacji politycznej, e-kampanii politycznej, e-mobilizacji i e-marketingu wyborczego • Komunikatory internetowe jako mechanizm uprawiania polityki przez przywódców współczesnych państw • Internet jako narzędzie wzmacniania partycypacji społecznej i politycznej

Sposoby i efekty wykorzystania internetu w dziedzinie spraw publicznych trzeba sytuować między wolnością i optymalizacją polityki a manipulacją, dezinformacją i destrukcją. Liczne przykłady pokazują, że może on być z powodzeniem wykorzystywany w procesach optymalizacji rządzenia, ale może być także narzędziem o znacznym potencjale destrukcji. Należy sądzić, że internet zachowa to swoje dwoiste oblicze także w przyszłości. Za pomocą interaktywnej komunikacji internetowej można współcześnie wspomagać tworzenie i prezentację programów politycznych, budowanie i aktywizowanie środowisk politycznych, polemikę z konkurentami politycznymi, a niejednokrotnie także gromadzenie funduszy wyborczych. Dzięki tej komunikacji są nawiązywane, tak ważne w działaniach publicznych, zindywidualizowane kontakty masowe w czasie rzeczywistym, bez ograniczeń wynikających z odległości. Promocja i konfrontacja polityczna w internecie tym się różni od działalności politycznej prowadzonej przy użyciu tradycyjnych środków: prasy, radia i telewizji, że umożliwia komunikowanie interaktywne, ale też – tu dotykamy ciemnej strony internetu – pozwala na działania w dużej mierze anonimowe lub prowadzone pod szyldem fałszywych tożsamości.

W XXI wieku standardem w komunikacji politycznej stały się e-kampanie polityczne, w tym e-mobilizacja i e-marketing wyborczy. Możliwości oddziaływania za pomocą narzędzi komunikacji elektronicznej są uwzględniane w programowaniu i prowadzeniu działalności politycznej oraz działań w ramach szeroko pojętego rządzenia. Ich pominięcie musiałoby być już obecnie uznane za nieracjonalny sposób postępowania.

Wartość i potencjał komunikacji politycznej w internecie dobitnie potwierdziły doświadczenia zebrane w okresie pandemii COVID-19, wywołanej przez koronawirusa SARS-CoV-2. W związku z wymogiem ograniczenia bądź zaprzestania bezpośrednich kontaktów społecznych, politycy pospiesznie przenosili wiosną 2020 r. swoje kontakty do internetu. Z dnia na dzień uruchamiano, często w trybie alarmowym, elektroniczne procedury debatowania i podejmowania decyzji w kolegialnych organach politycznych, w tym organach władzy publicznej. Komunikacja elektroniczna przeszła w tych warunkach ważny sprawdzian praktyczny, dowiodła swej użyteczności na płaszczyźnie aktywności politycznej. Nie można już mieć wątpliwości co do skuteczności – ale i potrzeby – kontaktowania się i oddziaływania za pomocą komunikacji internetowej w polityce. Należy się spodziewać, że w przyszłości działania polityczne będą w coraz większym stopniu prowadzone przy użyciu interaktywnych instrumentów komunikacji internetowej. W tej dziedzinie będą też doskonalone mechanizmy i zostanie podjęty wysiłek zmierzający do wyeliminowania mankamentów, które dały o sobie znać w czasie nagłego i wymuszonego przenoszenia polityki do internetu w związku z pandemią koronawirusa.

Powszechne wykorzystywanie narzędzi internetowych w polityce, jakie ma miejsce w sytuacji nadzwyczajnej wywołanej pandemią i związaną z nią przymusową izolacją społeczną, wpisuje się w proces zmian trwających od kilkunastu lat. Współcześni liderzy polityczni „zadomowili się" już w mediach społecznościowych oraz w przestrzeni komunikatorów cyfrowych. Wielu polityków konsekwentnie używa narzędzi komunikacji internetowej do kontaktów w sprawach publicznych. Przykładem może być prezydent Trump, który ze swojego prywatnego konta na Twitterze regularnie przekazywał komunikaty dotyczące prowadzonej polityki i innych kwestii o znaczeniu publicznym. Ta nowa forma kontaktowania się polityków ze światem zewnętrznym, także z otoczeniem międzynarodowym, oznacza odwrócenie tradycyjnego kierunku przepływu informacji na temat polityki, polegającego na tym, że media przekazują informacje upowszechnione wcześniej przez oficjalne agencje rządowe, obecnie bowiem to agencje informacyjne i prasa niejednokrotnie posiłkują się treściami zaczerpniętymi z wypowiedzi polityków w komunikatorach cyfrowych. Przykład aktywności Trumpa w mediach społecznościowych pokazuje, że wybierając tę drogę komunikacji społecznej, politycy muszą się liczyć z możliwością zablokowania swoich kontaktów z wyborcami przez administratorów

komunikatorów internetowych. Doszło do tego wiosną 2020 r., kiedy należąca do Amazona witryna do transmisji wideo tymczasowo zawiesiła konto Trumpa, motywując to jego „nienawistnym zachowaniem" w związku z policyjną interwencją, która doprowadziła do śmierci czarnoskórego mężczyzny, a następnie w lipcu tegoż roku, gdy zamknięto program SMS-ów Trumpa, i w sierpniu – wtedy bowiem prezydent USA został zablokowany na Facebooku po zamieszczeniu tekstu zawierającego ocenę, że pandemia COVID-19 jest mniej niebezpieczna niż sezonowa grypa. Sprawczość administratorów mediów społecznościowych dała też znać o sobie w okresie wyborów prezydenckich w USA w listopadzie 2020 r. Tweety Donalda Trumpa zawierające zapewnienia o własnym wyborczym zwycięstwie i zarzuty w sprawie rzekomych nieprawidłowości w procesach głosowania i liczenia głosów były regularnie blokowane lub też opatrywane adnotacją mówiącą o tym, że zawierają „treści, które mogą wzbudzać kontrowersje lub wprowadzać w błąd w kwestiach dotyczących udziału w wyborach lub innej procedurze obywatelskiej", oraz informacją, iż zabrania się korzystania z usług komunikatorów elektronicznych „w celu manipulowania lub ingerowania w wybory".

Internet daje nowe możliwości zwiększania partycypacji społecznej i politycznej oraz usprawniania komunikacji politycznej. Obywatele mają dzięki komunikacji internetowej bieżący dostęp do licznych danych, co daje im asumpt do interaktywnego włączenia się w sprawy publiczne. Mogą korzystać z różnych mechanizmów elektronicznej partycypacji (w tym konsultacji i dyskusji). Wśród rozwiązań e-administracji pojawiają się – szczegółowo analizuję to w dalszej części pracy – sposoby załatwiania na odległość licznych spraw urzędowych. Kontakty zdalne zadomowiły się już w edukacji i nauce. Zasadniczo zwiększają się możliwości kontrolowania podmiotów sprawujących władzę publiczną przez społeczeństwo. W ramach rządzenia narzędzia cyfrowe wspomagają pozyskiwanie informacji i zarządzanie nimi w czasie rzeczywistym, programowanie, synergiczne wykorzystywanie zasobów, usprawnianie wprowadzania w życie podjętych decyzji, ich ewaluację i promocję w społeczeństwie. Wybór dokonany na podstawie ogólnej reguły postępowania, opartej przeważnie na doświadczeniu, jest wspomagany, a niejednokrotnie wręcz wypierany przez decydowanie za pomocą algorytmów. Podstawowe znaczenie uzyskują w tym przypadku określone sekwencje logiczne (opisane najczęściej w postaci indeksu liczb, przy użyciu języka matematyki i informatyki) służące do matematycznego sformułowania istoty problemu i wyznaczające sposób (swoisty przepis) przechodzenia od zdefiniowanej parametrycznie sytuacji wyjściowej do zdefiniowanej także parametrycznie sytuacji ustalonej jako cel[1].

[1] Zob.: J.J. Nowak, *Wprowadzenie do matematycznego formułowania problemów decyzyjnych*, Warszawa 1999; N. Mileszyk, B. Paszcza, A. Tarkowski, *AlgoPolska. Zautomatyzowane podejmowanie decyzji w służbie społeczeństwu*, Kraków 2019.

7.2. Internet jako narzędzie politycznej dezinformacji i manipulacji

Internet jako narzędzie szerzenia dezinformacji umacniających podziały kulturowe i polityczne między ludźmi • Rozbudowa infrastruktury cyberwojny psychologicznej • Fałszywe obrazy upowszechniane w rzeczywistości wirtualnej jako nowa forma broni

Dostrzegając pozytywne efekty rozwoju internetu, nie można pominąć faktu, że stał się on także narzędziem politycznej dezinformacji i manipulacji – na niespotykaną dotąd skalę. Zasoby danych zgromadzonych w przestrzeni cyfrowej to coraz ważniejsze narzędzie wykorzystywane w konfrontacji politycznej. Posługując się nimi, można w przestrzeni politycznej kreować, pozycjonować i niszczyć dowolne osoby, inicjatywy, instytucje etc. Można identyfikować grupy wyborców i budować strategie porozumiewania się z nimi. Indywidualna komunikacja masowa z użyciem narzędzi internetowych oznacza możliwość nie tylko łączenia ludzi ponad granicami administracyjnymi, lecz także szerzenia dezinformacji, upowszechniania treści umacniających podziały kulturowe i polityczne między ludźmi. Tak więc, nowe rozwiązania technologiczne niosą ze sobą zarówno niezaprzeczalne korzyści, jak i liczne niebezpieczeństwa związane – najogólniej rzecz biorąc – z próbami manipulowania świadomością osób, na które pragnie się w określony sposób wpłynąć.

Internet jest doskonałym instrumentem prowadzenia działań psychologicznych, które – zgodnie z definicją przyjętą w siłach zbrojnych USA – są planowymi działaniami mającymi na celu przekazanie wybranym adresatom wyselekcjonowanych informacji i wskazówek „z zamiarem wpłynięcia na ich emocje, motywację, rozumowanie i w efekcie zachowanie". Chodzi tu o wywołanie lub wzmocnienie zachowań korzystnych dla podmiotu realizującego tego typu działania[2].

W sytuacji, w której wizerunki medialne nabierają coraz większego znaczenia, a nieraz znaczą więcej niż sprawdzone fakty, stałym elementem otoczenia rządzenia jest – rozrastająca się – machina politycznej manipulacji wirtualnej, która odciska swój, mniej lub bardziej widoczny, ślad na rządzeniu. Za pomocą cyfrowych technik, przy zastosowaniu narzędzi sztucznej inteligencji (AI), preparowane są przekazy upowszechniane następnie wśród milionów odbiorców. Fałszywe komunikaty słowne i obrazowe tworzone w rzeczywistości wirtualnej są wykorzystywane w walce o całkiem realne sprawy. Te mistyfikacje stają się tym groźniejsze, że przeciętny użytkownik internetu słabo radzi sobie z ich rozpoznawaniem. Istnieje więc pilna potrzeba opracowania skutecznych,

[2] T. Kacała, *Działania psychologiczne wybranych państw*, Toruń 2016, s. 9.

zaawansowanych narzędzi do wyłapywania oszukańczych treści pojawiających się w sieci i do identyfikowania ich twórców.

Trwają zaawansowane prace badawcze i wdrożeniowe, które mają doprowadzić do ograniczenia zagrożeń związanych z fałszywymi przekazami internetowymi[3]. Rozmiary i agresywność dezinformacji prowadzonej na platformach informacyjnych i komunikacyjnych w internecie zaczynają też zagrażać żywotnym interesom finansowym właścicieli i administratorów platform. Nagrania, filmy czy zdjęcia spreparowane techniką zwaną deepfake – z podrabianymi wizerunkami i wypowiedziami znanych osób publicznych, stają się przedmiotem publicznych dyskusji, często wywołują skandale polityczne i obyczajowe, a kiedy zostają zdemaskowane, naruszają podstawowy zasób kapitałowy mediów społecznych, jakim jest zaufanie. Wygenerowana przez algorytmy wypowiedź Baracka Obamy, w której były prezydent nazywa Donalda Trumpa głupkiem, fałszywki z wypowiedziami Władimira Putina i Trumpa, filmy ze spreparowanymi cyfrowo scenami porno z udziałem osób publicznych – to przykłady deepfake'ów, które budzą nieufność do platform, na których się ukazują, i wikłają te platformy w spory prawne. Łatwość przygotowania i upowszechniania nieprawdziwych wizerunków w przestrzeni internetowej przyczynia się do tego, że żyjemy – jak to określono w komentarzu portalu Politico – w erze niepewności. Jeśli wszystko można wiarygodnie sfałszować, to „skąd możemy wiedzieć, że coś jest prawdziwe?". Są to idealne warunki do zaprzeczania wszystkiemu, co zostało pokazane w mediach społecznościowych, a jest niewygodną prawdą[4].

Manipulacja w komunikacji internetowej okazuje się niezwykle skuteczna. Trzeba się więc liczyć z tym, że będzie stosowana także w przyszłości, a jej techniki będą udoskonalane. Należy do asortymentu środków, których państwa, organizacje, siły polityczne oraz politycy używają do oddziaływania na świadomość ludzi w celu realizacji własnych interesów. Na ogół pozostaje bezkarna (a przynajmniej daje poczucie bezkarności osobom, które ją stosują), gdyż w internecie nietrudno jest zachować anonimowość.

Łatwość wywołania sztucznego ruchu w komunikacji internetowej pozwala zafałszowywać rzeczywiste rozmiary poparcia dla poszczególnych inicjatyw czy poglądów. Dobry przykład takich działań przedstawia Oliver Milman, opisując wykrytą przez naukowców aktywność botów na Twitterze, która towarzyszyła ogłoszeniu w czerwcu 2017 r. deklaracji prezydenta Trumpa w sprawie wyjścia USA z porozumień paryskich dotyczących ochrony klimatu[5]. W sposób zorganizowany upowszechniano wówczas w internecie przekonanie, że nie

[3] https://konkret24.tvn24.pl/tech,116/wyscig-zbrojen-xxi-wieku-technologie-deepfake-coraz-lepsze-i-grozniejsze,960083.html.

[4] https://www.politico.eu/article/deepfake-videos-the-future-uncertainty.

[5] https://www.theguardian.com/technology/2020/feb/21/climate-tweets-twitter-bots-analysis.

zagraża nam katastrofa klimatyczna. Badacze z Brown University, po przebadaniu 6,5 miliona tweetów na temat kryzysu klimatycznego opublikowanych w dniach poprzedzających decyzję prezydenta i w ciągu miesiąca po niej, ustalili, że jedna czwarta wszystkich tych tweetów była każdego dnia automatycznie wytwarzana przez boty. Były to w zdecydowanej większości głosy poparcia dla decyzji Donalda Trumpa. Niejednokrotnie sięgano do dodatkowo opłaconej opcji gwarantującej większą widoczność.

W czasach przełomów politycznych czy w momentach nasilania się w społeczeństwie napięć i lęków pojawiają się irracjonalne interpretacje zdarzeń, także teorie spiskowe, skrajnie subiektywne komentarze itp. Trudne czasy zwiększają społeczne zapotrzebowanie na rozumienie tego, co się dzieje – ludzie poszukują sensu wydarzeń, a na tym próbują coś ugrać manipulatorzy, populiści, politykierzy. Znajduje to potwierdzenie w okresie walki z pandemią w 2020 r. Jedna z instytucji Unii Europejskiej (Europejska Służba Działań Zewnętrznych) wskazuje, że w działania zmierzające do wykorzystania w celach politycznych sytuacji walki z pandemią, tj. do rozpowszechniania w mediach społecznościowych fałszywych raportów i innych dezinformacji online, włączyły się Rosja i Chiny[6]. Pandemia stała się przedmiotem zmasowanej manipulacji w internecie, a aktywni na tym polu są także politycy. W mediach społecznościowych negowanie zagrożenia epidemicznego – a nawet zaprzeczanie istnieniu koronawirusa – często łączy się ze snuciem różnego rodzaju teorii spiskowych. Swój „wkład" w dezinformacyjną narrację na temat pandemii wniósł też, jak już wspomniałem, prezydent Trump.

Trwa swoisty pojedynek między twórcami narzędzi pozwalających identyfikować uczestników komunikacji elektronicznej a twórcami coraz bardziej zaawansowanych technologii maskowania faktycznej tożsamości nadawców informacji i komentarzy. W gruncie rzeczy jest to wyścig z czasem, ponieważ na udane próby demaskowania fałszerstw i manipulacji strona przeciwna szybko odpowiada tworzeniem nowych narzędzi, takich jak: Tor (The Onion Router), Tails (The Amnesic Incognito Live System), serwery proxy (tzw. serwery przekaźnikowe), generatory fałszywych tożsamości i anonimowe skrzynki e-mail[7]. Tak więc, z pewnością nadal będą doskonalone metody oddziaływania i techniki kamuflowania faktycznej tożsamości podmiotów aktywnych w internecie.

Produkowanie fake newsów, zatrudnianie internetowych hejterów i trolli, uruchamianie oprogramowania kreującego sieci botów oraz prowadzenie szeptanej propagandy internetowej – wszystko to stało się elementem walki

---

6 https://www.politico.eu/article/russia-china-disinformation-coronavirus-covid19-facebook-google.

7 K. Kucharski, *Narzędzia anonimizujące działania w Internecie jako instrumentarium do prowadzenia operacji informacyjnych w ramach wojny hybrydowej*, Agencja Bezpieczeństwa Wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego", wydanie specjalne, październik 2015, s. 85 i nast.

politycznej. Nic nie wskazuje na to, aby w internecie można się było wkrótce uporać z dezinformacją, fałszywymi kontami i trollami; dotychczasowe problemy zostają, w dalszym ciągu są trudne do rozwiązania, a dochodzą nowe niepokojące zjawiska. Komentatorzy zwracają uwagę, że może wzrastać zagrożenie manipulacjami dokonywanymi przez rodzimych aktorów politycznych, a więc tego typu działań można się spodziewać nie tylko ze strony nadawców operujących ze źródeł położonych poza granicami danego państwa[8]. Amerykańska dziennikarka Lydia Polgreen, była redaktorka naczelna HuffPost, stwierdziła, że pojawia się w tym kontekście niebezpieczne zaburzenie ekosystemu informacyjnego, które przekłada się negatywnie na funkcjonowanie systemów politycznych, podważa zaufanie do wyborów i instytucji demokratycznych, a w efekcie destabilizuje istniejący porządek światowy[9].

7.3. Wybory powszechne jako czas nasilania się zagrożeń związanych z nadużyciami nowych technologii w świecie polityki

Media społecznościowe i narzędzia cywilizacji cyfrowej środkami coraz intensywniej wykorzystywanymi w trakcie kampanii wyborczych i referendalnych • Wybory powszechne jako czas agresywnych działań dezinformacyjnych w internecie i naruszeń bezpieczeństwa systemów informatycznych • Wybory prezydenckie w USA w 2016 r. świadectwem niebezpiecznych dla demokracji związków brudnej polityki z postępem technologicznym • Skuteczność komunikacji internetowej w walce o głosy niezdecydowanych wyborców

Media społecznościowe oraz rozwiązania i technologie cyfrowe zostały na trwałe wpisane do arsenału środków stosowanych w trakcie kampanii wyborczych i referendalnych. Prekursorami używania narzędzi internetowych do prowadzenia swoich kampanii wyborczych stali się amerykańscy politycy ubiegający się o urząd prezydenta kraju. Dość powszechnie wskazuje się w tym kontekście przykład kampanii wyborczej w 2008 r., w której Barack Obama wykorzystał z sukcesem cyfrowe narzędzia komunikacji, docierając do elektoratu za pomocą swojej własnej witryny społecznościowej oraz swoich profili na portalach społecznościowych, szczególnie na MySpace i Facebooku[10].

---

8 https://www.politico.com/news/2019/12/01/fight-against-disinformation-2020-election-074422.

9 https://www.theguardian.com/commentisfree/2019/nov/19/the-collapse-of-the-information-ecosystem-poses-profound-risks-for-humanity.

10 J. Nowak, *Aktywność obywateli online. Teorie a praktyka*, Lublin 2011, s. 214 i nast. Zob. też: M. Kożdoń-Dębecka, *Internet w prezydenckich kampaniach wyborczych w USA w latach 2000–2012*, Warszawa 2019; K. Oświęcimski, M. Lakomy, *E-kampanie prezydenckie w USA i w Polsce*, Kraków 2017.

Po narzędzia elektroniczne sięgnął także Donald Trump w kampanii wyborczej w 2016 r., co w ogromnej mierze przyczyniło się do jego zwycięstwa. Mobilna aplikacja o nazwie America First miała wówczas około 120 tysięcy zarejestrowanych użytkowników. Jest rzeczą znamienną, że polityk ten, uznając, iż nastawione krytycznie do konserwatystów globalne sieci społecznościowe nie są mu życzliwe, także jako prezydent szukał alternatywnych kanałów elektronicznych kontaktów z wyborcami. Przed wyborami w 2020 r. jego sztab polityczny uruchomił własną aplikację na smartfony, mającą wzmacniać i aktywizować polityczną „armię Trumpa". Według informacji uzyskanych przez Politico, na wiele miesięcy przed wyborami 2020 r. zaczęto tworzyć bazę danych potencjalnych wyborców i przeznaczono milionowe sumy na reklamy cyfrowe i kontakty elektroniczne, które miały się przyczynić do dalszego powiększania grupy zwolenników. Równocześnie tworzono profile poszczególnych osób pozwalające indywidualizować treści przekazu elektronicznego kierowane do konkretnych wyborców w celu wzmocnienia poparcia z ich strony[11].

Politycy w USA nie są pod tym względem wyjątkiem. Instytucjonalni i personalni aktorzy polityczni na całym świecie angażują się w działania za pomocą nowych technologii, w efekcie czego „Polityka przeniknęła do cyberprzestrzeni, a cyberprzestrzeń zaczyna odgrywać funkcję coraz istotniejszej areny dla procesów politycznych"[12]. Internet stał się na trwałe ważnym środkiem elektronicznej komunikacji wyborczej[13]. Przykładowo w Wielkiej Brytanii w ciągu miesiąca przed wyborami do Izby Gmin w 2019 r. partie polityczne wydały ponad 2 miliony funtów na ukierunkowane reklamy elektroniczne. Należy zauważyć, że zarówno komisja wyborcza, jak i Biuro Komisarza ds. Informacji wskazywały na brak dostosowania krajowych zasad finansowania kampanii do wymogów związanych z efektywnym śledzeniem i nadzorowaniem wyborczych wydatków online[14]. Organy te powinny otrzymać pomoc od administratorów mediów społecznościowych, jednak na kilka dni przed wyborami doszło do awarii systemu na Facebooku, który ma wzmacniać – zgodnie z deklaracjami Marka Zuckerberga – transparentność sieci społecznościowej. Uniemożliwiło to zbadanie źródła płatnych wiadomości na Facebooku o łącznej wartości 7,4 miliona funtów. Niedostępnych było 40% brytyjskich reklam politycznych. Po usunięciu awarii okazało się, że blokowała ona dostęp do reklam wszystkich partii istniejących w Wielkiej Brytanii[15].

---

11 https://www.politico.com/story/2019/09/08/anti-conservative-bias-trump-1481831.

12 M. Lakomy, L. Porębski, N. Szybut, *Polityka 2.0…*, s. 10.

13 J. Żurawski, *Internet jako współczesny środek elektronicznej komunikacji wyborczej i jego zastosowanie w polskich kampaniach parlamentarnych*, Kraków 2010.

14 https://www.politico.eu/article/uk-general-election-electoral-commission-louise-edwards-facebook-google-advertising.

15 https://www.politico.eu/article/facebook-political-ads-general-election-united-kingdom.

Nie wolno zapominać o tym, że elektronicznymi technologiami komunikacyjnymi, a także innymi narzędziami tworzonymi na użytek cywilizacji cyfrowej, można się posługiwać w kampanii wyborczej i w trakcie samych wyborów na dwa – skrajnie różne – sposoby. Za w pełni akceptowalną należy uznać sytuację, kiedy uczestnicy wyścigu wyborczego i ich otoczenie używają owych narzędzi, respektując wspólnie ustalone zasady komunikacji, promocji i rywalizacji politycznej. Z kolei jako całkowicie niedopuszczalne – z prawnego i moralnego punktu widzenia – trzeba oceniać wykorzystywanie tych narzędzi do manipulacji i dezinformacji, szerzenia kłamstw i nienawiści. Taki splot nowoczesnej technologii i brudnej polityki najczęściej wiąże się z komercjalizacją komunikacji internetowej.

Wybory powszechne współcześnie prowokują zainteresowane – politycznie lub finansowo – strony do prowadzenia działań dezinformacyjnych w internecie i naruszeń bezpieczeństwa systemów informatycznych. Wybory coraz częściej odbywają się w warunkach internetowej wojny informacyjnej, w której biorą udział poszczególne państwa, siły polityczne i indywidualni politycy. Od połowy drugiej dekady XXI wieku, na skutek – przypisywanej Rosji – interwencji w przebieg wyborów w USA i w innych państwach oraz w związku z manipulacjami dotyczącymi referendum w sprawie wyjścia Wielkiej Brytanii z Unii Europejskiej, stało się jasne, że za pomocą fałszerstw internetowych oraz ingerencji w systemy informatyczne można wpływać na wynik wyborów. Niejednokrotnie dochodzi do zakłóceń wynikających z nadużywania internetu przez podmioty działające na terenie danego państwa.

Można z dużą pewnością przyjąć, że prawdziwym poligonem, na którym przetestowano sprzęgnięcie podejrzanych praktyk politycznych i nowych technologii, były wybory prezydenckie w USA w 2016 r. Niezależnie od – sygnalizowanego już wyżej – wykorzystania w kampanii wyborczej danych osobowych ponad 80 milionów użytkowników Facebooka udostępnionych firmie Cambridge Analytica, w tych wyborach miały miejsce wyraźne interwencje zewnętrzne w obszarze komunikacji internetowej ukierunkowane na kształtowanie wyniku wyborczego. Amerykańscy analitycy cyberbezpieczeństwa piszą w swojej książce o prawdziwej inwazji internetowej w kampanii wyborczej 2016 r., w czasie której nadawcy, zidentyfikowani jako pochodzący z Rosji, zarzucili internautów amerykańskich swoimi komentarzami i opiniami. Tylko przy wykorzystaniu Twittera, w ramach operacji noszącej znamiona ataku hakerskiego, mającej na celu zmanipulowanie opinii publicznej, boty administrowane przez podmiot rosyjski (Internet Research Agency) „wygenerowały 2,2 miliona twitów związanych z wyborami w ciągu zaledwie trzech ostatnich miesięcy przed wyborami. W ciągu ostatniego półtora miesiąca Twitter stwierdził, że rosyjską propagandę wysłano do użytkowników 454,7 miliona razy”[16].

[16] P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny…*, s. 191.

Były dyrektor FBI James Comey, podsumowując działania służb specjalnych prowadzone z udziałem analityków CIA, NSA, FBI i ODNI (Biura Dyrektora Wywiadu Narodowego), stwierdził w swoich wspomnieniach, że ich uczestnicy doszli „do zdecydowanego, graniczącego z pewnością i podzielanego przez wszystkich przekonania, że Rosja na ogromną skalę ingerowała w wybory prezydenckie w Stanach Zjednoczonych (…) poprzez cyberataki, media społecznościowe oraz rosyjskie media państwowe, stosując różne strategie: podważanie wiary społeczeństwa w amerykański proces demokratyczny, oczernianie Hillary Clinton i zmniejszanie jej szans na zwycięstwo wyborcze oraz wspieranie Donalda Trumpa”[17]. Jak pisze Comey, „Jądrem rosyjskiej kampanii była publikacja szkodliwych e-maili wykradzionych organizacjom i osobom związanym z Partią Demokratyczną. Pojawiły się również sygnały zakrojonych na szeroką skalę prób przeniknięcia do baz danych zawierających prowadzone przez poszczególne stany rejestry wyborców”[18].

Z analiz firmy Symantec wynika, że propagandowy atak z wykorzystaniem kanałów internetowych (głównie mediów społecznościowych), mający wpłynąć na wyniki amerykańskich wyborów w 2016 r., musiał być przygotowywany przez dłuższy czas. Wskazuje na to m.in. fakt, że – jak ustalono po zbadaniu prawie 3900 kont i 10 milionów tweetów użytych w tym ataku – średnie opóźnienie między utworzeniem konta a pierwszym tweetem wynosiło 177 dni. O zasięgu operacji na Twitterze świadczy fakt, że konto mające najwięcej udostępnień zebrało 6 milionów retweetów. Autorzy operacji musieli mieć do dyspozycji znaczne środki, umożliwiające wyzyskiwanie lokalnych informacji, odwoływanie się do tekstów prawdziwych uczestników sieci oraz prowadzenie kont także przez spersonalizowanych, a nie tylko zautomatyzowanych operatorów[19].

Udział Rosji w manipulowaniu zachowaniami wyborczymi został w dużym stopniu potwierdzony w raporcie Roberta Muellera, mianowanego prokuratorem specjalnym do nadzorowania federalnego śledztwa w tej sprawie. W dokumencie tym zapisano, że nie ma jednoznacznych dowodów na współpracę sztabu wyborczego Trumpa z Rosją. Zarazem jednak – jak głosi raport – w sztabie tym wiedziano już od kwietnia 2016 r. o przejęciu przez Rosję tysięcy e-maili Hillary Clinton i wierzono, że mieszanie się tego kraju w wybory prezydenckie w USA politycznie się opłaci, gdyż jest wymierzone przede wszystkim w główną rywalkę Trumpa[20]. W oświadczeniu wstępnym w trakcie przesłuchania w Kongresie w dniu 24 lipca 2019 r. Mueller powiedział, iż „dochodzenie wykazało, że rosyjski rząd ingerował w (…) wybory w sposób wszechstronny i systematyczny”, i dodał: „W trakcie mojej kariery widziałem

17 J. Comey, *Wyższa lojalność. Prawda, kłamstwo i przywództwo*, Kraków 2019, s. 330–331.
18 Tamże, s. 295.
19 https://www.politico.com/story/2019/06/05/study-russia-cybersecurity-twitter-1353543.
20 https://www.politico.com/story/2019/04/18/mueller-report-summary-key-findings-1280879.

wiele wyzwań dla naszej demokracji. Wysiłki rosyjskiego rządu, by ingerować w nasze wybory, należą do najpoważniejszych”[21].

Szukając dzisiaj wspólnego mianownika sytuacji politycznej w różnych państwach, można uznać, że jest nim polaryzacja sceny politycznej. To swego rodzaju *signum temporis*. W wielu krajach – w Polsce, niestety, również, jednak zjawisko to nie ominęło państw o bardziej niż u nas ugruntowanej demokracji i kulturze politycznej – doszło do głębokich podziałów politycznych w szerokich masach społeczeństwa, tzw. zwykli ludzie bezwzględnie opowiadają się za którymś z ostro zwalczających się obozów politycznych. W skład tych obozów, obok polityków i struktur instytucjonalnych, wchodzą sprzymierzone siły: „swoje” media, środowiska kultury i sztuki, zespoły ekspertów. Przypadki zmiany identyfikacji politycznej ludzi, czyli przepływy zwolenników między elektoratami obozu rządzącego i opozycji, są bardzo rzadkie. Niewiele znaczą tu nawet pewne słabości, potknięcia i błędy popełniane przez polityków, często zresztą przysparzają im one sympatii (co znajduje odbicie w ocenach: „swój chłop”, „jest taki jak my” itp.). Na zmianę afiliacji politycznej ludzi zasadniczo może wpłynąć jakaś nadzwyczajna okoliczność, wydarzenie o charakterze skandalu politycznego[22], finansowego lub obyczajowego, które wstrząsa opinią publiczną. (Inna sprawa, że obserwując szereg najrozmaitszych afer, społeczeństwo do pewnego stopnia znieczula się na nie, i można się zastanawiać, co naprawdę jest w stanie wywołać reakcję odrzucenia).

W sytuacji, gdy żaden z obozów politycznych nie ma jednoznacznej przewagi, a bardzo liczna grupa osób trwale identyfikuje się z którymś z nich, na znaczeniu zyskuje grono wyborców niezdecydowanych, bo to oni mogą przesądzić o wyniku wyborów powszechnych. Narzędzia komunikacji internetowej bardzo dobrze sprawdzają się w walce o ich głosy. Sztaby wyborcze starają się przede wszystkim odpowiedzieć sobie na pytanie, jak przekonać do siebie niezdecydowanych i nieaktywnych politycznie, jak ich – mówiąc potocznie – rozgryźć, co im obiecać, czym postraszyć. Odpowiedzi na te pytania stają się w istocie ważniejsze niż kwestie programowe.

Cyberprzestrzeń nadaje się wyjątkowo dobrze do stosowania technik oddziaływania perswazyjnego i wywierania wpływu, zwłaszcza wtedy, gdy dysponuje się konkretną wiedzą o sylwetkach politycznych swoich zwolenników i adwersarzy oraz o charakterystycznych cechach poszczególnych grup wyborców. Zasoby informacyjne internetu są doskonałym źródłem tej – kluczowej w działaniu polityków – wiedzy. Monitorowanie i analizowanie dostępnych w cyberprzestrzeni danych zaczyna być stałym elementem aktywności

---

21 https://www.politico.com/story/2019/07/24/mueller-opening-statement-full-text-transcript-annotated-1428431.

22 O roli skandalu w polityce zob. J.B. Thompson, *Skandal polityczny. Władza i jawność w epoce medialnej*, Warszawa 2010.

polityków. Rozpoznanie sytuacji jest dobrym punktem wyjścia do działań ukierunkowanych na wzmocnienie swojej pozycji politycznej i osłabienie pozycji adwersarzy. Te działania przybierają formę zorganizowanych kampanii wizerunkowych (ofensywnych i/lub obronnych) prowadzonych nie tylko za pomocą własnych narzędzi internetowych (stron internetowych, poczty e-mail, blogów), lecz także za pośrednictwem uczestników dyskusji internetowych, którzy w ramach fałszywych profili i tożsamości podejmują próby manipulowania ludźmi.

Wspomniana już afera z danymi użytkowników Facebooka przekazanymi sztabom politycznym przez Cambridge Analytica pokazała, że manipulacja w internecie może prowadzić do spaczenia obrazu świata realnego, a w konsekwencji do zachwiania racjonalności zachowań (czego dowodem może być fakt, że ludzie popierają coś lub kogoś wbrew swemu obiektywnemu interesowi, np. ekonomicznemu). Od połowy drugiej dekady XXI wieku kolejnych przykładów skoordynowanej manipulacji informacjami i narracjami w przekazie internetowym, w tym z wykorzystaniem coraz doskonalszych algorytmów, dostarczają wybory w większości państw, m.in. we Francji i w Niemczech oraz w Indiach i Ameryce Południowej.

Dezinformacja staje się poważnym wyzwaniem dla demokracji, tym bardziej że trwa proces ciągłego doskonalenia metod i narzędzi prowadzenia działań online, które mają na celu manipulowanie świadomością wyborców, wzmacnianie sił radykalnych, zaostrzanie podziałów społecznych, obniżanie frekwencji wyborczej lub podważanie zaufania do wyników wyborów. Pesymistyczną prognozę sytuacji w tej dziedzinie przedstawia Samuel Woolley, specjalizujący się na University of Texas w Austin w badaniach nad relacjami między automatyzacją, nowymi technologiami, polityką i mediami społecznościowymi. Jego zdaniem, wraz z rozwojem narzędzi sztucznej inteligencji, m.in. tworzeniem systemów imitujących ludzki głos, uczeniem maszynowym oraz kształtowaniem się rzeczywistości wirtualnej, przestrzeń polityczna będzie zmierzać ku cyfrowej dystopii. Nastanie epoka swoistej „propagandy obliczeniowej", tj. cyfrowej dezinformacji i nękania politycznego w internecie. Wspomniany badacz zaznacza jednak, że ten niepokojący scenariusz „technologicznego ataku" na rzeczywistość i prawdę nie musi się ziścić – przyszłość jest w rękach ludzi i tylko ludzie są w stanie odwrócić niepomyślny rozwój wydarzeń[23].

Mimo pojawiania się takich akcentów optymizmu, łatwo można popaść w przygnębienie z powodu inwazji fałszerstw, kłamstw, półprawd i manipulacji w polityce. Rzecz nie sprowadza się do przywołanych wcześniej przykładów – wyborów prezydenckich w USA i referendum w Wielkiej Brytanii, i nie

[23] Zob. S. Woolley, *The Reality Game: How the Next Wave of Technology Will Break the Truth*, New York 2020.

dotyczy tylko Rosji czy Chin. Politycy na całym świecie używają rozwiązań i narzędzi cyfrowych do manipulowania wyborami i wyborcami. W swoim raporcie z 2019 r. Freedom House zwraca uwagę na trzy dominujące modele internetowej ingerencji w wybory, zaznaczając równocześnie, że niejednokrotnie działania prowadzone w tej sferze wzajemnie się wzmacniają i są sukcesywnie modyfikowane, aby utrudnić ich wykrycie i zablokowanie[24].

Pierwszy z wyodrębnionych w raporcie modeli aktywności jest oparty na środkach informacyjnych. Obejmuje dyskretne i coraz bardziej inteligentne manipulowanie treściami na korzyść określonych państw lub sił politycznych za pomocą przekazów propagandowych, fałszywych wiadomości, tekstów opłacanych komentatorów, treści rozpowszechnianych z kont automatycznych (botów) oraz z przejętych kont w mediach społecznościowych. Tylko w ciągu jednego roku, który był poddany analizie, autorzy omawianego dokumentu odnotowali przypadki tego rodzaju aktywności podczas wyborów w 24 krajach. Jednym z przykładów były manipulacje związane z wyborami parlamentarnymi w Indiach w 2019 r., w ramach których rządząca Indyjska Partia Ludowa (Bharatiya Janata Party, BJP) i opozycyjny Indyjski Kongres Narodowy (INC) wprowadziły do internetu odpowiednio 1,2 miliona i 800 tysięcy swoich zwolenników w celu szerzenia przez nich dezinformacji na platformach elektronicznych, takich jak WhatsApp i Facebook. Inny przykład manipulacji informacyjnej pochodzi z Filipin, gdzie w maju 2019 r. rozpowszechniano specjalnie spreparowane informacje w zamkniętych grupach internetowych.

W drugim modelu ingerencji w przebieg wyborów lub referendów wykorzystuje się środki techniczne do ograniczania dostępu do niezależnych źródeł wiadomości i narzędzi komunikacji. Polega to głównie na blokowaniu i hakowaniu wybranych stron lub całkowitym odcinaniu dostępu do internetu. Jak stwierdzono w raporcie, takie działania w rozpatrywanym okresie były podejmowane w procesie wyborczym w 14 krajach. Podano następujące przykłady: kampania na rzecz zmian w konstytucji w Egipcie, gdzie przed referendum w 2019 r. zamknięto dostęp do stron internetowych niewygodnych dla prezydenta Abdela Fattaha al-Sisi; zablokowanie przed wyborami parlamentarnymi w Kambodży w lipcu 2018 r. kilkunastu niezależnych serwisów informacyjnych; sytuacja w lipcu 2018 r. w Zimbabwe w trakcie wyborów prezydenta; wielokrotne blokowanie w Bangladeszu przed wyborami w grudniu 2018 r. Skype'a używanego do kontaktów przez polityków opozycyjnych; zniszczenie w trybie ataku DDoS (*distributed denial of service* – rozproszona odmowa usługi) strony internetowej partii opozycyjnej przed wyborami prezydenckimi w Meksyku w lipcu 2018 r.

---

[24] https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/digital-election-interference.

Trzeci model ingerencji w przebieg wyborów opiera się na wykorzystywaniu środków prawnych do wprowadzania ograniczeń w dostępie do internetu oraz do karania za ujawnione w komunikacji elektronicznej negatywne stanowisko wobec rządzących. Według informacji zebranych przez autorów omawianego raportu, po takie środki sięgnęły władze w 12 krajach. Przykładowo: w Malawi władze aresztowały dwóch działaczy mediów społecznościowych za zamieszczenie w internecie treści, które zostały uznane za obrażające prezydenta przed wyborami w maju 2019 r.; w Turcji policja aresztowała kilka osób za obrażanie prezydenta Recepa Tayyipa Erdoğana w mediach społecznościowych przed wyborami prezydenckimi i parlamentarnymi w czerwcu 2018 r.; w Indiach przed wspomnianymi wyżej wyborami aresztowano dziennikarza za krytykę na Facebooku premiera Narendry Modiego; w Bangladeszu przed wyborami parlamentarnymi przyjęto regulacje ustawowe przewidujące karę więzienia za „propagandę internetową", które wykorzystano następnie do aresztowania redaktora jednego z kanałów informacyjnych.

7.4. Walka z patologiami cyfrowymi jako przedmiot działań systemowych i obszar nowych manipulacji

Ofensywa na rzecz wzmocnienia bezpieczeństwa informacyjnego i informatycznego w wyniku uznania patologii cyfrowych za zagrożenie dla demokracji • Różnice między amerykańskim i europejskim modelem regulacji ograniczających patologię w działaniu internetowych mediów społecznościowych • Problem regulacji internetowych reklam politycznych • Wymuszona aktywność globalnych operatorów internetowych na rzecz ograniczenia patologii w korzystaniu z technologii elektronicznych w polityce • Manipulacje i spory polityczne związane z walką z dezinformacją w cyberprzestrzeni

Demokracja musi się dzisiaj mierzyć z poważnym przeciwnikiem – zagrożeniami informacyjnymi i informatycznymi. W związku z tym, coraz więcej państw i organizacji międzynarodowych podejmuje systemowe działania zmierzające do ograniczenia ryzyka, jakie niesie ze sobą agresja propagandowa w internecie, nasilająca się podczas wyborów powszechnych. W ramach tych działań są podejmowane próby dostosowania prawa do nowych realiów komunikacji społecznej. Równocześnie poszczególne państwa i grupy państw prowadzą działania operacyjne polegające na monitorowaniu ingerencji informacyjnych i informatycznych. Rządy tych państw tworzą wyspecjalizowane zespoły do walki z dezinformacją internetową.

W Stanach Zjednoczonych przed częściowymi wyborami do Kongresu w 2018 r. stworzono – dla wzmocnienia bezpieczeństwa informacyjnego i informatycznego procesu wyborczego – mechanizmy współdziałania służb

specjalnych z operatorami internetu. W tzw. pokojach wojny w sposób systemowy monitorowano sytuację w komunikacji internetowej i na tej podstawie podejmowano decyzje o blokowaniu milionów fałszywych kont, które rozpowszechniały nieprawdziwe informacje. W kolejnych miesiącach przedmiotem intensywnych prac i żywej dyskusji politycznej stało się ograniczenie niebezpieczeństwa zmanipulowania wyników amerykańskich wyborów prezydenckich w 2020 r. W służbach specjalnych uruchomiono specjalne mechanizmy instytucjonalne wspomagające monitorowanie bezpieczeństwa procesu wyborczego. W połowie 2019 r. utworzono w strukturach wspólnoty wywiadowczej stanowisko specjalnego koordynatora do spraw bezpieczeństwa wyborów[25]. Szczegółową analizę zagrożeń internetowych zawierały raporty senackiej komisji do spraw wywiadu, w tym raport z połowy 2019 r., w którym opisano wcześniejsze, przypisywane Rosji, działania zakłócające wybory w 2016 r., m.in. próby uzyskania dostępu do systemów wyborczych w 50 stanach[26]. Wyrażono opinię, że jest bardzo prawdopodobne, iż Rosja kolejny raz podejmie próby zakłócenia wyborów w USA poprzez profesjonalnie przeprowadzone ataki propagandowe, przy wykorzystaniu mediów społecznościowych, oraz poprzez ingerencję w systemy teleinformatyczne infrastruktury wyborczej. Na tym tle pojawiły się daleko idące żądania zmian w prawie oraz projekty utworzenia „bezpartyjnej, pozarządowej Komisji Wyborczej ds. Cyfrowych w celu ochrony integralności (…) naszych wyborów przez wykrywanie, ujawnianie, ocenianie i przeciwdziałanie dezinformacji”[27].

W listopadzie 2019 r. we wspólnym oświadczeniu Prokuratora Generalnego, Sekretarza Obrony, pełniących obowiązki Sekretarza Bezpieczeństwa Wewnętrznego i Dyrektora Wywiadu Narodowego oraz Dyrektora FBI i Dowództwa Cybernetycznego USA[28] podkreślono, że „bezpieczeństwo wyborów jest najwyższym priorytetem dla rządu Stanów Zjednoczonych”. Zapewniono, że „rząd federalny traktuje priorytetowo udostępnianie danych wywiadowczych dotyczących zagrożeń oraz zapewnia wsparcie i usługi, które poprawiają bezpieczeństwo infrastruktury wyborczej w całym kraju”. Dano przy tej okazji wyraz przekonaniu, że przeciwnicy polityczni „chcą podważać (…) instytucje demokratyczne, wpływać na nastroje społeczne i wpływać na politykę rządu. Rosja, Chiny, Iran i inne zagraniczne nieprzyjazne podmioty będą starały się ingerować w proces głosowania lub wpływać na postrzega-

25 https://www.dni.gov/index.php/newsroom/news-articles/item/2024-odni-creates-new-position-dedicated-to-election-security.

26 https://www.politico.com/story/2019/07/25/russia-interference-2016-election-1435436.

27 https://www.politico.com/magazine/story/2019/07/25/russias-prepared-to-interfere-in-2020-will-the-us-be-ready-227477.

28 https://www.dni.gov/index.php/newsroom/press-releases/item/2063-joint-statement-from-doj-dod-dhs-dni-fbi-nsa-and-cisa-on-ensuring-security-of-2020-elections.

nie wyborców. Przeciwnicy mogą próbować osiągnąć swoje cele za pomocą różnych środków, w tym kampanii w mediach społecznościowych, kierując operacjami dezinformacyjnymi lub przeprowadzając destrukcyjne cyberataki na infrastrukturę stanową i lokalną".

Pod koniec drugiej dekady XXI wieku wzmogły się działania na rzecz bezpieczeństwa informacyjnego i informatycznego w Unii Europejskiej. Sukcesywnie przybywa mechanizmów mających charakter zapory przeciwko naruszeniom bezpieczeństwa w przestrzeni internetowej. Prawdziwa batalia wokół bezpieczeństwa informacyjnego i informatycznego miała miejsce w związku z wyborami do Parlamentu Europejskiego w 2019 r. Unia Europejska przeznaczyła wówczas na przeciwdziałanie dezinformacji w internecie 5 milionów euro. Wzmocniono rozwiązania zwalczające dezinformację w środowisku cyfrowym, które uruchomiono po raz pierwszy już w 2015 r. Utworzono system wczesnego ostrzegania i wprowadzono ścisłe monitorowanie przypadków dezinformacji w internecie[29]. Nałożono liczne obowiązki informacyjne na koncerny ze sfery komunikacji internetowej. Opracowano kodeks postępowania w zakresie zwalczania dezinformacji (Code of Practice on Disinformation) i doprowadzono do tego, że w październiku 2018 r. globalne platformy informacyjne zobowiązały się – na zasadzie samoregulacji – do przestrzegania tego kodeksu. W efekcie doszło do zamknięcia milionów fałszywych kont na Facebooku, YouTubie i Twitterze. Wzmożono aktywność tzw. Wschodniej Strategicznej Grupy Roboczej (East Strategic Communication Task Force) odpowiedzialnej za monitorowanie działań dezinformacyjnych oraz funkcjonującego od 2017 r. Europejskiego Centrum ds. Zwalczania Zagrożeń Hybrydowych w Helsinkach.

Po wyborach do Parlamentu Europejskiego w 2019 r., Unia Europejska oskarżyła Rosję, pierwszy raz tak otwarcie, o planowe i zmasowane działania dezinformacyjne, dokumentując kilkaset konkretnych przypadków. Według przedstawionej opinii, aktywność Rosji związana z wyborami europejskimi była ukierunkowana na obniżenie frekwencji wyborczej, polaryzację debat przedwyborczych i manipulację preferencjami wyborców. Komisja Europejska podała, że około 600 stron i grup, które usunięto w związku z rozpowszechnianiem dezinformacji w kilku państwach członkowskich Unii, wygenerowało łącznie 763 miliony wyświetleń[30].

W komunikacie Komisji Europejskiej wydanym 14 czerwca 2019 r.[31] stwierdzono, że przed wyborami do Parlamentu Europejskiego miała miejsce

---

[29] https://eeas.europa.eu/headquarters/headquarters-homepage/54866/action-plan-against-disinformation_en.

[30] *Miliardy kont usuniętych na Facebooku przed eurowyborami. „Rosyjskie źródła chciały zdławić frekwencję"*, Konkret24 z 16.06.2019.

[31] https://ec.europa.eu/poland/news/190614_disinformation_pl. Tam też linki do innych publikacji UE na temat bezpieczeństwa wyborów, w tym: planu działania na rzecz zwalczania dezin-

skoordynowana wroga aktywność, m.in. z wykorzystaniem botów i fałszywych kont, mająca na celu rozpowszechnianie na platformach internetowych materiałów pogłębiających podziały. W tym komunikacie przedstawiciele Komisji Europejskiej odpowiedzialni za sprawy jednolitego rynku cyfrowego, sprawiedliwości, bezpieczeństwa oraz gospodarki cyfrowej i społeczeństwa cyfrowego oświadczyli, że podjęte działania, w tym ustanowienie na poziomie europejskim i krajowym sieci ds. wyborów, pomogły chronić demokrację przed próbami manipulacji i przyczyniły się do ograniczenia wpływu operacji dezinformacyjnych. Komunikat głosił, że wrogie podmioty, w tym zagraniczne – zwłaszcza te, które mają rosyjskie powiązania – stale zmieniają swoje strategie, zaś zwalczanie dezinformacji stanowi wspólne, długofalowe wyzwanie dla instytucji UE i państw członkowskich. Podkreślono w nim szczególną odpowiedzialność platform internetowych za zwalczanie dezinformacji i odnotowano, że „Facebook, Google i Twitter poczyniły pewne postępy we wdrażaniu kodeksu postępowania w zakresie zwalczania dezinformacji". Przypomniano, że w sprawach bezpieczeństwa wyborów UE podjęła czworakie działania. Po pierwsze – zwiększono zdolności do identyfikowania dezinformacji i przeciwdziałania jej za pośrednictwem grupy zadaniowej ds. komunikacji strategicznej i komórki UE ds. syntezy informacji o zagrożeniach hybrydowych (Hybrid Fusion Cell) w ramach Europejskiej Służby Działań Zewnętrznych oraz systemu wczesnego ostrzegania. Po drugie – nawiązano współpracę z platformami i przedstawicielami branży internetowej przystępującymi na zasadzie dobrowolności do kodeksu postępowania w zakresie zwalczania dezinformacji. Po trzecie – podjęto działania mające na celu podnoszenie świadomości społecznej w przedmiocie dezinformacji i zwiększanie odporności społeczeństwa na nią. Po czwarte – wspierano wysiłki państw członkowskich na rzecz zapewnienia integralności wyborów i wzmocnienia odporności systemów demokratycznych.

Agnieszka Legucka w analizie opublikowanej przez Polski Instytut Spraw Międzynarodowych przypomniała, że „Rosja wykorzystuje do szerzenia dezinformacji media tradycyjne oraz internet, zwłaszcza media społecznościowe. Rosyjskie media prorządowe dysponują dużym zasięgiem i budżetem, np. RT i Sputnik operują w 100 państwach i prowadzą audycje w 30 językach, a roczny budżet RT wynosi ok. 270 mln euro i może konkurować z BBC World (budżet ok. 300 mln euro) czy z France Media Monde, właścicielem France24 (budżet ok. 260 mln euro). (…) Ważnym narzędziem dezinformacji jest tzw. fabryka trolli – Agencja Badań Internetowych (ABI), której właścicielem jest Jewgienij Prigożin, współpracownik Władimira Putina. Miesięczny budżet ABI to ok. 1 mln euro. Działa ona od 2013 r. i zatrudnia rotacyjnie ok. 80 osób,

formacji, wspólnego sprawozdania w sprawie realizacji planu działania na rzecz zwalczania dezinformacji i pakietu działań dotyczących zapewnienia wolnych i uczciwych wyborów europejskich.

podzielonych na sekcje zagraniczne. Trolle mają za zadanie prowadzić dyskusje w różnych językach europejskich i wywoływać skrajne emocje w internecie”[32].

Zachodzą dwa równoległe procesy: z jednej strony – upowszechnianie różnych form zorganizowanej dezinformacji politycznej w internecie, z drugiej – systemowe zwalczanie trolli i innych elementów infrastruktury internetowych fałszerstw i zakłóceń bezpieczeństwa. Te drugie działania wykraczają poza kwestie związane z zapewnieniem bezpieczeństwa wyborów. Trwają prace nad całościową standaryzacją niedopuszczalnych ingerencji internetowych i rozwiązaniami technologicznymi pozwalającymi identyfikować fałszywe informacje oraz narracje i inne formy dezinformacji w mediach społecznościowych i na platformach internetowych.

Podejście europejskie do zwalczania dezinformacji w internecie zostało przedstawione w komunikacie Komisji Europejskiej z 2018 r.[33]. Stwierdzono w nim, że dezinformacja podważa zaufanie do instytucji, mediów cyfrowych i tradycyjnych oraz szkodzi demokracjom przez utrudnianie obywatelom podejmowania świadomych decyzji, staje się podstawą radykalnych i ekstremistycznych idei i działań oraz ogranicza wolność słowa. Jak czytamy w dokumencie: „Głównym obowiązkiem podmiotów państwowych w zakresie wolności słowa i wolności mediów jest powstrzymanie się od ingerencji i cenzury oraz zapewnienie środowiska sprzyjającego włączeniu społecznemu i pluralistycznej debacie publicznej”. Komisja jednocześnie podkreśla, że istnieje potrzeba podjęcia kompleksowych działań politycznych i że w obliczu wyzwań związanych z dezinformacją „(…) nie możemy pozostać bezczynni”. Wymaga tego powaga sytuacji: „Masowe kampanie dezinformacyjne w internecie są często wykorzystywane przez różne podmioty krajowe i zagraniczne w celu siania nieufności i tworzenia napięć społecznych, co może mieć poważne konsekwencje dla naszego bezpieczeństwa. (…) kampanie dezinformacyjne prowadzone przez państwa trzecie mogą stanowić część zagrożeń hybrydowych dla bezpieczeństwa wewnętrznego, w tym procesów wyborczych, w szczególności w połączeniu z cyberatakami”. Komunikat wskazuje, że sposoby rozprzestrzeniania dezinformacji w internecie opierają się na algorytmach (wynikających z modelu biznesowego platform komunikacyjnych i decydujących o kolejności wyświetleń informacji), na reklamach cyfrowych i na technologiach internetowych (w tym usługach zautomatyzowanych, symulowanych profilach i tzw. fabrykach trolli).

W 2019 r. grupa ekspertów Komisji Europejskiej, pracujących od stycznia 2018 r. nad wzmocnieniem bezpieczeństwa informacyjnego w internecie, ustaliła na potrzeby działań operacyjnych definicję dezinformacji. Przyjęto, że

---

[32] A. Legucka, *Walka z rosyjską dezinformacją w Unii Europejskiej*, „Biuletyn PISM” 2019, nr 111.

[33] *Zwalczanie dezinformacji w internecie: podejście europejskie*, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, COM(2018) 236 final.

przez dezinformację, która może zagrażać demokratycznym procesom i wartościom, należy rozumieć „nieprawdziwe, niedokładne lub wprowadzające w błąd informacje, które są opracowane, przedstawiane i rozpowszechniane w celu osiągnięcia zysku lub z zamiarem wyrządzenia szkody publicznej”[34]. Zgodnie ze stanowiskiem prezentowanym przez Unię Europejską, potrzebne są silne powiązania między innowacją a polityką, aby kształtować przyszłe media społecznościowe i sieci jako bezpieczne, otwarte, kreatywne i godne zaufania środowisko[35]. Za główne zadania uznano ściślejszą współpracę państw członkowskich UE w tym zakresie (m.in. wspólne reagowanie na zagrożenia dezinformacją), zwiększanie wykrywalności oraz poprawę wyników analizy dezinformacji, pogłębianie współdziałania z platformami internetowymi i przemysłem, co ma służyć zwalczaniu dezinformacji oraz podnoszeniu świadomości społeczeństwa i jego odporności na dezinformację.

Jeśli chodzi o ograniczanie patologii w działaniu internetowych mediów społecznościowych, widać różnice między podejściem amerykańskim i europejskim. W USA są podejmowane w tym celu przede wszystkim próby wykorzystywania antymonopolowych przepisów i instytucji. Natomiast w Unii Europejskiej nacisk został położony na ochronę danych osobowych i blokowanie języka nienawiści. Trzeba przy tym zaznaczyć, że w USA przeciwdziałanie monopolizacji rynku mediów społecznościowych nie jest łatwe, gdyż założona w 1914 r. Federalna Komisja Handlu, stanowiąca podstawowe narzędzie instytucjonalne do walki z monopolami i do ochrony praw konsumentów, jest nie całkiem przygotowana pod względem kadrowym i finansowym do przeciwdziałania szkodliwym działaniom globalnych firm technologicznych. Przestarzałe prawo mocno utrudnia zastosowanie przepisów antymonopolowych przeciwko praktykom firm z Doliny Krzemowej. Przepisy ustawy o komunikacji z 1996 r. (w tym kluczowej w tych sprawach sekcji 230) nie dają możliwości rozliczania gigantów medialnych z treści zamieszczanych na ich platformach komunikacyjnych[36]. Z kolei w Unii Europejskiej, gdzie – jak wyżej wspomniałem – szczególny akcent kładzie się na ochronę danych osobowych użytkowników sieci internetowych, wzmocnienie gwarancji prywatności w obszarze administrowania tymi danymi i na blokowanie języka nienawiści, po przepisy antymonopolowe sięga się tylko pomocniczo. Znalazło to wyraz m.in. w uruchomieniu postępowań w sprawie dominacji Google’a i Apple’a

---

[34] *Walka z dezinformacją w internecie: eksperci apelują o większą przejrzystość platform internetowych*, Strasburg, 12 marca 2018 r., http://europa.eu/rapid/press-release_IP-18-1746_pl.htm. Zob. też raport końcowy grupy doradców, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

[35] Zob. https://ec.europa.eu/digital-single-market/en/policies/social-media-and-networks-innovation-and-policy.

[36] https://www.politico.com/story/2019/07/09/online-industry-immunity-section-230-1552241.

w sklepach z aplikacjami[37] oraz w nałożeniu na Google od 2017 r. grzywien o łącznej wysokości 8 miliardów euro za działania naruszające wolną konkurencję[38]. W podejściu europejskim zasadnicze znaczenie ma też zamiar zbliżenia standardów działania offline i online w sprawach politycznych, zwłaszcza dotyczących prowadzenia kampanii politycznych.

Wśród wyzwań związanych z patologiami w użytkowaniu mediów społecznościowych szczególnie istotne staje się uregulowanie kwestii internetowych reklam politycznych. Praktyka pokazuje bowiem, że reklamy te są w dużym stopniu wykorzystywane do dezinformacji i manipulacji prowadzonej przez podmioty, które ukrywają się pod fałszywymi tożsamościami. W USA, zgodnie z projektem ustawy z 2019 r. o uczciwych reklamach (Honest Ads Act), platformy cyfrowe skupiające ponad 50 milionów unikalnych miesięcznych użytkowników mają być zobowiązane do prowadzenia publicznego rejestru reklamodawców, którzy wydali ponad 500 dolarów na reklamy w ciągu ostatniego roku. Rejestr ma zawierać: cyfrową kopię reklamy, opis grupy docelowej, koszty reklamy, nazwę wspieranego podmiotu personalnego lub instytucjonalnego, dane kontaktowe nabywcy reklamy[39]. Znaczną reglamentację internetowych reklam politycznych wprowadzono w Kanadzie, aby ograniczyć zagrożenie obcą ingerencją w parlamentarną kampanię wyborczą w 2019 r. W związku z tym, na operatorów internetowych (Facebook, Google i in.) nałożono obowiązek utworzenia rejestru podmiotów kupujących reklamy polityczne oraz przyjęto zasadę, że nabywcy reklam politycznych mają dokonywać transakcji za pośrednictwem kanadyjskiego konta bankowego używanego wyłącznie do tego celu[40]. W Unii Europejskiej w maju 2018 r. weszły w życie przepisy w sprawie ochrony danych osobowych, które mówią, że jeśli dany podmiot zbiera czyjeś dane w określonym celu, musi uzyskać zgodę na ewentualne przekazanie ich dalej lub wykorzystanie w innym celu. Nowe regulacje zobowiązują też firmy do poinformowania w czasie nie dłuższym niż 72 godziny osoby, której dane dotyczą, o prawdopodobnym naruszeniu ochrony tych danych. W razie złamania tych przepisów przewidziano możliwość nakładania kar w wysokości do 4% globalnego rocznego obrotu firmy. Na uwagę zasługuje opinia, że Europa nie powinna się uzależniać od postępów w regulowaniu kwestii reklam politycznych w USA. Jak dosadnie ujął to lord David Puttnam: „Nie możemy siedzieć i czekać, aż zachodnie wybrzeże USA zdecyduje, że chcą się zachowywać jak ludzie”[41].

---

37 https://www.politico.com/story/2019/08/07/apple-antitrust-europe-united-states-1449919.

38 https://www.politico.eu/article/google-antitrust-competition-data-luxembourg-hearing-appeal.

39 https://www.cbsnews.com/news/facebook-hearings-what-is-the-honest-ads-act.

40 https://www.politico.com/story/2019/09/04/canada-foreign-election-meddling-1698209.

41 https://www.theguardian.com/media/2019/nov/05/uk-cant-rely-on-us-platforms-to-regulate-political-ads-inquiry-told.

Spór z powodu reklam politycznych zamieszczanych na platformach internetowych świadczy o tym, że nie ma w tych sprawach łatwych rozwiązań. Przykładowo, formułowane jest żądanie wprowadzenia odpowiedzialności administratorów tych platform za treść zamieszczanych ogłoszeń. Swoje stanowisko przedstawił m.in. aktor i komik Sacha Baron Cohen, który zaatakował Facebook i inne platformy mediów społecznościowych za umożliwienie szerzenia się dezinformacji i mowy nienawiści, i bez ogródek wypalił, że dla zysku Facebook wyświetlałby nawet reklamy Hitlera[42]. Jednak nie brakuje także opinii, że wprowadzenie nadzoru nad treścią ogłoszeń oznaczałoby cenzurę przekazów internetowych. Pojawiają się też propozycje rozwiązań kompromisowych. Clare O'Donoghue Velikić, kierująca w przeszłości w Facebooku zespołem do spraw reklam politycznych, zwraca uwagę, że profilowanie grupowe danych przez firmy jest praktykowane od wielu lat w marketingu politycznym i handlowym, zaś kluczowe znaczenie ma jednoznaczne ustalanie tożsamości zleceniodawców poszczególnych reklam i stworzenie potencjalnym odbiorcom reklam możliwości sprawdzenia, kto jest ich autorem i ile kosztowało zamieszczenie na platformie danego materiału, oraz ewentualne znakowanie politycznego charakteru reklam[43].

Chcąc uniknąć zagrożenia swojej pozycji, także globalni operatorzy internetowi podejmują wymuszone działania nastawione na ograniczanie patologii w korzystaniu z technologii elektronicznych w polityce. Ujawniane przypadki nadużyć w dysponowaniu przez sieci danymi swoich użytkowników oraz głośne afery demaskujące manipulacje polityczne w komunikacji internetowej nadwyrężają zaufanie użytkowników do mediów społecznościowych, a jednocześnie zwiększają presję na przyjęcie szczegółowych i restrykcyjnych regulacji tej sfery. Realne stają się plany objęcia korporacji wywodzących się z Doliny Krzemowej procedurami antymonopolowymi oraz kolejnymi śledztwami prowadzonymi w USA przez coraz więcej podmiotów na poziomie federalnym i stanowym, w tym przez Departament Sprawiedliwości, Federalną Komisję Handlu, obie izby Kongresu i prokuratorów[44]. Wysoce prawdopodobne są też restrykcyjne zmiany prawa w kwestiach istotnych dla globalnych korporacji internetowych i komunikacyjnych.

Globalne korporacje mediów internetowych przyjęły w 2018 r. taktykę polegającą na uspokajaniu sytuacji, tzn. przekonywaniu, że dostrzegają problem i w niezbędnym zakresie przeciwdziałają zjawiskom niepokojącym polityków oraz opinię publiczną. W tej taktyce można wyodrębnić trzy elementy. Pierwszym z nich jest samokrytyczne podejście do dotychczas stosowanych rozwiązań w zakresie ochrony danych użytkowników, monitorowania ruchu

[42] https://www.theguardian.com/technology/2019/nov/22/sacha-baron-cohen-facebook-propaganda.
[43] https://www.theguardian.com/commentisfree/2019/dec/06/facebook-political-ads-social-media.
[44] https://www.politico.com/story/2019/07/26/silicon-valley-anti-trust-1619256.

w sieci, treści przekazów zamieszczanych na swoich platformach oraz postępowania w dziedzinie kontraktowania i upowszechniania reklam, w tym przede wszystkim tzw. politycznych reklam problemowych. Drugim elementem taktyki przyjętej przez globalne korporacje internetowe jest eksponowanie tezy, że nieprawidłowości to już przeszłość, zaś nowe zasady ich działania gwarantują jakościową zmianę w tej dziedzinie. W związku z tym przedstawiciele kierownictw poszczególnych mediów społecznościowych obszernie informują o podejmowanych wysiłkach na rzecz wykrycia i wyeliminowania przypadków wykorzystania ich platform i narzędzi internetowych do celów nagannych politycznie, moralnie czy obyczajowo. Trzecim elementem taktyki tychże korporacji jest konsekwentne dążenie do ograniczenia kontroli zewnętrznej w swoich firmach i przeciwstawianie się obarczaniu ich odpowiedzialnością za treści zamieszczane przez użytkowników. Próby ustanowienia takiej kontroli są ukazywane jako zagrożenie wolności informacji, komunikacji społecznej i wyrażania opinii oraz wypełniania misji mediów społecznościowych, która polega na łączeniu i zbliżaniu do siebie ludzi na całym świecie.

O tym, że korporacje internetowe przyjęły taką właśnie taktykę obrony swoich interesów, dowodnie świadczy treść zeznań, jakie Mark Zuckerberg złożył w amerykańskim Senacie w 2018 r. w związku z wykorzystaniem danych użytkowników Facebooka w wyborach prezydenckich w USA w 2016 r. Zuckerberg przyznał się wówczas do błędów polegających na niewystarczającej ochronie danych użytkowników, które otworzyły drogę do manipulacji politycznych, m.in. poprzez fake newsy, zagraniczne interwencje w wybory i mowę nienawiści. Równocześnie zapewnił, że wdrożono już niezbędne zmiany systemowe w kierowanej przez niego firmie. W swoim wpisie na Facebooku wyraził opinię, że ingerowanie w wybory jest problemem wykraczającym poza jakąkolwiek platformę społecznościową, i stwierdził, że z tego powodu popiera ustawę o uczciwej reklamie (Honest Ads Act), a także stworzenie mechanizmów weryfikacji tożsamości i lokalizacji nadawców reklam politycznych oraz reglamentacji reklam problemowych, które mają kontekst polityczny. Podobne stanowisko szef Facebooka przedstawił w swojej korespondencji z Komisją Europejską[45].

Mnożą się sygnały wskazujące, że państwa są coraz bardziej zdeterminowane, aby wykorzystać swoje możliwości prawne i techniczne do blokowania dezinformacji, której źródłem są media społecznościowe. Jak się wydaje, administratorzy platform internetowych przyjmują do wiadomości konieczność poddania się niektórym regulacjom państwowym. Przemawiając w lutym 2020 r. na konferencji w sprawie bezpieczeństwa w Monachium, Zuckerberg

[45] https://tvn24bis.pl/ze-swiata,75/facebook-poprze-ustawe-w-sprawie-reklam-politycznych,827802.html.

określił Facebook jako formę pośrednią między gazetą a firmą telefoniczną. Przypomniał, że Facebook zatrudnia obecnie 35 tysięcy pracowników zajmujących się monitorowaniem treści pod kątem bezpieczeństwa, co zasadniczo ogranicza zagrożenie demokratycznych wyborów, jakie stwarza dezinformacja szerzona w internecie. Obiecał poparcie swojej korporacji dla regulacji państwowych w sprawach dotyczących wyborów, dyskursu politycznego, prywatności i obrotu danymi. Zaznaczył jednak równocześnie, że nie mogą to być rozwiązania uderzające w wolność internetu. Zwrócił też uwagę, że Facebook publikuje 100 miliardów informacji każdego dnia i nie jest możliwe ich szczegółowe sprawdzanie. Jak podkreślił, jego firma przeszła z modelu postępowania reaktywnego na proaktywny w sprawach zagrożeń bezpieczeństwa informacyjnego, co znalazło odzwierciedlenie w fakcie, że 99% treści sprzyjających działalności terrorystycznej oraz 80% treści mowy nienawiści jest usuwanych przed interwencją zewnętrzną[46].

Deklaracje w sprawie przyjęcia w Facebooku nowego modelu biznesowego, eksponującego prawa użytkowników i uznającego ich prywatność za priorytet, muszą być traktowane z dystansem. Jak poinformował „Guardian", jeszcze w połowie 2019 r. rozmowy prowadzone na Messengerze, którego właścicielem jest Facebook, były nagrywane i poddawane analizie przez zewnętrznych współpracowników w celu ulepszenia jakości narzędzi do przekładania mowy na tekst. Dotyczyło to użytkowników, którzy zgodzili się na transkrypcję swoich rozmów. Przy okazji wyszło na jaw, że podobna praktyka była stosowana w przypadku Apple'a, Google'a i Amazona oraz popularnego komunikatora Skype (w odniesieniu do osób, które aktywowały funkcję automatycznego tłumaczenia wypowiedzi)[47]. Także deklaracje kierownictw mediów społecznościowych o położeniu kresu nadużyciom popełnianym przy użyciu reklam politycznych, zwłaszcza tzw. reklam problemowych, trzeba przyjmować z dużą ostrożnością. Działania w tej dziedzinie okazują się bowiem mało skuteczne. Może o tym świadczyć wykorzystanie w 2019 r. płatnych reklam zamieszczanych w Google'u i na Facebooku do kampanii online atakującej Manfreda Webera i Fransa Timmermansa, kandydatów na przewodniczącego Komisji Europejskiej. Reklamy te zawierały linki przekierowujące użytkowników, którzy je oglądali, na artykuły przedstawiające w negatywnym świetle obu kandydatów. Firmy emitujące te reklamy odmówiły odpowiedzi na pytania, kto był ich zleceniodawcą, ile zapłacono za ich wyświetlanie, ile osób do nich dotarło i do których użytkowników kierowano reklamy[48].

---

46 https://www.theguardian.com/technology/2020/feb/15/mark-zuckerberg-facebook-must-accept-some-state-regulation.

47 https://tvn24bis.pl/ze-swiata,75/facebook-nagrywal-i-udostepnial-probki-rozmow-z-messengera,961131.html.

48 https://www.politico.eu/article/secret-ad-campaign-targets-top-jobs-race.

Mało przekonujące są również zapewnienia ze strony mediów społecznościowych, że udało im się zahamować tworzenie narzędzi manipulacji w swoim obszarze działania. W połowie 2019 r. badacze z Centrum Doskonałości Komunikacji Strategicznej NATO, które zajmuje się m.in. identyfikacją potencjalnych ingerencji zagranicznych w internecie, bez większego trudu zakupili w ramach swojego eksperymentu około 54 tysięcy nieautentycznych interakcji w mediach społecznościowych: fałszywych obserwujących, polubień, komentarzy lub obrazów treści online[49].

Dla mediów społecznościowych reklamy to istotny element dochodów. Przykładowo tylko w 2018 r. dochód brutto Facebooka z tytułu reklam w Wielkiej Brytanii wzrósł o prawie 30% i osiągnął rekordową wartość 1,6 miliarda funtów[50]. Uwarunkowania finansowe sprawiają, że stanowisko koncernów internetowych w kwestii ograniczeń w reklamach jest zmienne i niejednolite. W drugiej połowie 2019 r. Jack Dorsey, prezes Twittera, poinformował o wprowadzeniu w swoim serwisie zakazu zamieszczania płatnych reklam politycznych. Stwierdził, że „uzyskanie zasięgów przekazu politycznego powinno być zasłużone, a nie kupione", zaś reklamy polityczne bardzo często zawierają fake newsy i treści typu deepfake (informacje prawdziwe z ukrytym fałszywym przesłaniem)[51]. Decyzja Twittera postawiła w trudnej sytuacji prezesa Facebooka Marka Zuckerberga, który w sprawie reklam politycznych prezentuje niejednoznaczne stanowisko: chociaż bowiem deklaruje, że dostrzega zagrożenia ze strony reklam, to powstrzymuje się przed jednoznacznym ich zakazem, odwołując się przy tym do potrzeby zagwarantowania wolności informacji[52].

Według prognoz Advertising Analytics i Cross Screen Media dotyczących rynku reklamowego, wydatki na reklamę polityczną w kampanii wyborczej 2020 r. miały sięgać ogółem nawet 6 miliardów dolarów. Przewidywano, że 1,6 miliarda dolarów zostanie wydanych na wideo cyfrowe, a Facebook i Google będą pozyskiwać większość tych środków. Jak poinformował portal Politico, od maja 2018 r. do października 2019 r. Facebook zarobił 857 milionów dolarów na reklamach politycznych i problemowych, zaś Google i platforma wideo YouTube – 122 miliony dolarów. Twitter ujawnił, że z reklam politycznych emitowanych w kampanii podczas śródterminowych wyborów w USA w 2018 r. uzyskał około 3 milionów dolarów[53].

---

49 https://www.politico.eu/article/social-media-inauthentic-behavior-google-facebook-twitter-nato-stratcom.

50 https://www.theguardian.com/technology/2019/oct/11/facebook-paid-just-28m-on-record-16bn-earnings-in-the-uk.

51 https://www.polsatnews.pl/wiadomosc/2019-10-30/rewolucja-na-twitterze-zmiany-odczuja-rowniez-polacy/?ref=slider.

52 https://www.politico.com/news/2019/10/31/google-political-ads-063429.

53 https://www.politico.com/news/2019/10/30/twitter-dropping-all-political-ads-000308.

Stanowisko administratorów mediów społecznościowych w sprawie reklam politycznych należy odczytać jako wyraz woli zachowania zysków przy równoczesnym ograniczeniu krytyki ze strony podmiotów dążących do wyeliminowania tej formy promocji politycznej. Media społecznościowe konsekwentnie zmierzają do zmniejszenia zakresu swojej odpowiedzialności za fałszywe treści zawarte w reklamach i dążą do zaakceptowania zasady, że to sami użytkownicy internetu powinni decydować, czy reklamy akceptują czy też je odrzucają[54]. Przeciwnicy takiej taktyki wskazują na jej fałszywą podstawę, tj. pominięcie oddziaływania algorytmów opracowanych przez internetowe giganty z zamiarem zwiększenia zysków z reklam[55].

Kontrowersje wokół reklam politycznych w internecie nasiliły się w USA wraz ze wzrostem aktywności zwolenników zablokowania upowszechniania fałszywych informacji w mediach społecznościowych. W raporcie opublikowanym w połowie 2019 r. przez organizację obywatelską Avaaz podano, że fałszywe wiadomości wymierzone przeciwko amerykańskim politykom były od początku tego roku wyświetlane na Facebooku ponad 150 milionów razy. W raporcie odnotowano też fakt doskonalenia metod ataku internetowego. Fałszywe materiały ze stron, które podają się za legalne, zostały opublikowane 2,3 miliona razy na Facebooku i uzyskały prawie 9 milionów interakcji poprzez komentarze, „polubienia" lub udostępnianie innym stronom na Facebooku. Komentując te dane w kontekście wyborów w 2020 r., Fadi Quran, dyrektor kampanii w Avaaz, w rozmowie z Politico powiedział: „Zmierzamy do katastrofy wielkości Titanica"[56].

Portale i korporacje internetowe – obwiniane o niedostateczną obronę swoich użytkowników przed manipulacjami dokonywanymi za pomocą różnych fikcyjnych uczestników sieci – zaczynają energiczniej eliminować ze swoich stron treści pochodzące z fałszywych kont i usuwać ze swoich witryn fałszywe informacje. W utworzonych przez Facebook centrach ochrony przed manipulacjami wyborczymi pracowało na całym świecie w 2019 r. około 30 tysięcy osób korzystających z narzędzi sztucznej inteligencji. Szczegółowo analizowany jest ruch w sieci i na bieżąco są podejmowane działania ochronne. Blokuje się próby zakładania milionów fałszywych kont, które powstają w fabrykach trolli.

Każde kolejne wybory powszechne oznaczają swoisty stan alarmu dla administratorów globalnych narzędzi internetowych. Główną metodą działania jest blokowanie podejrzanych kont użytkowników sieci. Przykładowo w marcu 2019 r. poinformowano, że Facebook usunął ze swojego serwisu społecz-

54 https://www.politico.eu/article/facebook-political-ads-mark-zuckerberg.

55 https://www.theguardian.com/commentisfree/2020/jan/20/trump-election-facebook.

56 https://www.politico.com/news/2019/11/06/facebook-misinformation-disaster-2020-elections-066539.

nościowego oraz z platformy Instagram ponad 2 tysiące fałszywych profili związanych m.in. z Rosją, Iranem, Macedonią i Kosowem, których aktywność uznano za część zorganizowanych operacji informacyjnych. Według Nathaniela Gleichera[57], szefa do spraw polityki cyberbezpieczeństwa Facebooka, profile te stosowały taktykę tworzenia sieci kont, wzajemnie maskujących prawdziwą tożsamość operatorów i wprowadzających w błąd obserwujących je użytkowników. Gleicher poinformował wówczas także, że z serwisów Facebooka usunięto 513 grup, stron i profili angażujących się w działania o charakterze operacji informacyjnych, które można powiązać z Iranem. Działania te prowadzono w wielu krajach za pomocą fałszywych profili, zaś operatorzy posługujący się fałszywymi adresami starali się stworzyć wrażenie, że mieszkają w danym regionie bądź są przedstawicielami regionalnych mediów. Podszywali się oni niejednokrotnie pod prawdziwe organizacje polityczne i media działające w danym kraju i wykorzystywali usługi Facebooka do publikowania postów na temat bieżących wydarzeń politycznych. W upowszechnianych materiałach powielano poglądy zgodne z linią ideologiczną i polityczną irańskich mediów państwowych w sprawach napięć między Indiami i Pakistanem, konfliktów w Syrii i Jemenie czy stosunków izraelsko-palestyńskich. Strony te obserwowało około 1,4 miliona kont. Przedstawiciel Facebooka poinformował także o usunięciu ponad 1,9 tysięcy stron i grup uznanych za powiązane z Rosją, które były wyzyskiwane do zamieszczania treści dotyczących konfliktu trwającego we wschodniej części Ukrainy i rozwoju wydarzeń na Krymie.

Od pewnego czasu korporacje internetowe otwarcie już przyznają, że za „skoordynowanymi nieautentycznymi zachowaniami" w sieci stoją również niektóre państwa, w tym kraje Bliskiego Wschodu, które coraz częściej wykorzystują media społecznościowe, takie jak Facebook, Twitter czy YouTube, do działań politycznych. Tylko w pierwszej połowie 2019 r. Facebook zidentyfikował „nieautentyczne zachowania" w sieci pochodzące z 13 państw. Firma usunęła wówczas ze swojego serwisu społecznościowego ponad 350 kont i stron obserwowanych w sumie przez blisko półtora miliona użytkowników, które rozpoznano jako narzędzia politycznej propagandy Arabii Saudyjskiej. Poinformowano, że organizatorzy tych propagandowych działań wydali na swoją kampanię ponad 100 tysięcy dolarów[58]. Wciąż przybywa informacji o zamykaniu przez Facebook stron, które uznano za powiązane z rządami. Przykładowo w lutym 2020 r. poinformowano o zamknięciu wielu kont i stron internetowych, w przypadku których tropy prowadzą do rządów Rosji, Iranu, Wietnamu czy Mjanmy; ich zadaniem było wprowadzanie w błąd opinii

[57] Cyt. za materiałem PAP zamieszczonym w serwisie Polsat News 26.03.2019.

[58] https://www.tvn24.pl/facebook-usuwa-konta-serwisu-spolecznosciowego-sprzyjajace-arabii-saudyjskiej,957805,s.html.

publicznej oraz atakowanie innych państw, co odnosi się np. do stron rosyjskich atakujących Ukrainę w związku ze sporem o Krym[59].

Można przypuszczać, że administratorzy platform i komunikatorów internetowych będą musieli przyjąć strategię stałego ograniczania możliwości wykorzystywania udostępnianej przez nich przestrzeni informacyjnej do rozwijania patologicznych, motywowanych politycznie form aktywności. Leży to w ich własnym, dobrze pojętym interesie, w przeciwnym bowiem razie grozi im spadek zaufania użytkowników, co niesie ze sobą ryzyko strat biznesowych.

Walka z dezinformacją w cyberprzestrzeni natrafia na liczne trudności, a co więcej – sama staje się obszarem manipulacji i przedmiotem ostrych sporów politycznych. Praktyka pokazuje, że próby ograniczenia patologii w aktywności politycznej (lub parapolitycznej) w internecie i objęcia tej sfery regulacjami prawnymi są spóźnione i niepełne. Równocześnie trzeba zaznaczyć, że internet w dużym stopniu kojarzy się ludziom z wolnością, dlatego też wprowadzenie reglamentacji do przestrzeni internetowej spotyka się ze społecznym oporem.

Usuwanie dysfunkcjonalnych, szkodliwych społecznie i politycznie treści w serwisach internetowych nie jest łatwe również dlatego, że – jak już sygnalizowałem – działania takie są wykorzystywane do tłumienia wolności słowa, w tym utrudniania krytyki władz, przez państwa, w których utrzymuje się deficyt demokracji. Państwa te tradycyjnie dążą do blokowania niepodlegających kontroli kanałów kontaktów z zagranicą. Dostęp do globalnego internetu jest tam poddany reglamentacji i kontroli, gdyż dostawcy usług internetowych muszą korzystać z państwowego pośrednika. Przykładowo w Białorusi takim pośrednikiem w łączności internetowej z siecią światową jest państwowa firma Beltelekom. W skrajnych przypadkach dostęp do globalnego internetu jest całkowicie blokowany. Przykładowo w Korei Północnej oraz Chinach stworzono wewnętrzne platformy internetowe, izolowane od systemów globalnych i znajdujące się pod pełną kontrolą władz. W styczniu 2019 r. na liście Wielkiego Internetowego Muru znalazła się wyszukiwarka Microsoftu (Bing), która była ostatnią dostępną w Chinach globalną przeglądarką. Wcześniej, już w 2009 r., władze chińskie zablokowały dostęp do usług oferowanych przez serwis Twitter, a w kolejnych latach – do usług Google'a (2010), Instagramu (2014), Skype'a (2017)[60]. W 2015 r. zablokowano dostęp do chińskiej edycji Wikipedii, zaś w 2019 r. – do pozostałych jej wersji językowych.

---

[59] https://www.reuters.com/article/us-russia-facebook/facebook-says-it-dismantles-russian-intelligence-operation-targeting-ukraine-idUSKBN2061NC; https://www.rp.pl/Szalenstwa-tego-swiata/302219992-Kiedy-Facebook-jest-potezny-a-kiedy-umywa-rece.html.

[60] https://cyfrowa.rp.pl/globalne-interesy/30926-chiny-zablokowaly-wyszukiwarke-microsoftu; https://cyfrowa.rp.pl/globalne-interesy/34473-chiny-postawily-internetowy-wielki-mur-ameryka-bezsilna.

W sytuacjach napięć społecznych w wielu krajach wprowadza się ograniczenia w swobodnej komunikacji internetowej. Dla zilustrowania tego zjawiska można sięgnąć po przykłady z 2019 r. Indonezja odcięła wówczas dostęp do internetu we wschodniej Papui, aby zapobiec postom online inspirującym gwałtowne zachowania studentów protestujących po aresztowaniu osób obwinianych o brak szacunku dla flagi państwowej[61]. Turcja zablokowała 136 stron internetowych, w tym stronę z wiadomościami o prawach człowieka[62]. Cyfrowa izolacja wystąpiła okresowo podczas eskalacji napięć wewnętrznych w Iranie. Zachowując aktywność w ramach „wewnętrznego" internetu, zablokowano wówczas komunikację z adresami spoza granic kraju. Wykorzystano w tym celu fakt, że w Iranie komunikacja z globalnym internetem odbywa się kanałami znajdującymi się pod kontrolą państwa. Działania władz irańskich nie były jedynie uwarunkowane sytuacyjnie – dążeniem do zablokowania informacji na temat niepokojów społecznych, stanowiły bowiem fragment przygotowań do systemowego zamknięcia aktywności internetowej w tzw. Narodowej Sieci Informacyjnej[63]. Kolejny przykład to Indie, gdzie w 2019 r., w związku z napięciami na tle regulacji w sprawie obywatelstwa, zablokowano na kilka miesięcy dostęp do internetu w niektórych rejonach kraju, w tym w Kaszmirze. Działania te wywołały dotkliwe skutki ekonomiczne i społeczne, doszło bowiem do wielomilionowych strat korporacji telekomunikacyjnych[64] i nastąpiły zakłócenia w świadczeniu różnorodnych usług publicznych, w tym w obszarze ochrony zdrowia[65]. Sąd Najwyższy Indii uznał zaistniałą sytuację za niedopuszczalną, stwierdzając, że swoboda dostępu do internetu jest prawem podstawowym i może podlegać reglamentacji tylko w zakresie ściśle wyznaczonym w prawie[66]. Blokada internetu, w tym dostępu do stron internetowych mediów opozycyjnych, miała też miejsce w Białorusi w czasie protestów po uznanych za sfałszowane wyborach prezydenckich w sierpniu 2020 r. Działania te spotkały się z ostrą krytyką ze strony USA i 28 innych państw, w tym Polski, które we wspólnej deklaracji podkreśliły, że blokowanie internetu stanowi naruszenie swobody słowa i praw człowieka

---

61 https://www.reuters.com/article/us-indonesia-papua/indonesia-blocks-internet-in-papua-to-help-curb-violent-protests-idUSKCN1VC0EQ.

62 turkey-security-internet/turkishttps://www.reuters.com/article/us-h-court-lifts-block-on-foreign-backed-monitoring-group-website-idUSKCN1UY191.

63 https://www.theguardian.com/world/2019/nov/21/irans-digital-shutdown-other-regimes-will-be-watching-closely.

64 https://www.reuters.com/article/us-india-citizenship-telecoms/indias-internet-shutdowns-costing-mobile-carriers-millions-of-rupees-in-lost-revenue-idUSKBN1YV14P.

65 https://www.theguardian.com/world/2020/jan/05/the-personal-and-economic-cost-of-kashmirs-internet-ban.

66 https://www.reuters.com/article/us-india-kashmir-internet/indias-top-court-says-indefinite-kashmir-internet-shutdown-is-illegal-idUSKBN1Z90FR.

oraz ogranicza prawo do pokojowych zgromadzeń, wolności zrzeszania się i swobodę wypowiedzi, zaś „sfera publiczna online jest integralną częścią tętniącej życiem przestrzeni obywatelskiej offline”[67].

Wiele sygnałów wskazuje, że koncepcja odizolowania internetu krajowego od systemu światowych zasobów i łączy, przynajmniej na wypadek wystąpienia napięć społecznych, jest poważnie rozważana w Rosji. Władze tego państwa postrzegają internet przede wszystkim jako pole wojny informacyjnej. Zagrożenia związane z komunikacją elektroniczną są traktowane z najwyższą uwagą w sytuacji, gdy – według danych agencji badań rynku medialnego Mediascope – w połowie 2019 r. liczba użytkowników internetu w Rosji wynosiła prawie 96 milionów (to jest 78% ludności powyżej 12. roku życia)[68]. W 2019 r. wprowadzono w tym państwie do porządku prawnego ustawę, jak to określono w komunikacie agencji prasowej TASS, „blokującą rozpowszechnianie nieprawdziwych informacji oraz treści znieważających władze w Internecie”. Za rozpowszechnianie takich informacji grożą wysokie kary grzywny (dla obywateli do 100 tysięcy rubli, tj. około 1500 dolarów, a dla osób prawnych – 500 tysięcy rubli, tj. około 7600 dolarów) lub areszt administracyjny. Do blokowania informacji nie jest wymagana decyzja sądu, wystarcza wniosek Prokuratury Generalnej do Roskomnadzoru (federalnej służby do spraw nadzoru w sferze łączności, komunikacji masowej, technologii informacyjnych oraz mediów). Oficjalnie ma to być forma walki z fałszywymi informacjami. Przeciwko tym przepisom protestowali bezskutecznie pisarze, dziennikarze i obrońcy praw człowieka[69]. Regulacje stanowią uzupełnienie przepisów z lat 2012–2013, na mocy których władze zagwarantowały sobie prawo do blokowania bez sankcji sądu stron internetowych zawierających szkodliwe treści, oraz z lat 2014–2018, wprowadzających m.in.: sankcje karne za wykorzystywanie internetu do rozpowszechniania treści ekstremistycznych, obowiązek przechowywania przez okres sześciu miesięcy przez operatorów elektronicznych dokumentacji elektronicznej kontaktów internetowych i udostępniania tej dokumentacji służbom specjalnym bez nakazu sądu, zakaz anonimowości użytkowników komunikatorów internetowych oraz możliwość blokowania bez wyroku sądu stron internetowych organizacji uznanych za niepożądane[70]. W ustawie uchwalonej w kwietniu 2019 r. mówi się o stworzeniu rozwiązań technicznych i organizacyjnych pozwalających na funkcjo-

---

67 https://www.pap.pl/aktualnosci/news%2C719343%2Cusa-29-krajow-potepilo-blokade-internetu-na-bialorusi.html.

68 M. Domańska, *Zakneblować Runet, uciszyć społeczeństwo. Kremlowskie ambicje „suwerenizacji” Internetu*, Ośrodek Studiów Wschodnich, „Komentarze OSW”, nr 313, 4.12.2019, www.osw.waw.pl.

69 Serwis informacyjny wp.pl z 18.03.2019.

70 Zob. M. Domańska, *Zakneblować Runet…*

nowanie Runetu (rosyjskiego segmentu internetu) w warunkach odłączenia od globalnego internetu oraz przejęcie w sytuacjach krytycznych zarządzania internetem przez państwowy urząd – wspomniany wyżej Roskomnadzor. Urząd ten uzyskał prawo do filtrowania informacji w przestrzeni internetowej. Wprowadzono obowiązek inwentaryzacji i certyfikacji punktów wymiany informacji między internetem w Rosji a zasobami internetu globalnego. Od jesieni 2019 r. stworzono możliwość blokowania przez Roskomnadzor – w ramach systemu inspekcji pakietów – niepożądanych stron i serwisów informacyjnych[71].

Jesienią 2019 r. przeprowadzono w Rosji testy sprzętu do izolacji internetu, co wskazuje, że władze tego państwa nie wykluczają sięgania po chińskie wzory blokowania i cenzury komunikacji internetowej[72]. Działania te zbiegły się z wysuniętymi przez władze oskarżeniami, że Facebook i Google ingerowały w trakcie wyborów lokalnych za pomocą reklam politycznych w suwerenne sprawy Rosji i utrudniały przeprowadzenie demokratycznych wyborów w Federacji Rosyjskiej[73]. Rozważane są plany wprowadzenia obowiązku rejestracji przez użytkowników wszystkich urządzeń elektronicznych, które zapewniają dostęp do sieci internetowej[74]. Postanowiono też wprowadzić w Rosji od połowy 2020 r. zakaz sprzedaży urządzeń mobilnych, w tym smartfonów, komputerów i inteligentnych telewizorów, bez rosyjskiego oprogramowania. Zakazem tym objęto także urządzenia wyprodukowane w innych krajach. Przeciwnicy tej regulacji wskazywali, że może ona być wykorzystywana przez władze do instalowania w sprzęcie elektronicznym aplikacji ułatwiających monitorowanie zachowań społeczeństwa[75]. W grudniu 2019 r. zgłoszono projekt zakazu zamieszczania anonimowych i pisanych pod pseudonimami opinii w rosyjskim internecie, co oficjalnie ma ograniczyć rozpowszechnianie niesprawdzonych i fałszywych informacji[76]. Rosyjskie władze nakazują mediom społecznościowym, żeby lokalizowały na terenie Rosji serwery zawierające banki danych o obywatelach tego kraju. W latach 2019–2020 Facebook i Twitter zostały ukarane przez sąd grzywnami po 4 miliony rubli (tj. blisko 63 tysiące dolarów) za nieprzestrzeganie tej zasady[77].

---

71 Serwis informacyjny PAP z 22.04.2019.

72 https://www.reuters.com/article/us-russia-putin-internet/russia-checks-its-internet-can-work-if-cut-off-from-worldwide-web-idUSKBN1YR1W4.

73 https://www.reuters.com/article/us-russia-election-internet/russia-says-facebook-google-distributed-political-ads-on-election-day-idUSKCN1VT0K0.

74 https://tech.wp.pl/rosja-chce-rejestracji-wszystkich-urzadzen-elektronicznych-niepokojace-plany-rzadu-6443101340874369a.

75 https://www.rp.pl/Rosja/191129813-Rosja-zakazuje-sprzedazy-urzadzen-mobilnych-bez-rosyjskiego-oprogramowania.html.

76 https://cyfrowa.rp.pl/globalne-interesy/42158-rosja-anonimy-maja-zniknac-z-internetu?utm_source=rp&utm_medium=teaser_redirect.

77 https://www.reuters.com/article/us-russia-facebook-fine/russian-court-fines-facebook-63000-over-data-law-breach-ria-idUSKBN2071PK.

Liczne fakty dowodzą, że państwa, które blokują swobodne funkcjonowanie globalnej komunikacji, same – zwykle za pomocą domen działających pod fałszywymi tożsamościami – intensywnie wykorzystują narzędzia internetowe do narzucania swojej narracji w ważnych dla nich sprawach. Przykładem może być akcja podjęta w 2019 r. przez Chiny w obliczu napięć w Hongkongu. W sieci pojawiło się wówczas bardzo wiele negatywnych komentarzy i głosów „obywatelskiego" oburzenia z powodu protestów w Hongkongu przeciwko ustawie o ekstradycji osób podejrzanych o przestępstwa do Chin. Wystąpienia internetowe zostały zakwalifikowane przez kierownictwa mediów społecznościowych jako skoordynowane działania propagandowe władz chińskich, co doprowadziło do zamknięcia na YouTubie kilkuset domen i zawieszenia setek tysięcy kont na Twitterze i Facebooku, które uznano za powiązane z chińskim rządem[78].

Safa Shahwan, analityczka Atlantic Council, rozpatrując przypadek Kazachstanu, zwraca uwagę, że niedemokratyczne rządy mogą używać narzędzi cybernetycznych do operacji służących zachowaniu władzy[79]. Przypomina, że latem 2019 r. Google, Apple i Mozilla postanowiły blokować w swoich przeglądarkach certyfikat głównego urzędu certyfikacji Kazachstanu z powodu podejrzenia, że urząd ten przechwytuje komunikację między użytkownikami a stronami internetowymi i prowadzi nadzór nad użytkownikami internetu, którego wyniki są wykorzystywane do walki z oponentami władzy.

Państwa podejmujące próby reglamentacji komunikacji internetowej tradycyjnie powołują się na wymagania wynikające z potrzeby zagwarantowania bezpieczeństwa. Tak też było w Pakistanie, gdzie administratorzy mediów społecznościowych zostali na początku 2020 r. zobowiązani, pod rygorem zablokowania ich sygnału w komunikacji online, do udzielania pomocy organom ścigania w dostępie do danych i w usuwaniu treści internetowych uznanych za niezgodne z prawem[80].

Ograniczenia w komunikacji internetowej są nakładane nie tylko przez państwa niedemokratyczne. W niektórych przypadkach trudno jest odróżnić działania zmierzające do eliminowania patologii w sferze informacji i komunikacji internetowej od cenzury internetu przez organy władzy państwowej. Przykładem może tu być decyzja władz Australii i Nowej Zelandii o blokowaniu domen internetowych hostujących ekstremistyczne treści podczas zdarzeń kryzysowych i ataków terrorystycznych, podjęta po zamachach na

78 https://www.cbsnews.com/news/youtube-shuts-down-more-than-200-channels-spreading-hong-kong-protests-disinformation.

79 https://www.atlanticcouncil.org/blogs/new-atlanticist/how-governments-can-use-cyber-tools-irresponsibly-to-preserve-power.

80 https://www.reuters.com/article/us-pakistan-socialmedia/pakistans-government-approves-new-social-media-rules-opponents-cry-foul-idUSKBN2071YL.

dwa meczety w Christchurch (w Nowej Zelandii), w których zginęło ponad 50 wiernych. Trudno też o jednoznaczną ocenę wprowadzonej w 2019 r. w Singapurze ustawowej regulacji pozwalającej blokować w internecie „fałszywe wiadomości"; politycy opozycji uważali, że jest to narzędzie dające rządowi zbyt dużą władzę, zwłaszcza w obliczu zbliżających się wyborów. Organizacja non profit Reporterzy bez Granic, działająca na rzecz wolności prasy, nazwała to prawo „totalitarnym" i stwierdziła, że ma ono na celu wyeliminowanie debaty publicznej. Rząd utrzymywał, że jedynym celem ustawy jest ograniczenie ryzyka manipulacji internetowych, które są szczególnie groźne w kraju o mocno zróżnicowanej populacji, stanowiącej prawdziwą mieszankę etniczną i religijną[81]. W ramach tej regulacji internetowe platformy medialne zostały zobowiązane, pod karą grzywny, do usuwania lub korygowania treści, które rząd uważa za fałszywe, zaś osoby uznane za złośliwie rozpowszechniające fałszywe, szkodliwe dla interesu publicznego informacje w internecie podlegają karze pozbawienia wolności do lat dziesięciu[82]. Ustawa ta jest stosowana w praktyce. Na jej podstawie rząd Singapuru nakazał opozycyjnej Partii Demokratycznej opublikowanie poprawek do dwóch postów w mediach społecznościowych oraz artykułu na swojej stronie internetowej[83]. Wezwanie okazało się skuteczne i partia skorygowała swoje posty[84]. Równocześnie, w wyraźnym związku z nowymi regulacjami, Google przestał zamieszczać reklamy polityczne dotyczące Singapuru w okresie przed wyborami w tym państwie-mieście[85].

Jest rzeczą oczywistą, że odpowiedź na pytanie, czy i co należy cenzurować, będzie nasuwała wątpliwości i wywoływała spory. Potwierdzają to zarzuty w stosunku do kierownictw mediów społecznościowych w związku z podejmowanymi przez nie działaniami polegającymi na usuwaniu domen i treści uznanych za fałszywe i szkodliwe. Z pewnością dziedzina ta wymaga wprowadzenia ogólnie obowiązujących standardów.

---

81 https://www.reuters.com/article/us-singapore-fakenews/singapore-fake-news-law-ensnares-government-critics-idUSKBN1YK0KH.

82 https://www.reuters.com/article/us-singapore-fakenews/singapore-fake-news-law-set-to-come-into-force-on-wednesday-idUSKBN1WG3ND.

83 https://www.reuters.com/article/us-singapore-fakenews/singapore-invokes-fake-news-law-over-opposition-party-posts-idUSKBN1YI0DF.

84 https://www.reuters.com/article/us-singapore-fakenews/singapore-opposition-party-corrects-posts-under-fake-news-law-idUSKBN1YK09E.

85 https://www.reuters.com/article/us-google-singapore-election/google-halts-political-ads-in-singapore-as-election-looms-documents-idUSKBN1Y80JM.

7.5. Związki między polityką a technologiami cyfrowymi w Polsce

Włączanie narzędzi internetowych do gry politycznej w Polsce • Ekspansja mowy nienawiści • Sygnały o udziale trolli w utarczkach i kampaniach politycznych

Również w Polsce obecnie używa się narzędzi internetowych do gry politycznej. Jak wszędzie na świecie, także u nas występują rozmaite patologie związane z tą praktyką. I tak jak w wielu innych krajach, w Polsce kwestia dezinformacji i manipulacji w komunikacji cyfrowej pojawiła się w debacie politycznej (a także w świadomości społecznej) głównie za sprawą kontrowersyjnej aktywności użytkowników mediów społecznościowych oraz po ujawnieniu faktu, że politycy posługują się mową nienawiści (*hate speech*), czyli tzw. hejtem, lub raczej wyręczają (wysługują) się hejterami[86].

W Polsce mamy więc poważny problem: rozprzestrzenianie się mowy nienawiści w sferze publicznej. Jeśli, w ślad za Radą Europy[87], przez mowę nienawiści rozumieć każdą formę wypowiedzi, która „rozpowszechnia, podżega, propaguje lub usprawiedliwia nienawiść rasową, ksenofobię, antysemityzm lub inne formy nienawiści oparte na nietolerancji, włączając w to nietolerancję wyrażaną w formie agresywnego nacjonalizmu lub etnocentryzmu, dyskryminacji lub wrogości wobec mniejszości, migrantów lub osób wywodzących się ze społeczności imigrantów", to mnóstwo jej przykładów można spotkać w obrębie internetu w Polsce. Jak głosi komunikat z badań CBOS przeprowadzonych w 2019 r., wśród ankietowanych, którzy zetknęli się z mową nienawiści, aż 65% osób wskazało, że najbardziej kojarzy im się ona z internetem, a 55% – że najczęściej posługiwali się nią użytkownicy internetu[88]. Zjawisko jest więc rozpoznane, spotyka się też z silną krytyczną reakcją wielu ludzi i środowisk. Głosy nawołujące do powstrzymania fali nienawiści i do zwalczania wszelkich form przemocy, w tym agresji językowej w mediach społecznościowych, wzmogły się w 2019 r. po zabójstwie prezydenta Gdańska Pawła Adamowicza. Składane wówczas przez strony konfliktu politycznego deklaracje wyrzeczenia się mowy nienawiści szybko jednak okazały się nieaktualne.

---

[86] *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, red. M. Wrzosek, https://akademia.nask.pl/badania/Raport_CP_Dezinformacja_ONLINE.pdf; *Bezpieczne wybory. Badanie opinii o (dez)informacji w sieci*, red. R. Lange, https://www.nask.pl/pl/raporty/raporty/2592,Bezpieczne-wybory-raport-na-temat-dezinformacji-w-internecie.html?search=8771219.

[87] Rekomendacja R 97(20) Komitetu Ministrów Rady Europy, https://rm.coe.int/opening-session-2-parmar-the-legal-framework-for-addressing-hate-speec/16808ee4bf.

[88] Zob. *Mowa nienawiści*, CBOS, komunikat z badań nr 139 z 2019 r. (badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 4–11 lipca 2019 r. na liczącej 1077 osób reprezentatywnej próbie losowej dorosłych mieszkańców Polski).

Od czasu do czasu pojawiają się dowody na to, że politycy w Polsce (lub też osoby z ich otoczenia) uciekają się do manipulacji w internecie. W tych sprawach można się opierać przede wszystkim na informacjach pośrednich, najczęściej prasowych, które dotyczą sytuacji ujawnionych publicznie. To skłania do przypuszczenia, że nagłośnione afery to jedynie wierzchołek góry lodowej, jednak nie można już mieć wątpliwości co do tego, że patologie w postaci internetowych manipulacji występują i u nas. W połowie 2019 r. głośny się stał przypadek „wspomagania" przez osoby z kierownictwa i spośród pracowników Ministerstwa Sprawiedliwości internetowych ataków na sędziów, ujmowany w kontekście trwającego w Polsce sporu o kształt wymiaru sprawiedliwości. Skruszona hejterka ujawniła, że za wiedzą sędziego i zarazem wiceministra Łukasza Piebiaka, współdziałając z kilkoma innymi sędziami związanymi z Ministerstwem Sprawiedliwości, prowadziła za pomocą Twittera i komunikatora WhatsApp kampanię wymierzoną w sędziów – w tym w I Prezes Sądu Najwyższego Małgorzatę Gersdorf – krytykujących zmiany w sądownictwie dokonywane przez ministra Zbigniewa Ziobrę[89]. Działania te miały być wspomagane materiałami pozyskanymi z ministerstwa. Z kolei w środowiskach sprzyjających rządzącej prawicy pojawiły się oskarżenia o akcję trollowania prowadzoną przez ludzi skupionych wokół Urzędu Miasta Inowrocławia w trakcie kampanii wyborczej, której celem miało być osłabienie pozycji konkurentów Ryszarda Brejzy w wyborach samorządowych w 2019 r.[90]. Wykorzystywanie infrastruktury internetowej w walce politycznej sygnalizowała też dziennikarka tygodnika „Newsweek", która w 2019 r. w ramach dziennikarskiego śledztwa zatrudniła się w pobierającej dotacje państwowe firmie, będącej – jak się okazało – farmą trolli, zaangażowaną w atakowanie w mediach społecznościowych środowisk opozycyjnych wobec polityki rządu[91].

Symptomatyczny był przebieg sondażu elektronicznego zorganizowanego na Facebooku przez dziennik „Rzeczpospolita" w sprawie opinii na temat odwołania Zbigniewa Ziobro ze stanowiska ministra sprawiedliwości po aferze z trollami inspirowanymi przez ludzi z jego ministerstwa. Przez pierwsze dwie godziny głosy rozkładały się w tym sondażu w proporcji: 80% za dymisją ministra, 20% przeciw. Później proporcje głosów gwałtownie zaczęły się odwracać. Lawinowo przybywało zwolenników Ziobry. Na każdy głos oddawany za odwołaniem ministra, przypadało 50 głosów przeciw jego odwołaniu.

---

89 https://wiadomosci.onet.pl/tylko-w-onecie/sledztwo-onetu-farma-trolli-w-ministerstwie-sprawiedliwosci-czyli-za-czynienie-dobra/j6hwp7f; https://wiadomosci.onet.pl/kraj/konsekwencje-afery-w-ministerstwie-sprawiedliwosci-sedzia-cichocki-w-trybie/e3yshc4.

90 https://tvn24.pl/polska/inowroclaw-afera-fakturowa-prokuratura-bada-zeznania-osob-ktore-obciazaja-ryszarda-brejze-i-krzysztofa-brejze-ra965453-2282886.

91 https://www.rp.pl/Spoleczenstwo/191029469-Farma-trolli-za-dotacje-od-panstwa-Sledztwo-Newsweeka.html.

Redakcja sprawdziła, że były to głosy oddawane z kont pozbawionych zdjęcia profilowego, posiadających niewielką liczbę znajomych, które na co dzień nie obserwują profilu „Rzeczpospolitej" na Facebooku. Obserwatorzy tego głosowania nie mieli wątpliwości, że do akcji musiał wkroczyć zespół trolli wspomagający ministra[92].

Analiza stron internetowych partii politycznych oraz komentarzy pod informacjami zamieszczanymi na stronach portali informacyjnych wskazuje, że najbardziej aktywne w komunikacji za pomocą mediów społecznościowych było w Polsce w latach 2019–2020 środowisko prawicy. Na początku 2020 r., w wyniku awarii systemu Facebooka, można było przez kilka godzin pozyskiwać, zwykle dostępne tylko administratorom, informacje o tożsamości osób prowadzących na tym portalu profile znanych polityków i instytucji publicznych, w tym m.in. Mateusza Morawieckiego oraz Ministerstwa Sprawiedliwości, które mają po kilkadziesiąt tysięcy fanów. Materiał ten został poddany przez dziennikarzy analizie, która pokazała siatkę politycznych powiązań między osobami odpowiedzialnymi za prowadzenie stron na platformie. Wśród osób zarządzających kontami był m.in. dyrektor do spraw marketingu w PKO BP, pracownik biura posła PiS, radny z klubu PiS[93].

Na aktywność partii politycznych w mediach społecznościowych przy okazji wyborów w Polsce w 2019 r. zwróciła uwagę w swoim raporcie Jolanta Kamińska, która odwołując się do badań Fundacji Panoptykon, Fundacji ePaństwo oraz Sotrenderu, poinformowała, że w kampanii wyborczej do Parlamentu Europejskiego tylko na reklamy polityczne na Facebooku wydano w Polsce niemal 1,7 miliona złotych[94]. Najwięcej z tej sumy (ponad 0,5 miliona złotych) wydał komitet wyborczy Koalicji Europejskiej. Prawo i Sprawiedliwość wydało niecałe 300 tysięcy złotych, Konfederacja – nieco ponad 250 tysięcy, zaś Wiosna – ponad 213 tysięcy. Jak wynika z opublikowanego materiału, partie polityczne prowadziły internetowe kampanie wyborcze precyzyjnie ukierunkowane na różne grupy wiekowe i środowiskowe.

---

92 https://www.rp.pl/Nowe-technologie/190829669-Nagly-wzrost-poparcia-dla-Ziobry-Historia-sondy-na-Facebooku.html.

93 https://konkret24.tvn24.pl/tech,116/awaria-pokazala-kto-prowadzi-profile-politykow-na-facebooku,999605.html.

94 https://fakty.interia.pl/raporty/raport-wybory-parlamentarne-2019/aktualnosci/news-walka-o-wyborcow-na-facebooku-kto-nas-amierza,nId,3208218#utm_source=paste&utm_medium=paste&utm_campaign=chrome.

Rozdział ósmy

Ekspansja technologii informacyjnych, cyfryzacji i automatyzacji jako zasadnicze wyzwanie regulacyjne dla rządzenia

8.1. Potrzeba ukierunkowania wysiłku naukowego i technologicznego na realizację wartości podstawowych i interesów ludzi

Wyzwania regulacyjne związane z technologiami informacyjnymi i cyfryzacją • Potrzeba określenia standardów rozwoju narzędzi sztucznej inteligencji

Sprawy cyberprzestrzeni, robotyki i automatyzacji stają się w rządzeniu zasadniczym wyzwaniem regulacyjnym, potrzebna jest więc przemyślana, całościowa i społecznie zrozumiała polityka normatywna w tym zakresie. Jedne z najważniejszych problemów decyzyjnych, przed którymi stoi współczesny świat, wynikają z pokonywania kolejnych barier ludzkich możliwości w tworzeniu cyberprzestrzeni i sztucznej inteligencji. Ta sytuacja stawia przed rządzeniem – na wszystkich jego poziomach i we wszystkich jego dziedzinach – nowe strategiczne zadania, które muszą być wykonywane pod silną presją czasu. Nadal bowiem słuszne jest spostrzeżenie, że „potęga technologii rośnie szybciej niż mądrość, z jaką nią zarządzamy”[1].

W związku z rozwojem cywilizacji cyfrowej, w rządzeniu pojawia się wiele szczegółowych problemów wymagających analizy, uzgodnień oraz przemyślanych i zrozumiałych regulacji. Postęp technologii niesie też za sobą antynomie: między wolnością a bezpieczeństwem, ryzykiem a odpowiedzialnością, dowolnością w eksperymentowaniu a standardami etycznymi, prawami własności a równością i sprawiedliwością.

Z dużym opóźnieniem przebija się do szerszej świadomości fakt, że nowe możliwości, jakie oferują technologie cyfrowe w zakresie pozyskiwania,

[1] M. Tegmark, *Życie 3.0…*, s. 407.

przechowywania i wykorzystywania informacji, mają podstawowe znaczenie z punktu widzenia praw człowieka i obywatela. Mając to na względzie, należy przystąpić do wyznaczania aktualnych ram, zasad i standardów rozwoju narzędzi sztucznej inteligencji, bowiem prawo dotychczas nie nadążało za szybko zachodzącymi zmianami w sferze komunikacji elektronicznej i sztucznej inteligencji[2]. Obowiązujące obecnie regulacje prawne, które w jakiś sposób odnoszą się do tej sfery, można uznać za anachroniczne, gdyż w większości pochodzą z epoki przedcyfrowej.

8.2. Problemy etyczne i prawne dotyczące technologii cyfrowych

Potrzeba regulacji statusu prawnego działań podjętych samodzielnie przez urządzenia elektroniczne • Konieczność optymalizowania współdziałania ludzi z robotami i maszynami cyfrowymi

W perspektywie najbliższych lat, wraz z rozwojem inteligentnych technologii, rządzący będą musieli rozstrzygać wiele problemów o charakterze etycznym, wiążących się z operowaniem danymi wrażliwymi oraz z prowadzonymi badaniami naukowymi, wdrażanymi procedurami monitorowania aktywności ludzi, a także ze zwiększającymi się możliwościami wykorzystania narzędzi automatycznych na polu walki.

Wraz z upływem czasu i tworzeniem coraz doskonalszych technologii cyfrowych zwiększy się znaczenie uregulowania statusu prawnego działań podjętych samodzielnie przez urządzenia elektroniczne na podstawie delegacji udzielonej przez człowieka. Pojawi się problem odpowiedzialności za działanie autonomicznych urządzeń elektronicznych oraz – w dalszej kolejności – problem kontroli rekursywnego samodoskonalenia i klonowania się zdolności poszczególnych programów i urządzeń bez udziału człowieka, a także bez podporządkowania tego procesu interesom społecznym.

Ważnym – i długofalowym – zadaniem jest optymalizowanie współdziałania ludzi z robotami i maszynami cyfrowymi. Zadanie to muszą podejmować wspólnie reprezentanci różnych profesji, specjalności i środowisk: badacze, projektanci i wykonawcy nowych technologii komunikacyjnych i cyfrowych; politycy i decydenci wyznaczający standardy oraz kierunki działania instytucjonalnych podmiotów politycznych, gospodarczych i finansowych; administratorzy funkcjonujących już urządzeń i rozwiązań technologicznych; podmioty

[2] Na temat stanu regulacji prawnych dotyczących sztucznej inteligencji zob. M. Świerczyński, L. Lai (red.), *Prawo sztucznej inteligencji*.

uczestniczące w organizowaniu i prowadzeniu edukacji oraz w kształtowaniu opinii publicznej. Współdziałanie tak różnych podmiotów nie jest łatwe, wymaga bowiem odejścia od nastawienia na rywalizację i na partykularne interesy.

Niezbędnym warunkiem ukierunkowania wysiłku naukowego i technologicznego w dziedzinie narzędzi komunikacji społecznej oraz sztucznej inteligencji na podnoszenie poziomu cywilizacyjnego i usprawnianie życia ludzi, przy poszanowaniu godności, praw i wolności oraz różnorodności kulturowej, jest powszechne przyjęcie zasady odpowiedzialności. Ta zasada musi znaleźć wyraz w tworzonych rozwiązaniach normatywnych i organizacyjnych. Zaniechania i błędy w tej dziedzinie mogą prowadzić do powstania różnorodnych zagrożeń o globalnym, również egzystencjalnym, charakterze. Ryzyko wymknięcia się rozwoju sztucznej inteligencji spod kontroli jest zbyt duże, aby można było poniechać dotyczących tej dziedziny regulacji prawnych, ufając w zdrowy rozsądek badaczy, technologów, działaczy politycznych oraz ludzi finansów i biznesu.

8.3. Próby wspólnego wypracowania zasad rozwoju sztucznej inteligencji

Próby porządkowania przestrzeni aksjologicznej i normatywnej w związku z rozwojem nowych technologii

W istniejącej sytuacji trzeba więc pozytywnie ocenić próby porządkowania przestrzeni aksjologicznej i normatywnej w związku z rozwojem nowych technologii o podstawowym znaczeniu dla ludzi. Rośnie świadomość faktu, że postępowi technologicznemu musi towarzyszyć wypracowywanie standardów w zakresie badań, wdrożeń i eksploatacji rozwiązań nowych technologii. O zrozumieniu tej konieczności świadczą działania podejmowane w środowiskach naukowych, organizacjach międzynarodowych, poszczególnych państwach oraz w ramach struktur administrujących konkretnymi programami i urządzeniami.

Wśród inicjatyw podejmowanych w środowiskach naukowych, na uwagę zasługuje próba wypracowania uzgodnionych zasad rozwoju sztucznej inteligencji na konferencji w Asilomar (USA) w styczniu 2017 r. W powstałym dokumencie, wyrażającym pragnienie, by narzędzia sztucznej inteligencji były włączane do działań służących ludziom, zawarto 23 związane z tym zasady postępowania. Jako cel badań nad sztuczną inteligencją wskazano tworzenie „dobroczynnej sztucznej inteligencji". Podkreślono, że należy finansować badania służące zapewnieniu „użytecznego wykorzystania" sztucznej inteligencji, w tym poprzez zagwarantowanie dużej odporności przygotowywanych rozwiązań na awarie i niedopuszczalne ingerencje z zewnątrz, przygotowanie

infrastruktury prawnej sztucznej inteligencji (m.in. na potrzeby zarządzania ryzykiem z nią związanym), nadanie sztucznej inteligencji odpowiedniego statusu prawnego i etycznego. Za rzecz niezbędną uznano konstruktywną wymianę poglądów między badaczami i politykami, rozwijanie kultury współpracy, zaufania i przejrzystości oraz uzgadnianie standardów bezpieczeństwa.

Zawarte w omawianym dokumencie szczegółowe zalecenia w sprawie podejmowanych działań w dziedzinie sztucznej inteligencji i ich wyników dotyczyły m.in.: rozliczalności i przejrzystości prawnej; odpowiedzialności za moralne implikacje użycia systemów sztucznej inteligencji; zgodności z wartościami ludzkimi oraz godnością ludzką, prawami i wolnościami, a także różnorodnością kulturalną; poszanowania prywatności człowieka; ukierunkowania na wspólne korzyści; unikania wyścigu zbrojeń w zakresie śmiercionośnej broni autonomicznej. Rozpatrując omawiane zagadnienia w perspektywie długoterminowej, zalecono, by „unikać mocnych założeń dotyczących górnych granic przyszłych możliwości sztucznej inteligencji", uwzględniać zagrożenie katastrofą lub zagrożenie życia ludzi oraz kontrolować i zabezpieczać procesy rekursywnego samodoskonalenia tworów sztucznej inteligencji. Końcowym akordem dokumentu było stwierdzenie, że „superinteligencja powinna być rozwijana wyłącznie w służbie powszechnie podzielanych ideałów etycznych i z korzyścią dla całej ludzkości, a nie dla jednego państwa czy organizacji"[3].

8.4. Działania na rzecz uregulowania zasad i standardów rozwoju inteligentnych technologii

Zagadnienia inteligentnych technologii w regulacjach ONZ, Unii Europejskiej, OECD i ISO

Problemy związane z uregulowaniem zasad i standardów rozwoju inteligentnych technologii są już dostrzegane i podejmowane w instytucjach politycznych na szczeblu ogólnoświatowym, regionalnym i krajowym. Widać zmiany w podejściu do sztucznej inteligencji, polegające na tym, że w coraz większym stopniu uwzględnia się kwestie zagrożeń stwarzanych przez nowe technologie.

Wśród inicjatyw na rzecz kształtowania ładu cywilizacji cyfrowej, na poziomie ogólnoświatowym na uwagę zasługują przede wszystkim te, które są podejmowane w Organizacji Narodów Zjednoczonych. Przykładowo, w latach 2018–2019 pod auspicjami Sekretarza Generalnego ONZ pracował specjalny zespół, w którym znalazło się 20 niezależnych ekspertów pocho-

[3] M. Tegmark, *Życie 3.0...*, s. 422–425.

dzących z różnych kontynentów i państw, posiadających różne kwalifikacje zawodowe i akademickie w dziedzinach związanych z technologią i polityką. Ze względu na to, że problemy stanowiące przedmiot prac panelu miały dotyczyć w największym stopniu ludzi młodych, do udziału w pracach zespołu zaproszono też kilka osób poniżej 35. roku życia. Po dziewięciu miesiącach, w czerwcu 2019 r. ogłoszono raport końcowy pt. *Era cyfrowej współzależności* (*The Age of Digital Interdependence*)[4]. W tym dokumencie, przygotowanym w konsultacji z rządami, sektorem prywatnym, organizacjami społeczeństwa obywatelskiego, organizacjami międzynarodowymi, ze środowiskiem akademickim i społecznościami technicznymi na całym świecie, przedstawiono obraz technologii cyfrowej i wpływ tej technologii na politykę. Przy okazji prac zespołu, Sekretarz Generalny ONZ António Guterres podkreślił znaczenie pytań o bezpieczeństwo, sprawiedliwość i prawa człowieka w erze cyfrowej, uznał środki i poziomy współpracy międzynarodowej w tych kwestiach za niewystarczające w stosunku do wyzwań i wyraził przekonanie, że potrzebna jest ściślejsza współpraca, aby sprostać tym wyzwaniom i zmniejszyć pojawiające się zagrożenia.

Raport zawiera trzy podstawowe części, w których omówiono kolejno: zagadnienia związane z ograniczaniem wykluczenia cyfrowego – ukazanego jako zjawisko zagrażające wykorzystaniu technologii cyfrowej do stymulowania zrównoważonego rozwoju; zagadnienia związane z prawami człowieka i bezpieczeństwem w dziedzinie cyfrowej; problemy globalnej współpracy cyfrowej na tle analizy dotychczasowych braków w tej dziedzinie.

Na końcu dokumentu umieszczono pięć zasadniczych zaleceń w sprawach kształtowania przyszłości technologii cyfrowej u zarania nowej ery cyfrowej[5]. Pierwsza rekomendacja odnosiła się do budowy do 2030 r. cyfrowej gospodarki i społeczeństwa cyfrowego w sposób gwarantujący każdej dorosłej osobie niedrogi dostęp do sieci cyfrowych oraz cyfrowych usług finansowych i zdrowotnych. W ramach tego zalecenia wskazano na potrzebę: tworzenia sojuszy na rzecz udostępniania „cyfrowych dóbr publicznych"; przyjęcia polityki wspierającej integrację cyfrową z równoprawnym udziałem kobiet i grup marginalizowanych; opracowania i stosowania jasnych wskaźników pozwalających mierzyć poziom włączenia cyfrowego. Druga rekomendacja odnosiła się do rozwijania zdolności ludzkich i instytucjonalnych. W jej ramach zalecono ustanowienie regionalnych i globalnych „cyfrowych centrów pomocy" dla rządów, organizacji społeczeństwa obywatelskiego i sektora prywatnego. Trzecia rekomendacja odnosiła się do ochrony praw człowieka. Autorzy raportu sformułowali w tym zakresie następujące postulaty: Sekretarz Generalny ONZ

[4] Tekst raportu zob. https://digitalcooperation.org/report/.

[5] https://digitalcooperation.org/panel-launches-report-recommendations/.

powinien przeprowadzić globalny przegląd stosowania norm z zakresu praw człowieka w świecie technologii cyfrowych; korporacje mediów społecznościowych powinny współpracować z rządami, międzynarodowymi i lokalnymi organizacjami społeczeństwa obywatelskiego oraz ekspertami w dziedzinie praw człowieka; projekty autonomicznych inteligentnych systemów muszą jasno określać odpowiedzialność za użycie tych systemów. Kolejna, czwarta rekomendacja zawarta w omawianym dokumencie zalecała promowanie w zakresie rozwiązań cyfrowych zaufania, bezpieczeństwa i stabilności oraz wypracowanie w tych sprawach wspólnych standardów. Podstawowe znaczenie miała ostatnia, piąta rekomendacja, akcentująca potrzebę wspierania globalnej współpracy cyfrowej i wskazująca, że Sekretarz Generalny ONZ powinien przyczynić się do opracowania zaktualizowanych mechanizmów globalnej współpracy cyfrowej i wpisać te kwestie do agendy – przypadającej w 2020 r. – 75. rocznicy powstania ONZ. Oceniając swoje wnioski jako pilne, autorzy raportu podkreślili równocześnie, że w omawianych w raporcie sprawach społeczność międzynarodowa nie musi zaczynać od zera i może się opierać na ustanowionych mechanizmach współpracy cyfrowej, w tym forach i sieciach rządów, przemysłu, organów technicznych i społeczeństwa obywatelskiego, a także na istniejących przepisach i „miękkim prawie".

Wyraźne przyspieszenie działań programowych i regulacyjnych w związku z rozwojem nowych technologii komunikacyjnych oraz doskonaleniem narzędzi sztucznej inteligencji nastąpiło już w pierwszych latach drugiej dekady XXI wieku w Unii Europejskiej. Działania te odnoszą się w UE przede wszystkim do takich zagadnień, jak: kierunki rozwoju, dopuszczalne granice i standardy nowych technologii, zagwarantowanie bezpieczeństwa i ochrona standardów etycznych prowadzonych badań i wdrażanych projektów, w tym transparentność badań, ochrona danych, poszanowanie godności człowieka oraz odpowiedzialność za uzyskiwane wyniki. Strategia w tych sprawach została przyjęta w kwietniu 2018 r.

W marcu 2019 r., na podstawie propozycji ekspertów, w swoim wstępnym stanowisku Komisja Europejska przedstawiła siedem rekomendacji wiążących się z pracami nad sztuczną inteligencją (SI)[6]. Po pierwsze – systemy SI powinny się przyczynić do kształtowania sprawiedliwych społeczeństw, wspierając ludzkie interesy i fundamentalne prawa, a nie do zmniejszenia i ograniczania ludzkiej autonomii. Po drugie – należy tworzyć godne zaufania algorytmy, dzięki którym systemy te będą bezpieczne, wiarygodne i wewnętrznie spój-

[6] http://europa.eu/rapid/press-release_IP-19-1893_pl.htm. Zob. też Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – *Budowanie zaufania do sztucznej inteligencji człowieka* (COM(2019) 168), https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.

ne w całym cyklu swojego funkcjonowania. Po trzecie – obywatele powinni mieć pełną kontrolę nad swoimi danymi, a dane ich dotyczące nie mogą być wykorzystywane do ich dyskryminowania czy krzywdzenia. Po czwarte – trzeba opracować rozwiązania, które zagwarantują, że wszystkie systemy SI będzie można identyfikować. Po piąte – należy dostosować systemy SI do ludzkich zdolności, umiejętności i wymagań oraz praktycznych potrzeb. Po szóste – systemy SI powinny być przygotowywane pod kątem wzmacniania pozytywnych zmian społecznych, odpowiedzialności ekologicznej i szans na przetrwanie i rozwój. Po siódme – trzeba zagwarantować w ramach prac nad SI zastosowanie rozwiązań i mechanizmów pozwalających wziąć odpowiedzialność za wszystkie tworzone systemy. Zapowiedziano, że w dalszych pracach Unia Europejska będzie dążyć do budowania międzynarodowego konsensu w sprawie SI ukierunkowanej na człowieka i w 2020 r. dokona oceny wyników programu pilotażowego.

W ścisłym związku z pracami w Unii Europejskiej zmierzającymi do uregulowania standardów rozwoju sztucznej inteligencji pozostają działania ukierunkowane na tworzenie efektywnych mechanizmów cyberbezpieczeństwa[7]. W 2019 r. wypracowano nowe zasady certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych. To pierwsze rozwiązania normatywne w Unii Europejskiej ujmujące całościowo i jednolicie sprawy certyfikacji cyberbezpieczeństwa rynku cyfrowego. Zgodnie z przyjętymi rozwiązaniami, sam proces certyfikacji ma przebiegać na poziomie krajowym. Równocześnie wzmocniono zaplecze instytucjonalne mające w praktyce czuwać nad przestrzeganiem przyjętych zasad[8]. Działającą od 2004 r. Europejską Agencję Bezpieczeństwa Sieci i Informacji przekształcono w Agencję UE ds. Cyberbezpieczeństwa i nadano jej stały mandat. Agencja odgrywa kluczową rolę w zapewnieniu wysokiego poziomu cyberbezpieczeństwa w UE, a do jej zadań należy m.in.: wspieranie państw członkowskich oraz instytucji, organów i jednostek organizacyjnych UE we wdrażaniu europejskiej polityki cyberbezpieczeństwa, aktywność w sprawach budowy zdolności, gotowości i bezpieczeństwa sieci i systemów informacyjnych UE, pomoc w wypracowywaniu zdolności państw członkowskich UE do reagowania na incydenty i zapobiegania przestępstwom w cyberprzestrzeni, promowanie certyfikacji produktów, usług i procesów ICT, w tym sieci i rynku cyfrowego, oraz zwięk-

[7] I. Oleksiewicz, *Zarys polityki cyberbezpieczeństwa Unii Europejskiej. Casus Polski i RFN*, Warszawa 2019.

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. L 151 z 7.06.2019. Zob. też J. Balcewicz, R. Babraj, *Analiza. Akt o cyberbezpieczeństwie – nowy mandat ENISA i certyfikacja cyberbezpieczeństwa*, maj 2019, www.cyberpolicy.nask.pl.

szanie społecznej świadomości i kompetencji cyfrowych poprzez działania edukacyjne.

Powszechnie oczekuje się, że sposób podejścia do sztucznej inteligencji, w ramach którego dostrzega się nie tylko szanse, lecz także zagrożenia, jakie ona niesie, przyjmie się i będzie rozwijany podczas kadencji organów Unii Europejskiej powołanych po wyborach do europarlamentu w 2019 r. Wybrana w 2019 r. na przewodniczącą Komisji Europejskiej Ursula von der Leyen wpisała do programu swoich działań opracowanie regulacji dotyczących skoordynowanego europejskiego podejścia do ludzkich i etycznych implikacji sztucznej inteligencji. Należy więc przewidywać, że w Unii Europejskiej zmieni się rozłożenie akcentów programowych w odniesieniu do świata nowych technologii; w trakcie zakończonej w 2019 r. kadencji Komisji Europejskiej nacisk był położony przede wszystkim na zagwarantowanie prywatności w sieci, cyberbezpieczeństwo, prawa autorskie i telekomunikację[9].

W swoim przemówieniu wygłoszonym 27 listopada 2019 r. na sesji plenarnej Parlamentu Europejskiego von der Leyen, przy okazji prezentacji kolegium komisarzy, z całą stanowczością stwierdziła, że cyfryzacja stanie się zasadniczym priorytetem w działaniu Komisji Europejskiej. Zaakcentowała fakt, iż cyfryzacja umożliwia rzeczy, które były nie do pomyślenia nawet w życiu poprzedniego pokolenia, oraz wyraziła opinię, że integracja bez digitalizacji nie ma przyszłości, zaś cyfryzacja zmieni społeczeństwo, gospodarkę i administrację. Przewodnicząca Komisji Europejskiej podkreśliła też, że w sprawach cyfryzacji trzeba się zająć istniejącymi niebezpieczeństwami i zapewnić równowagę tam, gdzie rynek sam tego nie może dokonać. W tym kontekście wskazała sześć zadań szczegółowych. Pierwszy z nich to uzyskanie postępu w Europie w zakresie własnych technologii kwantowych, sztucznej inteligencji i kluczowych technologii chipowych – poprzez integrację zasobów finansowych i możliwości badawczych. Drugi to promowanie i wykorzystanie zasobów naukowych i przemysłowych. Trzeci – stworzenie przyszłościowej infrastruktury ze wspólnymi standardami, obejmującej sieci i bezpieczne chmury obliczeniowe obecnej i przyszłych generacji. Czwarty – uwzględnienie faktu, że podstawowym składnikiem cyfryzacji są dane, co powoduje, iż przepisy o ochronie danych muszą zostać odpowiednio zastosowane do sztucznej inteligencji w celu ochrony tożsamości cyfrowej. Piąty – zapewnienie innowacji dzięki wykorzystaniu całego potencjału wiedzy ukrytej w danych, umożliwienie rządom i firmom dzielenia się danymi i bezpiecznego ich łączenia. Szósty – wyciągnięcie wniosków z faktu, że bezpieczeństwo cybernetyczne i cyfryzacja to „dwie strony tego samego medalu", co nadaje priorytetowy charakter

[9] https://www.politico.eu/article/juncker-commission-digital-legacy-policies-tech-social-media-data/; https://www.politico.eu/article/ai-data-regulator-rules-next-european-commission-takes-aim/.

bezpieczeństwu cybernetycznemu. Na uwagę zasługuje powiązanie w omawianym przemówieniu kwestii konkurencyjności europejskich firm z surowymi wymaganiami bezpieczeństwa i jednolitym europejskim podejściem do niego. W tym kontekście padły słowa o potrzebie stworzenia wspólnej platformy działań w powyższych sprawach – Europejskiej Agencji ds. Bezpieczeństwa Cybernetycznego[10].

Trzeba dodać, że zapowiedzi standaryzacji rozwiązań cyfrowych w Unii Europejskiej zbiegły się w 2019 r. z kolejnymi wezwaniami do zaktualizowania unijnych zasad dotyczących internetu i mediów społecznościowych ze strony przedstawicieli mediów tradycyjnych oraz nadawców i dostawców usług szerokopasmowych. Przykładem takiego wezwania może być apel, z którym wystąpił w listopadzie Jeremy Darroch, dyrektor generalny grupy Sky. Zauważył on, że potężne firmy technologiczne działają wspólnie przeciwko uchwaleniu ustawy o usługach cyfrowych, w sytuacji gdy rozwiązania eksponujące wolność w internecie i ograniczenie nadzoru regulacyjnego nie uwzględniają zagrożeń internetowych. Rozwiązania te nie pozwalają skutecznie przeciwstawiać się używaniu internetu do celów moralnie nagannych oraz do zachowań przestępczych, m.in. do wykorzystywania seksualnego dzieci, upowszechniania fałszywych wiadomości i manipulacji politycznych. Nie umożliwiają też efektywnego blokowania biznesowych działań operatorów internetowych, którzy nie ponoszą odpowiedzialności za udostępniane treści[11]. Apel przedstawiciela Sky jest wyrazem napiętych stosunków – czy nawet antagonizmów – między mediami tradycyjnymi i społecznościowymi. Ze strony administratorów mediów społecznościowych niejednokrotnie padają oskarżenia, że media głównego nurtu są zbyt mocno uzależnione od ośrodków władzy państwowej oraz linii programowej redaktorów naczelnych, a treści przez nie generowane i upubliczniane wymagają korekty i uzupełnienia w mediach społecznościowych, które cechują się wolnością przekazu. Tak właśnie Mark Zuckerberg tłumaczył m.in. motywy uruchomienia projektu, w wyniku którego powstał Facebook, dzięki czemu „ponad 2 miliardy ludzi ma teraz większą szansę na wyrażenie siebie", zaś „miliony oczu i uszu oddanych użytkowników stosują organiczny test prawdy"[12].

Stosunkowo wcześnie kwestiami standaryzacji cyberprzestrzeni zajęła się Organizacja Współpracy Gospodarczej i Rozwoju (OECD). Już w 1980 r. organizacja ta wydała wytyczne w zakresie ochrony prywatności. W 1992 r. wypracowano wytyczne w sprawie ochrony społeczeństw przed zagrożeniami cybernetycznymi, zaś w 2002 r. uzgodniono wytyczne dotyczące bezpieczeństwa

[10] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_19_6408.

[11] https://www.politico.eu/sponsored-content/its-time-to-update-the-eus-internet-rules/.

[12] https://www.politico.com/magazine/story/2019/11/06/facebook-mark-zuckerberg-iraq-war-229903.

systemów i sieci informatycznych. Istotne znaczenie miały przyjęte w ramach OECD w 2014 r. zalecenia w sprawie zasad kształtowania polityki internetowej, których podstawowym przesłaniem było wzmocnienie gwarancji wolności w komunikacji internetowej. Zarazem jednak w dokumencie podkreślono konieczność zagwarantowania w internecie ochrony prywatności, bezpieczeństwa dzieci, ochrony własności intelektualnej i swobodnego przepływu informacji. Za rzecz niezbędną uznano wzmocnienie międzynarodowej współpracy w tych sprawach, a także elastyczność i wielostronność procesu dochodzenia do poszczególnych rozwiązań.

W przedstawionym przez OECD katalogu zasad i zaleceń znalazły się: swobodny przepływ informacji na świecie; otwarty i globalny internet; inwestycje i konkurencja w szybkich sieciach i usługach; transgraniczne świadczenie usług; współpraca zainteresowanych stron w procesach wypracowywania polityki; dobrowolne przyjęcie kodeksu postępowania przez podmioty działające w komunikacji internetowej; rozwijanie zdolności do wprowadzania publicznie dostępnych i wiarygodnych danych do procesu tworzenia polityki; zapewnienie przejrzystości i odpowiedzialności w komunikacji internetowej; zwiększenie spójności i skuteczności ochrony prywatności na poziomie globalnym; maksymalizowanie indywidualnego upodmiotowienia, kreatywności i innowacyjności; ograniczenie odpowiedzialności pośrednika internetowego; współpraca w promowaniu bezpieczeństwa w internecie; nadanie odpowiedniego priorytetu wysiłkom w kierunku egzekwowania prawa[13].

Przyjęte w czerwcu 2019 r. zasady OECD dotyczące sztucznej inteligencji promują sztuczną inteligencję (AI), która jest „innowacyjna i godna zaufania, szanuje prawa człowieka i wartości demokratyczne". Jak czytamy w dokumencie, oparte na tych zasadach standardy sztucznej inteligencji są wystarczająco praktyczne i elastyczne, by mogły być przydatne w warunkach szybko zachodzących zmian; są też powiązane z wcześniej wypracowanymi standardami OECD w takich obszarach, jak prywatność, zarządzanie ryzykiem w zakresie bezpieczeństwa cyfrowego i odpowiedzialne postępowanie biznesowe.

W omawianym dokumencie OECD sformułowano pięć uzupełniających się reguł „odpowiedzialnego zarządzania wiarygodną sztuczną inteligencją". Oto one: „Sztuczna inteligencja powinna przynosić korzyści ludziom i planecie poprzez stymulowanie wzrostu sprzyjającego włączeniu społecznemu, zrównoważony rozwój i dobrobyt. Systemy AI powinny być zaprojektowane w sposób, który szanuje praworządność, prawa człowieka, wartości demokratyczne i różnorodność oraz powinny obejmować odpowiednie zabezpieczenia – na przykład umożliwiające interwencję człowieka w razie potrzeby – w celu zapewnienia sprawiedliwego społeczeństwa. Należy zapewnić przejrzystość

[13] http://www.oecd.org/sti/ieconomy/internet-policy-and-governance.htm.

i odpowiedzialne ujawnianie informacji na temat systemów sztucznej inteligencji, aby ludzie rozumieli wyniki oparte na sztucznej inteligencji. Systemy AI muszą działać w sposób solidny i bezpieczny przez cały cykl życia, a potencjalne zagrożenia powinny być stale oceniane i zarządzane. Organizacje i osoby opracowujące, wdrażające lub obsługujące systemy sztucznej inteligencji powinny ponosić odpowiedzialność za ich prawidłowe funkcjonowanie zgodnie z powyższymi zasadami"[14].

Przedstawiono również pięć zaleceń dla rządów. Zdaniem OECD, rządy powinny: ułatwiać inwestycje publiczne i prywatne w badania i rozwój sztucznej inteligencji; wspierać ekosystemy AI dzięki infrastrukturze cyfrowej oraz technologiom i mechanizmom wymiany danych i wiedzy; wspierać politycznie procesy wdrażania wiarygodnych systemów AI; zapewniać ludziom umiejętności w zakresie sztucznej inteligencji; współpracować ponad granicami i sektorami, aby osiągać postęp w odpowiedzialnym zarządzaniu wiarygodną sztuczną inteligencją. Za szczególnie ważne zadanie uznano opracowanie wskaźników do pomiaru i analizy badań, rozwoju i wdrażania AI. Zapowiedziano utworzenie przez OECD obserwatorium polityki sztucznej inteligencji.

Wypracowaniem standardów ochrony prywatności w cyberprzestrzeni zajęła się Międzynarodowa Organizacja Normalizacyjna (ISO). W połowie 2019 r. ISO opublikowała pierwsze międzynarodowe standardy zarządzania informacjami o prywatności (ISO/IEC 27701), w których określono wymagania „dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji specyficznym dla prywatności". Rozszerzając wypracowane przed 20 laty normy ISO/IEC 27001 i ISO/IEC 27002, a także ponad 40 międzynarodowych standardów szczegółowych obejmujących m.in. zagadnienia bezpieczeństwa w chmurze oraz zasady identyfikowania przestępców informatycznych i korporacyjnych naruszeń bezpieczeństwa informacji (ISO/IEC 27017 i ISO/IEC 27018), sformułowano wytyczne adresowane do wszystkich organizacji, w tym firm publicznych i prywatnych, podmiotów rządowych i organizacji non profit[15].

8.5. Strategia rozwoju sztucznej inteligencji w Polsce: diagnoza i zadania

Diagnoza stanu rozwoju sztucznej inteligencji w Polsce • Indeksacja wyzwań gospodarczych, finansowych i rozwojowych, edukacyjnych, etycznych, prawnych związanych ze sztuczną inteligencją

[14] http://www.oecd.org/going-digital/ai/principles.

[15] https://www.iso.org/standard/71670.html; https://www.iso.org/news/ref2360.html.

Obszerna, merytoryczna diagnoza stanu rozwoju sztucznej inteligencji w Polsce i czekające nasz kraj zadania w tym zakresie zostały przedstawione w 2018 r. przez zespół pracujący pod auspicjami Ministerstwa Cyfryzacji. W dokumencie pt. *Założenia do strategii AI w Polsce* szczegółowo omówiono wyzwania związane ze sztuczną inteligencją, które pojawiają się w gospodarce, w sektorze finansów i rozwoju, edukacji oraz w dziedzinie etyki i prawa. W tym samym dokumencie zaprezentowano plan działań Ministerstwa Cyfryzacji na lata 2018–2019 dotyczących sztucznej inteligencji[16]. Dokument ten zawiera wartościową analizę problemów, które wymagają rozwiązania.

Mając na uwadze wyzwania dla gospodarki związane ze sztuczną inteligencją, w *Założeniach…* wyodrębniono: perspektywę krótkoterminową – okres do 2 lat, w którym za kluczowe uznano: opracowanie programów wsparcia projektów z zakresu ICT o wysokim potencjale gospodarczym, rozwijanie Krajowych Inteligentnych Specjalizacji (KIS), uruchomienie programu sektorowego ukierunkowanego na gospodarkę opartą na danych, pilotażowe przedsięwzięcia komercyjne i projekty badawczo-rozwojowe, zaangażowanie firm z sektora publicznego do udziału w projektach z zakresu gospodarki opartej na danych oraz sztucznej inteligencji; perspektywę średnioterminową – okres do 6 lat, w ramach którego zalecono przede wszystkim podjąć działania umożliwiające polskiej gospodarce uniknięcie odpowiednika „pułapki średniego rozwoju" w gospodarce opartej na danych; perspektywę długoterminową – okres do 2030 r., w którym szczególnie ważne będzie bieżące monitorowanie rozwoju sytuacji gospodarczej i dostosowanie działań do dynamicznie zmieniającej się rzeczywistości.

W obszarze finansów i rozwoju wskazano, że: Polska gospodarka w coraz większym stopniu gromadzi dane, jednak w dalszym ciągu słabo je analizuje; lista krajów, które przodują w rozwoju AI na świecie, mocno pokrywa się z listą liderów innowacji w ogóle; na świecie trwa wyścig związany ze sztuczną inteligencją, który ma wymiar wojskowy i gospodarczy; AI przetransferuje bogactwo do tych krajów, które będą potrafiły ją budować i kontrolować; niezbędne są w Polsce (omówione szczegółowo w dokumencie) rozwiązania tworzące dla AI system profesjonalnej transformacji obejmujący silnych liderów, jasne cele i właściwe narzędzia, złożony z ekosystemu technologicznego, edukacyjnego, naukowego, wsparcia państwowego, start-upowego i biznesowego.

W sprawach edukacji wskazano na: potrzebę systemowego budowania – na każdym etapie kształcenia – kompetencji niezbędnych do tworzenia, wdrażania i korzystania z technologii opartych na AI; niski poziom edukacji cyfrowej dzieci i młodzieży oraz niski odsetek Polaków gotowych uczyć się

[16] *Założenia do strategii AI w Polsce. Plan działań Ministerstwa Cyfryzacji*, Warszawa, 9 listopada 2018, mc.gov.pl.

przez całe życie i dostosowywać swoje kompetencje do zachodzących zmian rynku pracy, co w sumie jest barierą rozwoju AI; konieczność szybkiego zwiększenia liczby specjalistów tworzących rozwiązania bazujące na AI i wspierania zespołów naukowych pracujących nad projektami AI oraz dawania większej liczbie studentów technologii informacyjnej (*information technology*, IT) możliwości zdobywania doświadczenia praktycznego; niebezpieczeństwo niedopasowania umiejętności pracowników do potrzeb gospodarki opartej na nowych technologiach, co może hamować rozwój kraju i zwiększać ryzyko bezrobocia technologicznego; potrzebę zapewnienia silnego przywództwa politycznego i transformacji cyfrowej instytucji publicznych we wszystkich działach administracji rządowej, pod kierunkiem silnego cyfrowego lidera w każdym z tych działów; znaczenie kształcenia umiejętności i postaw związanych z AI – takich jak umiejętność pracy z danymi i traktowanie ich jako aktywa, świadomość działania algorytmów, logiczne myślenie oraz kompetencje etyczne i społeczne.

Istotne, zasługujące na szersze omówienie, treści dokumentu opracowanego przez ekspertów Ministerstwa Cyfryzacji dotyczyły wyzwań w dziedzinie etyki i prawa związanych ze sztuczną inteligencją. Podstawowe znaczenie z punktu widzenia prowadzenia polityk publicznych ma założenie, że administracja państwowa powinna wziąć odpowiedzialność za wypracowanie standardów etycznych i regulacji prawnych. Według autorów raportu, podejście administracji rządowej do zagadnień etycznych i prawnych AI powinno się charakteryzować: proaktywnością, inkluzywnością, lokalnym nastawieniem (uwzględnieniem specyfiki i zaawansowania technologicznego kraju), elastycznością wobec zmieniających się realiów technologicznych i społecznych, systematycznością działań oraz aktywnością i stanowczością w przypadku naruszeń standardów etycznych i prawnych. Celem powinno być wypracowanie stałych, przejrzystych i efektywnych mechanizmów pozwalających na zapewnienie ochrony praw podstawowych, skuteczne pozyskiwanie wiedzy o skutkach społecznych AI, wyznaczanie standardów etycznych AI, wspieranie stanowienia prawa wysokiej jakości regulującego obszary związane z wykorzystaniem AI.

Uznano, że do istotnych zagadnień prawnych związanych z rozwojem AI należy: zapewnienie ochrony praw człowieka (w tym zapewnienie prywatności i transparentności oraz przeciwdziałanie dyskryminacji); zapewnienie szerokiego dostępu do danych, przy pełnym poszanowaniu zasad ochrony danych osobowych (w tym przeciwdziałanie próbom ustanowienia prawa „własności" danych maszynowych); zapewnienie ochrony praw konsumenta w związku z wykorzystaniem AI; wypracowanie zasad odpowiedzialności cywilnej za szkody wyrządzone przy wykorzystaniu AI (w tym zasad odpowiedzialności za szkody spowodowane przez pojazdy autonomiczne); określenie zasad i uwarunkowań wykorzystania AI w procesie zawierania umów; rozważanie

wprowadzenia systemu wsparcia dla osób, które stracą pracę w związku z wdrożeniem AI.

Autorzy dokumentu uznali, że „Rozpoznanie pojawiających się wątpliwości natury etycznej i prawnej, wiedza na temat skutków społecznych oraz wypracowanie sprawnych mechanizmów stanowienia prawa pozwoli Polsce zminimalizować potencjalne negatywne skutki wykorzystania AI, zapewnić bezpieczeństwo obywateli i wyznaczać wysokie standardy etyczne oraz jasne regulacje sprzyjające wykorzystaniu AI w instytucjach publicznych i różnych sferach gospodarki dla dobra wspólnego”[17]. Za szczególnie ważne uznano wypracowanie mechanizmów pozwalających na ujawnianie tożsamości sztucznej inteligencji przez uwierzytelnianie partnerów relacji, których jedną ze stron są ludzie, zaś drugą stroną są urządzenia AI, a także na ograniczenie zakresu decyzji wiążących dla obywateli, które mogą być podejmowane automatycznie przez systemy AI.

Wskazując konieczność zapewnienia efektywnej ochrony praw podstawowych w ramach projektów dotyczących sztucznej inteligencji, przywołano następujące wartości: godność, wolność (którą warunkują: zrozumiałość, prywatność i ochrona danych, ujawnianie tożsamości sztucznej inteligencji, ograniczanie zakresu stosowalności narzędzi automatycznych – zwłaszcza wykorzystywania ich przez podmioty wykonujące funkcje publiczne i społeczne), równość (z położeniem nacisku na: przeciwdziałanie powstaniu kolejnego obszaru wykluczenia społecznego, ograniczanie stronniczości algorytmów i stronniczości danych, ochronę osób podatnych na sugestię, kształtowanie rynku pracy), sprawiedliwość (realizująca się poprzez: równoprawność dostępu do AI i do informacji, odpowiedzialność w świecie podległym działaniu algorytmów, przejrzystość działań, reprezentatywność standardów etycznych).

Jak stwierdzono w *Założeniach…*, etyczna ocena przedsięwzięć AI, finansowanych lub współfinansowanych ze środków publicznych, mających na celu zapewnienie ochrony praw podstawowych wymaga: identyfikacji i systematyzacji ryzyk etycznych, analizy wpływu na obywateli, pozyskania wiedzy o skutkach społecznych wdrażania rozwiązań AI, wypracowania rozwiązań prowadzących do minimalizowania negatywnego wpływu AI, zarządzania zmianami społecznymi i wdrażania odpowiednich regulacji na poziomie polityki państwa.

Zdaniem autorów raportu, w dążeniu do celu określonego jako „Osiągnięcie zdolności do koordynowania w skali kraju działań służących identyfikacji skutków społecznych AI, zapobiegania negatywnym skutkom AI lub reagowania na nie, wypracowywania standardów etycznych mających na celu wspieranie AI w budowaniu społeczeństwa dobrobytu, budowania transparentności i zaufania społecznego do AI oraz wspierania administracji w zakresie

[17] Tamże, s. 121.

stanowienia prawa dotyczącego różnych wymiarów AI" – niezbędne jest powołanie ośrodka analiz AI finansowanego z pieniędzy publicznych. Ośrodek taki powinien łączyć w sobie cechy organizacji branżowej, skupiającej kluczowe firmy i podmioty, z mocnym wsparciem naukowym oraz zaangażowaniem podmiotów administracji państwowej i innych podmiotów publicznych.

Wśród kwestii prawnych wymagających rozstrzygnięcia, m.in. w ramach działań legislacyjnych, wskazano na potrzebę zagwarantowania: prawa do prywatności, prawa do równego traktowania, transparentności (w tym dostępu do informacji o działaniach algorytmów), dostępu do danych. Zestawiono pojawiające się wątpliwości i problemy prawne w zakresie prawa cywilnego oraz prawa własności intelektualnej, zaliczając do tej grupy m.in. kwestie: osobowości prawnej AI, odpowiedzialności odszkodowawczej za szkody spowodowane przez AI, wykorzystywania AI w procesie zawierania umów, ochrony konsumenta, prawa własności intelektualnej. W zakresie prawa administracyjnego i postępowań administracyjnych rekomendowano ustalenie podstawowych zasad automatyzacji czynności w stosunkach administracyjnoprawnych na linii państwo–obywatel. Jako odrębne problemy wskazano zagadnienia opodatkowania pracy robotów oraz wsparcia dla osób, które utraciły pracę w związku z zastosowaniem narzędzi AI.

We wrześniu 2020 r., po kilkunastomiesięcznych konsultacjach, Komitet Rady Ministrów do spraw Cyfryzacji zatwierdził dokument pt. *Polityka rozwoju sztucznej inteligencji w Polsce*, w którym nakreślono cele i zadania związane z AI w perspektywie krótkoterminowej (do 2023 r.), średnioterminowej (do 2027 r.) i długoterminowej (po 2027 r.). Oddzielnie przedstawiono zadania w dziedzinie: podnoszenia kompetencji cyfrowych społeczeństwa[18], wsparcia przez państwo przedsiębiorstw innowacyjnych, rozwoju interdyscyplinarnych badań oraz przygotowania kadry ekspertów od AI, edukacji, współpracy międzynarodowej, wsparcia sektora publicznego w realizacji zamówień na rzecz AI. W dokumencie uwzględniono problemy projektowania rozwiązań, badań, rozwoju, wdrożenia, stosowania i używania AI oraz wyłączenia z obrotu poszczególnych produktów. Założono, że proces wdrożenia i finansowania programu ma być koordynowany na poziomie rządowym. Dokument ten wymaga zatwierdzenia przez Radę Ministrów.

O potrzebie edukacji polskiego społeczeństwa w zakresie nowych technologii świadczy wymownie przykład aktywności normotwórczej Rady Miasta Kraśnik, która przyjęła uchwałę w sprawie uczynienia tego miasta „strefą wolną od 5G". Radni wycofali się z uchwały dopiero pod wpływem prześmiewczej

[18] Na temat potrzeby prowadzenia takich działań zob. A. Tarkowski i in., *Analiza strategii i działań mających na celu rozwój kompetencji cyfrowych w państwach Unii Europejskiej*, https://cppc.gov.pl/images/Analiza_strategii_i_dzia%C5%82an_majacych_na_celu_rozwoj_kompetencji_cyfrowych_w_panstwach_Unii_Europejskiej.pdf.

krytyki w mediach społecznościowych. Trzeba jednak zaznaczyć, że zaprezentowane przez nich podejście do nowych technologii nie jest w Europie wyjątkiem; według stanu z jesieni 2020 r., aż w 10 państwach Unii Europejskiej zarejestrowano przypadki niszczenia instalacji naziemnej sieci 5G, w tym podpalenia wież transmisyjnych tej sieci, na fali oskarżeń o wywieranie przez nią szkodliwego wpływu na zdrowie ludzi.

Rozdział dziewiąty

Cywilizacja cyfrowa jako wyzwanie dla rządzenia w sferze bezpieczeństwa

9.1. Nowe cyfrowe możliwości i zagrożenia w sferze działań ofensywnych, obronnych i ochronnych

Zagrożenia związane z prowadzeniem za pomocą środków niemilitarnych wojny sieciowej • Wpisanie internetu do katalogu narzędzi agresji propagandowej prowadzonej przez państwa

Wraz z rozwojem technologii informacyjnych i cyfrowych pojawiają się nowe wyzwania w dziedzinie bezpieczeństwa informatycznego i informacyjnego. Z umacnianiem się obecności nowych technologii wokół nas wiążą się bezpośrednio różne aspekty bezpieczeństwa międzynarodowego oraz bezpieczeństwa państw, pozapaństwowych struktur instytucjonalnych, a także pojedynczych osób.

Od dawna wskazuje się na zagrożenia związane z prowadzeniem za pomocą środków niemilitarnych wojny sieciowej (zwanej nieraz netwojną). Jej istotą jest wpływanie na świadomość społeczną (i w ślad za tym – na zachowania ludzi). Wiąże się ona bezpośrednio z cyberwojną, która ma na celu zakłócenie możliwości operowania informacją (traktowaną jako zasób strategiczny) w systemach o najważniejszym znaczeniu dla działania państwa, podmiotów niepaństwowych oraz poszczególnych ludzi[1]. Współcześnie wojna informacyjna staje się coraz ważniejszym elementem rzeczywistości. Upowszechnienie internetu i mediów społecznościowych stworzyło dla niej wyjątkowo sprzyjające warunki[2].

---

[1] J. Arquilla, D. Ronfeldt, *Cyberwar is coming!*, w: J. Arquilla, D. Ronfeldt (red.), *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND Corporation 1993, http://www.rand.org.

[2] Zob.: T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016; J. Lebiedź, W. Krztoń, B. Stefaniuk, *Współczesne wyzwania bezpieczeństwa narodowego. Zarządzanie kryzysowe, wojna*

Walka w cyberprzestrzeni odbywa się formalnie przede wszystkim między operatorami i administratorami różnych systemów informatycznych a hakerami. Obecnie można jednak już z prawdopodobieństwem graniczącym z pewnością stwierdzić, że za hakerami ukrywają się niejednokrotnie państwowi zleceniodawcy i mecenasi. Tradycyjne operacje wojskowe są w ramach działań hybrydowych łączone z atakami propagandowymi, dezinformacją i cyberatakami. Jako przykłady takich działań można wskazać kampanię propagandową władz USA mającą osłonić inwazję wojskową na Irak w latach 2003–2005, a także operacje dezinformacyjne w trakcie aneksji Krymu przez Rosję w 2014 r. W istocie, historia zna wiele wcześniejszych przypadków łączenia walki zbrojnej z agresją propagandową i dezinformacją (oczywiście, do pewnego czasu prowadzoną bez udziału technologii informatycznych). Najbardziej znane tego typu fakty z okresu po II wojnie światowej przypomniał w opublikowanej niedawno książce Thomas Rid[3]. Dezinformacja, traktowana jako aktywne narzędzie walki politycznej, opiera się na stale doskonalonych mechanizmach zorganizowanego, profesjonalnego kłamstwa, które współcześnie jest na wielką skalę upowszechniane w cyberprzestrzeni.

Internet jest w naszych czasach wykorzystywany przez niektóre państwa do uprawiania agresywnej propagandy. Gra informacyjna staje się istotnym elementem walki o wpływy i dominację w świecie. W przeszłości miały już miejsce konflikty militarne i polityczne wywołane przez rozpowszechnianie fałszywych informacji[4]. Internet, wyposażony w zaawansowane technologie pozwalające wytwarzać budzące zaufanie odbiorcy obrazy i filmy, w tym manipulować zapisami mowy i materiałem zdjęciowym, doskonale nadaje się do prowadzenia tego typu działań. Miejsce klasycznych metod ataku zajmują ofensywne działania w cybersferze – coraz lepiej zorganizowane i kamuflowane kampanie propagandowe, zjawiska dezinformacji i manipulacji, inspirujące określone zachowania destrukcyjne przy wykorzystaniu zasad socjotechniki[5]. Ta tendencja będzie się nasilać[6]. Taką ocenę potwierdzają pośrednio nawet

informacyjna w cyberprzestrzeni, rzeczywistość wirtualna, Warszawa 2018; R. Rajczyk, *Nowoczesne wojny informacyjne*, Warszawa 2016; M. Wrzosek, S. Markiewicz, Z. Modrzejewski (red.), *Informacyjny wymiar wojny hybrydowej*, Warszawa 2019; P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny…*

[3] Th. Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, New York 2020.

[4] Zob. zestawienie takich konfliktów: https://www.politico.com/magazine/story/2019/07/05/fake-news-real-war-227272.

[5] R. Brzeski, *Wojna informacyjna – wojna nowej generacji*, Komorów 2014; A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

[6] L. Freedman, *Przyszła wojna. Wizja przyszłej wojny. Jak ją sobie wyobrażano dawniej? Jak widzimy ją dzisiaj?*, Warszawa 2019, s. 299 i nast.

oficjalne dokumenty poszczególnych państw, w tym krajów, które dążą do uzyskania dominującej pozycji w świecie.

W Rosji jako formalną przesłankę podejmowania skoordynowanych działań informacyjnych tradycyjnie wskazuje się dążenie do zagwarantowania bezpieczeństwa państwa[7]. Jednak z czasem w ujęciach doktrynalnych większą rolę zaczęto przypisywać działaniom ofensywnym ukierunkowanym na poszerzenie wpływów Rosji w świecie[8]. W praktyce wojskowa strategia informacyjna Rosji przewiduje zintegrowanie tradycyjnych działań ofensywnych z operacjami o charakterze informacyjno-psychologicznym i cybernetycznym. Zamiarem władz jest narzucanie opinii publicznej mocarstwowej narracji o polityce Rosji, w tym szczególnie o aktywności na rzecz umacniania stref wpływów (m.in. w Ukrainie i Syrii)[9].

Cyberprzestrzeni przypadła ważna rola w polityce bezpieczeństwa w Chinach. Przyjęto tam strategię przygotowania się do prowadzenia działań ofensywnych i obronnych w cyberprzestrzeni oraz w sferze informacyjno-propagandowej. W ustawie o bezpieczeństwie narodowym z lipca 2015 r. kluczowe znaczenie nadano możliwości prowadzenia efektywnych działań w cyberprzestrzeni. W dokumencie tym uznano wolność panującą w cyberprzestrzeni za jedno z istotnych źródeł zagrożeń wewnętrznej stabilizacji w państwie oraz zapowiedziano działania idące w kierunku kontrolowania internetu i kształtowania sieci informatycznej podzielonej na „sektory narodowe". Wiele wskazuje na to, że Chiny wykorzystują cyberprzestrzeń do celów wywiadowczych: nielegalnie i niejawnie, także za pomocą grup hakerskich, penetrują strategiczne bazy danych innych krajów, podmiotów gospodarczych i administratorów platform internetowych[10].

W narodowej strategii wywiadowczej USA na 2019 r., uzyskiwanie informacji o zagrożeniach cybernetycznych wskazano jako jeden z siedmiu głównych priorytetów służb. Z kolei w strategii kontrwywiadu Stanów Zjednoczonych Ameryki na lata 2020–2022, przedstawionej przez Narodowe Centrum Kontr-

---

[7] Zob. *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej* (zatwierdzona dekretem Prezydenta Federacji Rosyjskiej nr Pr-1895 z dnia 9 września 2000 r.), w: M. Berliński, R. Zulczyk, *Federalna Służba Bezpieczeństwa Federacji Rosyjskiej*, Warszawa 2016, s. 235 i nast.

[8] Por. m.in. dekret Prezydenta FR z dnia 22 maja 2015 r. *O niektórych problemach bezpieczeństwa informacyjnego FR* oraz *Doktryna bezpieczeństwa informacyjnego* z dnia 5 grudnia 2016 r. Zob.: A. Kuczyńska-Zonik, *Strategia bezpieczeństwa informacyjnego Federacji Rosyjskiej*, w: J. Trubalska, Ł. Wojciechowski (red.), *Bezpieczeństwo państwa w cyberprzestrzeni*, Lublin 2017, s. 97 i nast.; Y. Harrel, *Rosyjska cyberstrategia*, Warszawa 2015.

[9] J. Darczewska, *Rosyjskie siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*, Ośrodek Studiów Wschodnich, Warszawa 2016, Prace OSW nr 57.

[10] Zob.: P. Borkowski, *Koncepcja cyberbezpieczeństwa w ujęciu Chińskiej Republiki Ludowej – wybrane aspekty*, Agencja Bezpieczeństwa Wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13 (7), s. 49 i nast.; M. Kaczmarski, *Chiny przyjmują nowe prawo o bezpieczeństwie narodowym*, Analizy Ośrodka Studiów Wschodnich, 15.07.2015.

wywiadu i Bezpieczeństwa (NCSC) w lutym 2020 r., operacje cybernetyczne i techniczne prowadzone przez inne państwa zostały uznane, obok ataków na infrastrukturę krytyczną, kluczowe łańcuchy dostaw, gospodarkę i instytucje demokratyczne, za jedno z najważniejszych zagrożeń bezpieczeństwa USA. Podkreślono, że takie państwa, jak Rosja, Chiny, Iran, Kuba i Korea Północna, oraz takie podmioty niepaństwowe, jak libański Hezbollah, ISIS i Al-Kaida, dysponują stale rozwijanymi zdolnościami wywiadowczymi i zaawansowanymi technologiami, w tym coraz doskonalszymi narzędziami cybernetycznymi, urządzeniami biometrycznymi, zdjęciami w wysokiej rozdzielczości, ulepszonym sprzętem służącym do nadzoru technicznego, szyfrowania i analizy dużych zbiorów danych. Podmioty te starają się wpływać na amerykańską opinię publiczną. Rozwój technologii nowej generacji, w tym technologii 5G i sztucznej inteligencji, daje wrogom zewnętrznym – czy też zagranicznym konkurentom politycznym – zwiększone możliwości zbierania danych wywiadowczych i prowadzenia operacji cybernetycznych przeciwko Stanom Zjednoczonym[11].

9.2. Wzrastające uzależnienie państw i ludzi od niezakłóconego funkcjonowania narzędzi cyfrowych

Wzrost znaczenia gwarancji bezpieczeństwa systemów informatycznych • Doskonalenie instrumentów destrukcyjnego oddziaływania na rozwiązania i zasoby teleinformatyczne • Systemowy charakter działań dotyczących bezpieczeństwa w cyberprzestrzeni • Reaktywność w działaniach rządów i instytucji międzynarodowych w sprawach bezpieczeństwa elektronicznego

Konsekwencją upowszechnienia urządzeń i technik elektronicznych w instytucjach publicznych oraz w życiu poszczególnych ludzi jest narastające uzależnienie państw i ludzi od niezakłóconego funkcjonowania różnych narzędzi cyfrowych. Zadaniem najwyższej wagi staje się zagwarantowanie bezpieczeństwa systemów informatycznych. Kwestie cyberbezpieczeństwa nabierają kluczowego znaczenia[12]. Dotyczy to w pierwszym rzędzie infrastruktury krytycznej państwa, w tym sieci energetycznych, zaopatrzenia w wodę, systemów łączności, sieci transportowych i finansowych. Powszechna informatyzacja niesie za sobą ryzyko celowo wywołanych lub przypadkowych awarii tych systemów w newralgicznych dla państw instytucjach, procedurach i zbiorach danych.

[11] https://www.dni.gov/index.php/newsroom/press-releases/item/2098-ncsc-unveils-the-national-counterintelligence-strategy-of-the-u-s-2020-2022.

[12] M. Górka, *Cyberbezpieczeństwo jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku*, Warszawa 2014.

Incydenty w cybersferze mogą naruszać ważne interesy danych podmiotów pozapaństwowych oraz godzić w wartości i interesy ludzi, w skrajnych przypadkach stwarzając zagrożenie życia lub zdrowia[13].

Do stale doskonalonych instrumentów przeznaczonych do destruowania rozwiązań i zasobów teleinformatycznych należą różne formy cyberataku. Jak podaje Jan Zych, wśród metod i technik cyberataków mieszczą się różne rodzaje złośliwego oprogramowania (m.in. wirusy, robaki sieciowe, konie trojańskie, dialery, bonety, bomby logiczne) oraz inne działania wymierzone w bezpieczeństwo lub funkcjonalność sieci: skanowanie, oszustwa prowadzące do ujawnienia wrażliwych danych, zablokowanie systemów teleinformatycznych (m.in. rozsyłanie spamu, zapełnienie serwerów, wykorzystanie nieujętych w dokumentacji furtek pozwalających na przejęcie kontroli nad urządzeniem, zagłuszanie i zakłócanie funkcjonowania sieci, uszkodzenie urządzeń przy wykorzystaniu impulsów elektrycznych i elekromagnetycznych wysokiej mocy lub częstotliwości)[14].

Wzrasta przekonanie, że działania na rzecz bezpieczeństwa w cyberprzestrzeni muszą mieć charakter systemowy i wieloelementowy[15]. Chodzi tu zwłaszcza o rozwiązania i działania: polityczne – związane głównie z budowaniem międzynarodowej współpracy w tej dziedzinie; prawne – obejmujące przede wszystkim standaryzację aktywności w cybersferze, w tym w zakresie zabezpieczeń oraz dostępu do zasobów danych, a także ustalenie zasad odpowiedzialności prawnej za niedopuszczalne zachowania lub zaniechania w sprawach bezpieczeństwa sieci i urządzeń teleinformatycznych; instytucjonalne i proceduralne – zapewniające monitorowanie sytuacji oraz przeciwdziałanie operacyjne w przypadku pojawienia się incydentów godzących w bezpieczeństwo teleinformatyczne; edukacyjne – obejmujące kształtowanie świadomości i umiejętności w sprawach cyberbezpieczeństwa; naukowo-badawcze – związane z projektami i wdrożeniami podwyższającymi poziom zabezpieczeń przed intencjonalnymi i awaryjnymi zagrożeniami w cyberprzestrzeni. Najwyższą rangę uzyskują działania prewencyjne, w tym aktywność kontrwywiadu cybernetycznego oraz właściwe zabezpieczenie urządzeń i sieci komunikacji teleinformatycznej.

Rządy i instytucje międzynarodowe muszą się w kwestiach bezpieczeństwa elektronicznego w dużej mierze ograniczać do zachowań reaktywnych, bowiem inicjatywa wypracowywania nowych metod i technik agresji cybernetycznej należy raczej do hakerów. Często dysponują oni znacznymi środkami finan-

---

13 Zob.: M. Marczyk, R. Janczewski, B. Terebiński (red.), *Militarne aspekty cyberbezpieczeństwa państwa w czasie działań hybrydowych przeciwko RP*, Warszawa 2020; M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne…*; C. Banasiński (red.), *Cyberbezpieczeństwo…*

14 Szczegółowy opis metod i technik cyberataków, zob. J. Zych, *Teleinformatyka dla bezpieczeństwa…*, s. 115 i nast.

15 E. Lucas, *Oswoić cyberświat. Tożsamość, zaufanie i bezpieczeństwo w internecie*, Warszawa 2017.

sowymi i zdolnościami technicznymi do realizacji swoich planów, zwłaszcza wtedy, gdy są na usługach państw używających agresji w cyberprzestrzeni do osiągania swoich celów politycznych i ekonomicznych. Przeciwdziałanie tym praktykom wymaga także ogromnych środków finansowych i rozbudowanych systemów instytucjonalnych (w tym kontrwywiadu elektronicznego) do monitorowania i analizowania kontekstu technologicznego i geopolitycznego oraz standaryzacji i blokowania tysięcy przypadków agresji elektronicznej. Przykładowo, w USA system taki (noszący nazwę Einstein) jest sukcesywnie rozbudowywany od 2009 r. Koszty instalacji i obsługi tego systemu w okresie do 2018 r. szacuje się na 5,7 miliarda dolarów. W Narodowej Agencji Bezpieczeństwa funkcjonuje elitarna jednostka, która zatrudnia kilkuset osób pracujących w trybie całodobowym i korzysta z wyników tajnych operacji szpiegowskich[16].

Zdolność ograniczania istniejących zagrożeń w cybersferze jest w bardzo dużym stopniu uzależniona od posiadania przez szerokie kręgi użytkowników komunikacji internetowej wiedzy o bezpiecznych zachowaniach w sieci i o metodach działania elektronicznych agresorów. Z tego powodu zmieniają się schematy zachowania w sprawach bezpieczeństwa w internecie służb specjalnych i innych organów wchodzących w skład systemów cyberbezpieczeństwa. Podmioty te, tradycyjnie operujące w sferze informacji niejawnych i nieskore do dzielenia się posiadaną wiedzą, w tym przypadku podejmują coraz częściej aktywne działania informacyjne.

9.3. Ewolucja pola walki i konfliktów w związku z rozwojem technologii cyfrowych

Wzrost liczby cyberataków na infrastrukturę informatyczną poszczególnych państw, miast i instytucji oraz na urządzenia informatyczne używane przez osoby prywatne • Eskalacja ataków cybernetycznych do poziomu stanowiącego zagrożenie dla bezpieczeństwa międzynarodowego • Problem powstawania zabójczych autonomicznych systemów broni

Pod wpływem upowszechniania i doskonalenia technologii cyfrowych następuje ewolucja pola walki i charakteru konfliktów militarnych. Klawiatura komputera i powierzchnia ekranów dotykowych, łącza internetowe i narzędzia inteligentnych technologii zaczynają wspomagać, a nawet zastępować bomby i inne środki rażenia stosowane dotychczas na polu walki. Możliwości, jakie

[16] https://www.politico.com/agenda/story/2017/10/11/government-cyber-attack-companies-000539.

oferują nowe technologie cyfrowe, sprawiają też, że do konfliktów mogą się niepostrzeżenie włączać podmioty niepaństwowe o anonimowej tożsamości.

Zmiany obszaru i charakteru współczesnych konfliktów wymagają nowych kompetencji podmiotów państwowych odpowiedzialnych za obronę i bezpieczeństwo wewnętrzne. Obraz tej nowej sytuacji w odniesieniu do USA ukazali w połowie 2019 r. dwaj amerykańscy autorzy zaangażowani w zwalczanie dezinformacji w internecie: Stanley McChrystal – emerytowany generał armii, i David Eichenbaum – konsultant do spraw mediów. W swoim artykule stwierdzili oni m.in.: „Nasze wojsko jest przyzwyczajone do prowadzenia i wygrywania konwencjonalnych wojen z czołgami, wojskami i samolotami. Ale dzisiejsze cyfrowe pole bitwy przedstawia zupełnie nowy krajobraz – taki, w którym aktorzy państwowi i niepaństwowi uczestniczą w szalejącej asynchronicznej wojnie informacyjnej (…). Nasi przeciwnicy są zdecentralizowani – mieszanka wrogich obcych mocarstw, niepaństwowych aktorów i jednostek, od Rosji i Chin po wewnętrzne zagrożenia (…). W niektórych przypadkach korzystali nawet z platform internetowych, aby osiągnąć cele zarezerwowane dotychczas tylko dla otwartej wojny”[17].

Ataki cybernetyczne przenoszą się do świata materialnego. Realne staje się niebezpieczeństwo cyberwojny. Planowe niszczenie lub modyfikowanie systemów informacyjnych państwa lub przepływających przez te systemy informacji stanowi poważne zagrożenie, które nakazuje przygotować cywilne i militarne struktury państwowe do obronnego i ofensywnego przeciwdziałania. Należy się zgodzić z opinią, że już obecnie większość konfliktów między państwami podlega „cybernetyzacji”, gdyż sukces lub porażka uczestników tych konfliktów zależą od działań prowadzonych w sieciach komputerowych[18]. Ponieważ przebieg konfliktów jest w tak dużym stopniu uzależniony od niezawodnego działania systemów elektronicznych, zablokowanie funkcjonowania i infiltracja sieci komputerowych będą odgrywać coraz istotniejszą rolę na współczesnym polu walki.

Pisząc, że ataki cybernetyczne przenoszą się do świata materialnego, mam na uwadze szczególnie wydarzenia z przełomu 2009 i 2010 r., kiedy za pomocą złośliwego oprogramowania komputerowego Stuxnet doprowadzono do uszkodzenia wirówek służących do wzbogacania uranu w zakładach w Iranie. W sposób zakamuflowany zaatakowano urządzenia formalnie odizolowane od łączy sieciowych, wykorzystując robaka umieszczonego w sterownikach Siemensa używanych w procesie technologicznym. Działania te zostały przypisane służbom amerykańskim i izraelskim. Przypadek ten pokazuje również,

---

17 https://www.politico.com/magazine/story/2019/07/25/russias-prepared-to-interfere-in-2020-will-the-us-be-ready-227477.

18 K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe” 2011, nr 17, s. 17.

że szkody spowodowane konfliktem cybernetycznym mogą się szybko rozprzestrzenić poza zamierzony cel, bowiem tym samym złośliwym oprogramowaniem zainfekowano inne systemy komputerowe[19].

Każdy rok przynosi kolejne przypadki ataków na infrastrukturę informatyczną poszczególnych państw, miast i instytucji oraz na urządzenia informatyczne będące w posiadaniu osób prywatnych. Przykładowo, można wskazać liczne, przypisywane Rosji, destrukcyjne działania cybernetyczne prowadzone w latach 2016–2018 na Ukrainie, z wykorzystaniem szkodliwego oprogramowania znanego jako NotPetya, wywołujące zakłócenia w łączności rządowej oraz w sieci infrastruktury krytycznej, w tym w produkcji i dystrybucji energii elektrycznej oraz w funkcjonowaniu programu podatkowego, banku centralnego i lotniska w Kijowie. To złośliwe oprogramowanie rozprzestrzeniało się, infekując systemy w Stanach Zjednoczonych i wielu krajach w Europie i Azji[20]. W tym samym okresie, na przełomie 2016 i 2017 r., doszło do ataku cybernetycznego na sieci internetowe w Arabii Saudyjskiej, usunięto wtedy dane z kilkudziesięciu sieci państwowych i komercyjnych. Na całym świecie mnożą się przypadki ataków *ransomware* i *malware*, które zakłócają funkcjonowanie globalnych linii przesyłowych i produkcyjnych. W 2018 r. miał miejsce zmasowany, jak dotychczas największy atak cybernetyczny, przypisywany Korei Północnej, przeprowadzony za pomocą oprogramowania *ransomware* WannaCry, który zablokował sieci komputerowe w szpitalach, uniwersytetach i przedsiębiorstwach w ponad stu różnych krajach. Sprawcy ataku domagali się zapłaty okupu i zagrozili usunięciem danych zgromadzonych w pamięci zainfekowanego sprzętu[21]. W 2018 r. doszło też do ataku cybernetycznego na sieci informatyczne miasta Atlanta w amerykańskim stanie Georgia. Używając złośliwego oprogramowania, uszkodzono ponad jedną trzecią spośród 424 programów wykorzystywanych przez miasto do świadczenia usług, w tym usług w ramach infrastruktury krytycznej[22].

Eskalacja konfliktów cybernetycznych w skrajnych przypadkach stwarza zagrożenie bezpieczeństwa międzynarodowego. W 2019 r. doszło do wzajemnego zestrzelenia przez Iran i USA dronów operujących w strefie konfliktu na Bliskim Wschodzie[23]. Te incydenty, wraz z nasilającymi się wzajemnymi atakami na infrastrukturę krytyczną obu państw, potwierdziły, że konfrontacja militarna zaczyna się przenosić do cyberprzestrzeni. Przy okazji tego starcia

19 https://www.politico.com/story/2019/07/13/trump-cybersecurity-defense-1415650.

20 https://www.politico.com/story/2018/02/15/white-house-blames-russia-for-massive-ukraine-cyberattack-638151.

21 https://www.politico.com/story/2017/12/18/trump-north-korea-cyberattack-wannacry-290222.

22 https://www.dni.gov/index.php/ctiic-newsroom/item/1899-statement-for-the-record-mr-michael-moss-for-confirmation-before-the-senate-select-committee-on-crime-and-terrorism-to-be-deputy-director-of-the-cyber-threat-intelligence-integration-center.

23 https://www.politico.com/story/2019/07/18/trump-warship-iranian-drone-1422145.

cybernetycznego minister ds. łączności i technologii informacyjnej Iranu poinformował, że system zapór sieciowych tego kraju zneutralizował w 2018 r. 33 miliony ataków cybernetycznych[24].

Nasuwa się tutaj wniosek, że istnieje zależność między wzrostem liczby cyberataków wymierzonych w infrastrukturę państwową a zagrożeniem urządzeń elektronicznych podmiotów pozapaństwowych i osób indywidualnych. Nasilenie się napięć w stosunkach między Waszyngtonem i Teheranem oraz zwiększenie liczby amerykańskich ataków cybernetycznych na cele w Iranie[25] doprowadziły bowiem do lawinowego wzrostu ataków irańskich hakerów na systemy komputerowe (m.in. systemy energetyczne i zasoby podmiotów naukowych) w USA. O destrukcyjnych możliwościach tego typu działania świadczy atak z 2012 r. – o którego przeprowadzenie podejrzewano Iran – kiedy to za pomocą złośliwego oprogramowania „wyczyszczono" dyski twarde około 30 tysięcy zainfekowanych komputerów saudyjskiej państwowej firmy naftowej Saudi Aramco.

Postęp w rozwoju inteligentnych technologii doprowadził do powstania systemów broni autonomicznej, tj. urządzeń bojowych mogących samodzielnie – bez ingerencji człowieka – podejmować decyzje co do wyboru i zaatakowania konkretnego celu. Pojawia się w związku z tym pytanie o dopuszczalność używania w konfliktach tego typu broni, w tym zwłaszcza zabójczych autonomicznych systemów broni. Często dochodzi przecież do błędów w operacjach wykonywanych z zastosowaniem narzędzi elektronicznych, przede wszystkim dronów, a błędy te przynoszą nieraz tragiczne następstwa. Pokazują one, jak duże jest ryzyko tkwiące w działaniach militarnych na odległość. Dziś są to operacje prowadzone przy użyciu bezzałogowych obiektów sterowanych ze znacznej odległości przez ludzi. Jednak obserwując tempo rozwoju technologii elektronicznych, należy sądzić, że już niedługo cały proces sterowania tymi obiektami będzie obsługiwany przez roboty pełniące rolę automatycznych pilotów. Wiążą się z tym poważne problemy prawne, etyczne i polityczne. Pojawiają się zagrożenia dla przestrzegania norm międzynarodowego prawa humanitarnego, poszanowania praw człowieka, w tym zasady jego niezbywalnej godności. Istnieją też – co w kontekście decydowania politycznego jest szczególnie ważne – „przesłanki, że bezzałogowe systemy uzbrojenia zwiększają prawdopodobieństwo konfliktów zbrojnych, to znaczy obniżają polityczny próg użycia siły"[26].

---

[24] https://www.cyberdefence24.pl/amerykanski-atak-na-irak-w-cyberprzestrzeni-analiza.

[25] https://www.politico.com/story/2019/06/21/us-iran-cyberattacks-3469447; https://www.politico.com/story/2019/07/13/trump-cybersecurity-defense-1415650.

[26] Szerzej na temat problemów związanych z tym zagadnieniem piszą A. Dahlmann i M. Dickow w ekspertyzie przygotowanej dla Niemieckiego Instytutu Spraw Międzynarodowych i Bezpieczeństwa, https://www.swp-berlin.org/10.18449/2019RP03/#hd-d15993e810.

Dziś na dużą skalę są wykorzystywane drony. Najwcześniej sprzęt ten pojawił się w USA, gdzie w latach 90. XX w. był stosowany do obserwacji wojskowej, w Wielkiej Brytanii i Izraelu. Z czasem drony znalazły się m.in. w arsenałach Pakistanu, Turcji i państw arabskich. W zamiarach ofensywnych zaczęto się posługiwać dronami po atakach terrorystycznych z 11 września 2001 r. w USA. Analitycy przewidują, że w ciągu najbliższych 10 lat na świecie zostanie zakupionych ponad 80 000 dronów monitorujących i 2000 dronów szturmowych. Sukcesywnie spadają koszty ich produkcji. Problemem jest znaczna liczba błędów w identyfikowaniu celów ataków. Wiążą się z tym straty ludzkie i materialne wykraczające poza efekty założone w poszczególnych atakach[27].

Specjaliści zajmujący się tą problematyką wskazują, że siły zbrojne inwestują obecnie miliony dolarów w projekty technologii autonomicznych dronów. Prace te nie znajdują się jeszcze na bardzo zaawansowanym etapie, ale tak duże zaangażowanie finansowe musi się przełożyć na stałe ulepszanie tego narzędzia walki. Eskadry dronów wysłano już w 2018 r. do ataków na rosyjską bazę lotniczą Hmeimim w zachodniej Syrii. Jak zauważył Paul Scharre, analityk badający broń wykorzystującą sztuczną inteligencję, „był to pierwszy przypadek ataku dronem masowym i najwyższa liczba dronów, których (…) aktorzy niepaństwowi używali jednocześnie podczas operacji bojowej”[28]. We wrześniu 2019 r. przedstawiciele armii rosyjskiej stwierdzili, że zestrzelili w tymże roku prawie 60 dronów wokół bazy Hmeimim. Według analityków, drony mogą w ciągu dekady osiągnąć zdolność oceniania celów, dzielenia zadań i wykonywania ich przy ograniczonej interakcji człowieka. W 2018 r. Agencja Zaawansowanych Projektów Badawczych Obrony USA ujawniła, że w trakcie testów niewielka eskadra jej dronów z powodzeniem dzieliła się informacjami, przydzielała zadania i podejmowała skoordynowane decyzje taktyczne zarówno wobec wstępnie zaprogramowanych, jak i nowych, pojawiających się niespodziewanie zagrożeń[29].

Planuje się stworzenie autonomicznych urządzeń bojowych, w tym śmiercionośnych systemów broni, nie tylko z przeznaczeniem dla przestrzeni powietrznej. Przykładowo, w USA są prowadzone zaawansowane prace nad stworzeniem zrobotyzowanych, zdalnie sterowanych pojazdów bojowych (*robotic combat vehicle*, RCV), a równocześnie zaczęto testować miniaturowe drony (ważące mniej niż 33 gramy), które mają być wsparciem dla piechoty[30]. Instalowanie blokad zapobiegającym nadużyciom w wykorzystaniu urządzeń

---

27 https://www.theguardian.com/news/2019/nov/18/killer-drones-how-many-uav-predator-reaper.

28 https://www.theguardian.com/news/2019/dec/04/are-drone-swarms-the-future-of-aerial-warfare.

29 Tamże.

30 https://cyfrowa.rp.pl/technologie/roboty/35844-zrobotyzowane-pojazdy-bojowe-to-przyszlosc-amerykanskiej-armii?utm_source=rp&utm_medium=teaser_redirect.

komplikuje fakt, że technologie stanowiące podstawę działania broni autonomicznej są obecnie przedmiotem bardzo zaawansowanych prac nad ich zastosowaniem w urządzeniach cywilnych. Mało realne jest wstrzymywanie tych prac decyzjami administracyjnymi.

Dominuje pogląd, że broń autonomiczna musi pozostawać pod kontrolą człowieka, a tym samym, że człowiek ma zachować władzę decyzyjną w przypadku jej użycia. Takie stanowisko zajął w 2018 r. Parlament Europejski[31]. Na początku 2020 r. Izumi Nakamitsu, pełniąca funkcję wysokiego przedstawiciela Narodów Zjednoczonych do spraw rozbrojenia, stwierdziła, że ograniczenie zagrożenia ze strony autonomicznych „zabójczych robotów" należy do jednych z najważniejszych zadań i wymaga przyjęcia w tej sprawie regulacji w prawie międzynarodowym. W czasie rozmów na ten temat uzyskano już poparcie 30 krajów i ponad 140 organizacji pozarządowych[32]. Postęp technologiczny następuje jednak szybciej niż proces wypracowania niezbędnych regulacji międzynarodowych. Sytuacja jest tym trudniejsza, że – podobnie jak w innych kwestiach dotyczących rozwoju technologii cyfrowych – także w tej występują istotne różnice między państwami. Niektóre państwa, np. Belgia i Austria, podjęły już decyzję o zakazie stosowania broni autonomicznej, ale inne, m.in. Wielka Brytania, zajęły w tej sprawie radykalnie odmienne stanowisko. Stosowanie takiej broni dopuszczają, z różnymi zastrzeżeniami, Niemcy i Francja. Należy się spodziewać nacisków na szersze dopuszczenie do używania broni autonomicznej, jako narzędzia pokonującego bariery czasu i odległości oraz umożliwiającego wysyłanie mniejszej liczby żołnierzy w rejon walki[33].

9.4. Państwowi hakerzy ingerujący w świadomość społeczną i włamujący się do urządzeń elektronicznych oraz oprogramowania komputerowego – jako zagrożenie bezpieczeństwa

Rosja, Chiny, Iran i Korea Północna w czołówce państw oskarżanych o wykorzystywanie fałszywych tożsamości do atakowania celów politycznych i infrastrukturalnych w innych krajach • Mechanizmy działania głównych państwowych hakerów ingerujących w świadomość społeczną i włamujących się do urządzeń elektronicznych • Stałe ulepszanie sposobów ingerencji w systemy informacyjne i informatyczne

[31] Rezolucja Parlamentu Europejskiego z dnia 12 września 2018 r. *W sprawie autonomicznych systemów broni* (2018/2752), Dz.U.UE.C.2019.433.86.

[32] https://www.politico.eu/article/top-un-official-its-not-too-late-to-curb-ai-powered-weapons.

[33] https://www.swp-berlin.org/10.18449/2019RP03/#hd-d15993e810.

Służby specjalne USA nie ukrywają, że infrastruktura krytyczna tego państwa jest zagrożona przez ataki – działających pod fałszywymi tożsamościami – operatorów pochodzących głównie z Rosji, Chin, Iranu i Korei Północnej. Jak stwierdził w 2018 r. Michael Moss, zastępca dyrektora Cyber Threat Intelligence Integration Center (CTIIC), amerykańskiego centrum wywiadowczego zajmującego się analizą zagrożeń cybernetycznych, państwa te traktują operacje cybernetyczne jako narzędzie o charakterze strategicznym przeznaczone do ataków na infrastrukturę krytyczną, szczególnie w sektorze energetycznym, handlowym, wodnym i lotniczym[34]. Moss wskazał na zagrożenia szpiegostwem cybernetycznym ze strony Chin i stałe dążenia tego państwa do uzyskania dostępu do zasobów informacji podmiotów działających w sferze obrony, komunikacji oraz przemysłu informatycznego. Oświadczył również, że Iran stale penetruje narzędzia informatyczne w USA i bada ich podatność na oddziaływania destrukcyjne, aby stworzyć sobie podstawy do ewentualnego ataku cybernetycznego. Według tego samego źródła, aktywność hakerów pochodzących z Korei Północnej ma ścisły związek z próbami ograniczenia dolegliwości sankcji gospodarczych nałożonych na ten kraj i ma tworzyć sprzyjające warunki w potencjalnym konflikcie z Koreą Południową. Hakerzy z Korei Północnej mają na swoim koncie m.in. opracowanie i wprowadzenie w 2017 r. do cyberprzestrzeni szkodliwego oprogramowania *ransomware* WannaCry oraz dokonanie w 2016 r. za pomocą narzędzi cybernetycznych kradzieży 81 milionów dolarów z Banku Bangladeszu. Zdaniem amerykańskich służb specjalnych, związane z koreańskimi strukturami władzy grupy hakerów (m.in. Lazarus Group, BlueNorOff i AndAriel) są odpowiedzialne za włamania do międzynarodowych banków i kont klientów w USA, Bangladeszu, Indiach, Meksyku, Pakistanie, na Filipinach, w Korei Południowej, na Tajwanie, w Turcji, Chile i Wietnamie[35]. Jak można się było spodziewać, władze Korei Północnej ostro protestują przeciwko takim oskarżeniom[36].

Obecnie całkiem dobrze są już rozpracowane dotychczasowe mechanizmy działania państwowych hakerów ingerujących w świadomość społeczną i włamujących się do urządzeń elektronicznych oraz oprogramowania komputerowego. Dotyczy to w pierwszej kolejności Rosji, gdzie działania w płaszczyźnie propagandowej są prowadzone przede wszystkim przez Federalną Służbę Bezpieczeństwa (FSB), zaś w zakresie ingerencji w systemy informatyczne przez

---

34 https://www.dni.gov/index.php/ctiic-newsroom/item/1899-statement-for-the-record-mr-michael-moss-for-confirmation-before-the-senate-select-committee-on-crime-and-terrorism-to-be-deputy-director-of-the-cyber-threat-intelligence-integration-center.

35 https://www.reuters.com/article/us-northkorea-usa-sanctions/u-s-imposes-sanctions-on-north-korean-hacking-groups-blamed-for-global-attacks-idUSKCN1VY1RB.

36 https://www.reuters.com/article/us-northkorea-cyber/north-korea-denies-it-amassed-2-billion-through-cyberattacks-on-banks-idUSKCN1VM18K.

Główny Zarząd Wywiadowczy (GRU) Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, oraz Chin, gdzie hakerzy są powiązani przeważnie ze strukturami wojskowymi. Rozmiary państwowej ingerencji w systemy elektroniczne nie są do końca znane. Agresorzy z oczywistych powodów zaprzeczają wszelkim oskarżeniom. Nie powinien także dziwić fakt, że zaatakowani najczęściej bardzo wstrzemięźliwie informują o zaistniałych incydentach.

W Rosji główne zadania związane z internetową agresją propagandową wykonywał dotychczas zespół działający pod nazwą Internet Research Agency. Ta struktura, ulokowana w Petersburgu, popularnie zwana rosyjską farmą trolli, korzystając z usług dobrze opłacanych hakerów świadomości, masowo zasypuje przestrzeń internetową na całym świecie spreparowanymi informacjami i komentarzami oraz podejmuje działania zmierzające do pobudzenia w sieci przyjaznej dyskusji skupionej wokół swoich tez. Rozmiary tej działalności dobrze ilustrują przykłady, które przedstawili w swojej publikacji Peter W. Singer i Emerson T. Brooking. Piszą oni m.in. o podszywającym się pod afroamerykańskiego działacza rosyjskim trollu, którego wpisy na Facebooku były udostępnione w sieci ponad 103 miliony razy. Dają też przykład aktywności rosyjskich trolli w fotograficznym serwisie Instagram, w ramach którego, według badań z 2017 r., treści nadawane z Petersburga z 28 adresów „przyciągnęły 145 milionów lajków, komentarzy i umieszczonych w nich wideo”[37].

Rosji są przypisywane liczne ingerencje w systemy informatyczne innych państw i organizacji. Zadania z tym związane pozostają najczęściej w kompetencji wojskowych służb specjalnych. W trakcie śledztwa prowadzonego w USA w 2018 r. ustalono, że operatorzy z dwóch jednostek rosyjskiego wywiadu wojskowego GRU – jednostki nr 26165, zajmującej się hakowaniem systemu, oraz jednostki nr 74455, zajmującej się rozpowszechnianiem propagandowych informacji – ingerowali w wybory prezydenckie w 2016 r. Punktem wyjścia było uzyskanie ponad 300 haseł, co pozwoliło m.in. obserwować w czasie rzeczywistym działania sztabu Partii Demokratycznej. Następnie przeprowadzono serię skoordynowanych operacji wywierania wpływu, także przy wykorzystaniu globalnej sieci anonimowych serwerów[38].

W niektórych państwach coraz większy niepokój budzą możliwe zagrożenia ze strony rosyjskich grup hakerów powiązanych ze służbami specjalnymi. Już w 2014 r. w raporcie przedstawionym przez firmę McAfee oraz Centrum Studiów Strategicznych i Międzynarodowych z Waszyngtonu podano, że na terenie byłego ZSRR funkcjonuje 20 do 30 globalnych grup mających takie

---

37 P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny…*, s. 159.

38 https://www.politico.com/story/2018/07/13/mueller-indictments-russia-election-hacking-military-intelligence-kremlin-722194. Zob. M. Isikoff, D. Corn, *Rosyjska ruletka. Jak Putin zaatakował Amerykę i wygrał wybory dla Donalda Trumpa*, Warszawa 2018.

zdolności, jakie istnieją „na poziomie państwa narodowego", co oznacza, że mogą podejmować niemal każde działanie cyberprzestępcze[39].

Podejrzenia o zagrożenie ze strony rosyjskich grup hakerskich towarzyszyły m.in. wyborom niemieckim w 2017 r. Wpłynęły na to zarówno echa wyborów amerykańskich w 2016 r., jak i wydarzenia na własnym terenie, zwłaszcza ataki na infrastrukturę informatyczną parlamentu w 2015 r., kiedy to przestał działać system komputerowy Bundestagu. Badająca ten incydent komisja parlamentarna powiązała atak z aktywnością zespołu rosyjskich hakerów (znanego jako grupa APT28, Sofacy lub Fancy Bear) i stwierdziła, że nie jest jasne, co padło ich łupem. Dalsze dochodzenie pozwoliło zebrać dowody potwierdzające udział osób powiązanych z rosyjskimi służbami wojskowymi GRU w tymże ataku, a w 2020 r. rząd niemiecki zażądał oficjalnie od Rosji wydania osoby, którą niemieccy prokuratorzy podejrzewają o jego przeprowadzenie. Na szczeblu Unii Europejskiej podjęto przygotowania do nałożenia sankcji na rosyjskich hakerów[40].

Atak informatyczny na Bundestag nie stanowił odosobnionego incydentu, miały bowiem miejsce inne ataki na krytyczną infrastrukturę komputerową w Niemczech, m.in. wiosną 2016 r. zaatakowano Unię Chrześcijańsko-Demokratyczną (CDU), usiłując dotrzeć do nazw kont i haseł członków partii. W odpowiedzi m.in. w strukturach służb bezpieczeństwa utworzono jednostki reagowania cybernetycznego, przebudowano system serwerów rządowych oraz wzmocniono pozycję Narodowego Centrum Obrony Cybernetycznej[41]. Wszystkie te działania nie były jednak w stanie zapobiec wielkiemu wyciekowi na przełomie 2018 i 2019 r. danych dotyczących różnych środowisk politycznych (oprócz skrajnie prawicowej partii Alternatywa dla Niemiec), w ramach którego zostały ujawnione na Twitterze dokumenty wewnętrzne największych partii i dane osobowe ponad 100 polityków, w tym prywatne dokumenty kanclerz Angeli Merkel. Ale tym razem nie działali rosyjscy hakerzy. Jak się okazało, ten spektakularny atak był dziełem niemieckiego hakera.

Wciąż jednak pojawiają się informacje na temat motywowanych politycznie cyberataków w poszczególnych państwach europejskich, przeprowadzanych – według wszelkiego prawdopodobieństwa – przez operatorów z Rosji. Przykładem może być akcja wymierzona w dziennikarzy i ekspertów Bellingcat, zaangażowanych w ujawnienie sprawców zamachu na byłego agenta GRU Siergieja Skripala, a wcześniej zajmujących się zestrzeleniem pasażerskiego boeinga 777 wykonującego lot numer MH17 nad wschodnią Ukrainą w 2014 r.

---

39 https://www.politico.com/story/2014/06/cybercrime-yearly-costs-107601.

40 https://www.politico.eu/article/europe-reached-its-tipping-point-on-russian-hacking-germany-bundestag-cyberattack.

41 https://www.politico.eu/article/germanys-cyber-security-chief-on-hacking-russia-and-problem; https://www.politico.eu/article/hacked-information-bomb-under-germanys-election.

O akcji tej poinformowało w 2019 r. kierownictwo ProtonMail, szwajcarskiego serwisu poczty elektronicznej[42]. W 2019 r. opublikowano wyniki śledztwa prowadzonego przez specjalny zespół Google'a i organizacji FireEye (zajmującej się przestępstwami cybernetycznymi), które potwierdziły wcześniejsze podejrzenia o zaatakowanie przez hakerów pracujących dla rosyjskich służb specjalnych sztabu wyborczego Emmanuela Macrona w czasie kampanii wyborczej we Francji w 2017 r. Autorzy raportu ustalili, że akcja dezinformacyjna została w tym przypadku przeprowadzona za pomocą spersonalizowanych ataków (*spear phishing*)[43]. Podejrzana rosyjska kampania dezinformacyjna została wykryta przed wyborami parlamentarnymi w Wielkiej Brytanii w 2019 r. Według informacji firmy Reddit zajmującej się mediami społecznościowymi, w tej kampanii upowszechniono w internecie poufny dokument brytyjskiego rządu związany z wcześniejszymi działaniami dezinformacyjnymi, co wyraźnie przyczyniło się do zaostrzenia i tak już trudnej sytuacji politycznej w Wielkiej Brytanii. W tym samym czasie ujawniono też dokumenty pokazujące relacje brytyjsko-amerykańskie w – istotnych dla nastrojów politycznych w okresie poprzedzającym wybory – kwestiach ochrony zdrowia. W obu przypadkach wykorzystano media społecznościowe do swoistej „wtórnej infekcji" w ramach akcji wielokrotnego powielania tych dokumentów w przestrzeni internetowej[44].

W Chinach przestrzeń internetowa była wykorzystywana pierwotnie przede wszystkim do uprawiania szpiegostwa przemysłowego i militarnego oraz do kradzieży na wielką skalę własności intelektualnej. P.W. Singer nazwał w 2014 r. w swojej analizie działania szpiegowskie państwa chińskiego w internecie największą kradzieżą w historii ludzkości[45]. Aktywność hakerów związanych z państwem chińskim jest wymierzona nie tylko przeciwko innym państwom, lecz także przeciwko konkurencyjnym firmom internetowym. W latach 2014–2017 przypadki hakowania z adresów chińskich stwierdzono m.in. w Ericssonie, szwedzkiej firmie produkującej sprzęt telekomunikacyjny. Po szczegółowej analizie okazało się, że zaatakowanych zostało pięciu z dziesięciu największych dostawców usług technologicznych na świecie, co w efekcie pozwoliło dotrzeć do zasobów strategicznych podmiotów przez nie obsługiwanych, w tym amerykańskich stoczni wojskowych budujących okręty podwodne z napędem jądrowym. Najbardziej aktywna w tej działalności okazała się grupa należąca do systemu APT10 (Advanced Persistent Threat 10) monitorowanego w sposób

---

42 https://tvn24bis.pl/ze-swiata,75/protonmail-poinformowal-o-ataku-phishingowym-na-bellingcat,956622.html.

43 https://wiadomosci.onet.pl/swiat/francja-wywiad-wojskowy-rosji-wykradl-dane-ze-sztabu-emmanuela-macrona/zgnlxf4.

44 https://www.politico.eu/article/reddit-suspected-russian-disinformation-campaign-ahead-of-uk-election.

45 https://etbrooking.com.

niejawny przez chińskie Ministerstwo Bezpieczeństwa Państwowego i powiązanego z jednostką wojskową 61398 zajmującą się włamaniami informatycznymi[46].

Obecnie państwo chińskie wyraźnie wzmogło działania polegające na wykorzystywaniu narzędzi internetowych do upowszechniania na świecie określonej narracji osnutej wokół zagadnień strategicznych. Przykładowo, jak już sygnalizowałem, w połowie 2019 r. Twitter i Facebook poinformowały, że powstrzymały wspieraną przez chiński rząd kampanię w mediach społecznościowych, której autorzy pochodzili z Chin, a której celem było osłabianie protestów w Hongkongu[47]. W 2020 r. istotnym elementem narracji chińskiej w internecie stały się kwestie dotyczące źródeł i przebiegu pandemii koronawirusa. Bliższe analizy pokazują, że państwo chińskie w swojej działalności propagandowej korzysta nawet z takich – pozornie neutralnych – narzędzi internetowych, jak TikTok, aplikacja społecznościowa przeznaczona do udostępniania samodzielnie nagranych, krótkich materiałów, m.in. wideoklipów, popularna zwłaszcza wśród ludzi młodych, pobierana na całym świecie, w tym w Stanach Zjednoczonych. Aplikacja ta powstała w 2016 r. w chińskiej firmie ByteDance, której wartość szacowano w 2019 r. na 75 miliardów dolarów[48], i należy do najczęściej pobieranych w sklepie iOS. Tylko w pierwszym kwartale 2019 r. użytkownicy Google Play pobrali ze sklepu Apple iOS ponad 220 milionów tej aplikacji[49]. TikTok jest wskazywany ostatnio jako trzecia najpopularniejsza aplikacja na świecie, która stała się bardzo ważnym elementem kultury internetowej i sposobem komunikacji dla pokolenia Z. Przez kilka lat, które minęły od utworzenia tej aplikacji, została ona pobrana przez internautów ponad 2 miliardy razy. Z pewnością dla władz chińskich było – i jest – istotne utrzymanie kontroli nad treściami rozpowszechnianymi w tak masowej skali. Jak się okazało, TikTok został poddany cenzurze (głównie chodzi o blokowanie filmików o tematyce politycznej, np. ukazujących antyrządowe protesty w Hongkongu czy chińskie represje wobec Ujgurów) i służy wspieraniu chińskiej polityki zagranicznej[50]. W 2019 r. dowództwo Marynarki Wojennej Stanów Zjednoczonych uznało, że aplikacja TikTok stanowi

---

46 https://www.reuters.com/article/us-china-cyber-cloudhopper-special-repor/special-report-inside-the-wests-failed-fight-against-chinas-cloud-hopper-hackers-idUSKCN1TR1DK; https://www.reuters.com/article/us-britain-election-foreign/leak-of-classified-papers-ahead-of-uk-election-tied-to-russian-operation-reddit-idUSKBN1YA2IQ.

47 https://www.rp.pl/Nowe-technologie/190829998-Twitter-i-Facebook-Kampania-Chin-wymierzona-w-Hongkong.html; https://content.fireeye.com/apt-41/rpt-apt41.

48 P. Januszewska, *15 sekund do sławy*, „Newsweek" 2019, nr 5, wydanie specjalne pt. *Technoczłowiek. Przewodnik po cyberświecie*, s. 112; https://www.theguardian.com/news/audio/2019/dec/30/the-strange-world-of-tiktok-a-look-back.

49 https://www.politico.com/magazine/story/2019/11/02/the-trouble-with-tiktok-229890.

50 https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.

zagrożenie dla cyberbezpieczeństwa, i zakazało jej używania na rządowych urządzeniach mobilnych[51]. W połowie 2020 r. prezydent Donald Trump wydał zakaz korzystania w USA z aplikacji TikTok, powołując się na to, że zagraża ona bezpieczeństwu narodowemu, polityce zagranicznej i gospodarce Stanów Zjednoczonych. Ta decyzja, będąca elementem wojny technologicznej między USA i Chinami, dotyczyła też innej popularnej aplikacji do przesyłania danych pochodzącej z Chin: WeChat. Działania władz amerykańskich mają na celu usunięcie z internetu w USA chińskich narzędzi telekomunikacyjnych, aplikacji oraz usług w chmurze[52]. We wrześniu 2020 r. prezydent Trump zaostrzył jeszcze swoje stanowisko i polecił zablokować na terenie Stanów Zjednoczonych działanie kilku chińskich aplikacji, w tym TikTok[53].

Rozpoznanie domen, kanałów i mechanizmów dotychczasowych agresywnych działań państw w cyberprzestrzeni prowadzi niejednokrotnie do zablokowania jakichś działań, jednak nie rozwiązuje sprawy systemowo. Stale są bowiem ulepszane sposoby ingerencji informacyjnej i informatycznej, trwa konkurencja pod nazwą „Kto kogo?" (potocznie mówiąc: ogra). Ogólny kierunek zmian wyznacza w tym zakresie: dekoncentracja adresów, z których są nadawane określone treści i impulsy elektroniczne; tworzenie siatek zainfekowanych routerów „śpiochów", które w przyszłości mogłyby być wykorzystane przez hakerów do rozpoczęcia ofensywnych działań cybernetycznych; operowanie informacjami prawdziwymi umiejętnie wymieszanymi z treściami fałszywymi; odwoływanie się w przekazie propagandowym do argumentów i sytuacji o charakterze lokalnym, co ma potwierdzić wiarygodność tego przekazu. Do przeciwdziałania nowym tendencjom i praktykom dezinformacyjnym konieczne są ciągłe i systemowe analizy oraz odpowiednie zasoby ludzkie. Dziennikarze jednego z komercyjnych kanałów telewizji w Polsce w swoim raporcie zwracają uwagę na kilka nowych sposobów dezinformacji, takich jak posługiwanie się spreparowanymi dokumentami, podszywanie się pod znanych polityków oraz tworzenie równolegle w różnych językach sieci powiązanych kont i stron internetowych. Akt dezinformacji zazwyczaj obejmuje umieszczenie w internecie fałszywej informacji, powielanie jej w różnych językach za pomocą licznych kont stworzonych niejednokrotnie specjalnie na potrzeby tego procederu, promowanie treści dezinformacyjnych na Facebooku[54].

---

51 https://www.theguardian.com/technology/2019/dec/21/us-navy-bans-tiktok-from-mobile-devices-saying-its-a-cybersecurity-threat.

52 https://www.reuters.com/article/us-usa-china-apps-pompeo-breakingviews/breakingviews-pompeos-chinese-web-wall-is-a-tall-order-idUSKCN2520KG; https://www.politico.com/news/2020/08/07/tiktok-trump-executive-order-392558.

53 https://cyfrowa.rp.pl/globalne-interesy/52008-kolejny-zwrot-akcji-w-sprawie-tiktoka-zaskakujacy-ruch-chinczykow?utm_source=rp&utm_medium=teaser_redirect.

54 https://konkret24.tvn24.pl/swiat,109/operacja-wtorna-infekcja-analitycy-demaskuja-nowe-strategie-dezinformacyjne,952575.html.

Programując działania w sferze rządzenia, dane państwo nie może (a na pewno nie powinno) liczyć na to, że inne państwa będą się powstrzymywały od prób wykorzystywania internetu do dezinformacji i narzucania swojej narracji politycznej. Takie ofensywne – i zarazem agresywne – poczynania prowadzą bowiem w dużej mierze do osiągnięcia założonych celów. Potwierdzają to badania wykonane w 2019 r. przez zespoły naukowców z Oksfordu i uniwersytetu w Amsterdamie dotyczące skuteczności narzucania tematów i klimatu dyskusji internetowej przez rosyjską inwazję propagandową w czasie kampanii wyborczej w USA w 2018 r. Z badań przeprowadzonych przy użyciu specjalnie dobranych metod obliczeniowych wynikało, że treści ostro polaryzujące opinię publiczną, które dominowały w przekazie internetowych trolli w ciągu trzech do dziesięciu dni, górowały następnie nad całą dyskusją w internecie[55].

Nie tylko Rosja i Chiny wykorzystują do realizacji swoich planów politycznych, gospodarczych i militarnych różnorodne mechanizmy infekowania treści i rozwiązań systemowych w komunikacji elektronicznej. Według ustaleń poczynionych w ramach Computational Propaganda Research Project na Uniwersytecie Oksfordzkim, które przytoczyli w swojej publikacji Singer i Brooking, co najmniej dwadzieścia dziewięć państw postępuje podobnie, aby „sterować opinią publiczną, rozpowszechniać dezinformację i osłabiać krytyków". Zgodnie z tymi samymi ustaleniami badawczymi, tylko w 2017 r. wybory krajowe w co najmniej osiemnastu państwach stały się przedmiotem takich działań[56].

Same korporacje internetowe dostrzegają, że ich produkty są wykorzystywane do prowadzenia zmasowanych państwowych akcji dezinformacyjnych. Przykładowo w 2019 r. Facebook poinformował o skoordynowanych i nieautentycznych działaniach osób powiązanych z władzami Arabii Saudyjskiej, które były prowadzone z 350 zamkniętych przez korporację kont i stron śledzonych przez ponad 1,4 miliona osób[57].

9.5. Cyberprzestępczość jako wyzwanie dla rządzenia

• Internet jako obszar działań przestępczych • Rosnące koszty generowane przez cyberprzestępczość • Zamazywanie się granic między internetową działalnością przestępczą motywowaną finansowo a cybernetyczną agresją polityczną

55 https://euvsdisinfo.eu/figures-of-the-week-3-10.

56 P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny…*, s. 162.

57 https://www.dobreprogramy.pl/Facebook-staje-sie-tuba-propagandowa-dla-rzadow.-Firma-samabije-na-alarm,News,103052.html.

Zasadniczym wyzwaniem w walce o zagwarantowanie bezpieczeństwa staje się fakt, że przestępczość przenosi się do internetu. Popełniane są tam przestępstwa polegające na kradzieży tożsamości poszczególnych ludzi i instytucji, wykradaniu danych i ingerowaniu w treść dokumentów internetowych[58]. Mnożą się przypadki blokowania urządzeń teleinformatycznych połączonego z wymuszaniem opłat za przywrócenie sprawności tych urządzeń. Terroryści i grupy przestępcze korzystają z internetu, aby rekrutować, organizować i aktywizować swoich zwolenników, szerzyć swoją ideologię, zbierać fundusze, pozyskiwać informacje wywiadowcze oraz koordynować działania[59]. Biorąc pod uwagę cele, skalę i skutki przestępstw w internecie, a także uwzględniając fakt, że różne dziedziny życia oraz funkcjonowania struktur społecznych i instytucji publicznych są coraz bardziej uzależnione od systemów komunikacji internetowej, tak przecież podatnej na bezprawne ingerencje, trzeba nadawać najwyższą rangę zagadnieniom przeciwdziałania cyberprzestępczości.

Sprawcy przestępstw o charakterze terrorystycznym zmierzają do możliwie szybkiego poinformowania dużej liczby ludzi o swych „dokonaniach". Szerzenie strachu jest bowiem nieodłącznym elementem – i w dużym stopniu również założeniem – działań terrorystycznych. Przykład ataków w 2019 r. na meczety w Christchurch w Nowej Zelandii, które sprawca transmitował na żywo na Facebooku w trwającej 17 minut relacji, wskazuje, że internet może być – i jest – z powodzeniem wykorzystywany do nagłaśniania zamachów terrorystycznych. Masakrę, w której zginęło ponad 50 osób, w ciągu 24 godzin obejrzały miliony osób. Zdarzenie to – podobnie jak wiele innych – niezbicie dowodzi ogromnego znaczenia regulacji przeciwdziałających dystrybucji materiałów propagujących terroryzm w internecie i pozwalających ustalić tożsamość ich autorów.

Cyberprzestępczość generuje coraz większe koszty. Jak w 2014 r. szacowano w raporcie McAfee i waszyngtońskiego Centrum Badań Strategicznych i Międzynarodowych, straty finansowe dla światowej gospodarki wynikające z działalności cyberprzestępców wynosiły 575 miliardów dolarów rocznie, w tym dla gospodarki USA – około 100 miliardów dolarów. Największe koszty były związane z kradzieżą tajemnic handlowych i własności intelektualnej, blokowaniem urządzeń i sieci oraz różnymi przestępstwami finansowymi[60]. Eksperci oceniają, że w 2020 r. koszty cyberprzestępczości mogą wzrosnąć do

---

58 T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny*, Warszawa 2013.

59 Zob.: M. Skibińska, D. Siemieniecka, K. Majewska, *Cyberagresja. Zjawisko, skutki, zapobieganie*, Toruń 2020; A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm…*; K. Wiak, A. Podraza, P. Potakowski (red.), *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa 2013; J. Kowalewski, M. Kowalewski, *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*, Warszawa 2017.

60 https://www.politico.com/story/2014/06/cybercrime-yearly-costs-107601.

2 bilionów dolarów[61]. Do rozwoju cyberprzestępczości w 2020 r. przyczyniło się masowe przenoszenie do internetu różnych form aktywności, w ramach tzw. pracy zdalnej, związane z blokadami fizycznych kontaktów w warunkach pandemii koronawirusa. Ułatwieniem dla cyberprzestępców były ograniczone kompetencje informatyczne i mała świadomość zagrożeń ze strony nowych użytkowników internetu.

Jak zauważył w 2018 r. w swojej informacji na temat zagrożeń w cyberprzestrzeni – wspomniany już wyżej – Michael Moss, przestępczość cybernetyczna podmiotów niepaństwowych ma przede wszystkim charakter finansowy i jest ukierunkowana na osiągnięcie zysku, ale równocześnie trzeba się liczyć z tym, że w tej dziedzinie „granica między działalnością przestępczą i państwową stanie się coraz bardziej zamazana, ponieważ państwa postrzegają narzędzia cyberprzestępcze jako stosunkowo niedrogie i dające się ukryć środki umożliwiające ich działanie”[62].

Zjawisko nakładania się internetowej działalności przestępczej mającej na celu pozyskiwanie środków finansowych i aktywności służącej realizacji interesów państwowych można obserwować na przykładzie chińskiej grupy hakerskiej APT41. Według raportu opublikowanego w 2019 r. przez firmę FireEye, ta działająca od 2012 r. grupa hakuje za pomocą szkodliwego oprogramowania gry wideo, aby zarabiać pieniądze, a równocześnie tworzy przyczółki działań szpiegowskich przy wykorzystaniu zainfekowanego sprzętu. Ślady jej działalności wykryto w ciągu siedmiu lat w 14 krajach (Francji, Indiach, Włoszech, Japonii, Birmie, Holandii, Singapurze, Korei Południowej, Afryce Południowej, Szwajcarii, Tajlandii, Turcji, Wielkiej Brytanii i Stanach Zjednoczonych) w dziedzinach związanych z chińskimi interesami politycznymi i gospodarczymi, w tym w sektorze opieki zdrowotnej, zaawansowanych technologii, mediów, farmaceutyki, telekomunikacji i edukacji. Autorzy wspomnianego raportu podkreślają, że w przypadku aktywności grupy APT41 istnieje niewyraźna granica między wspieraniem władz państwowych i przestępczością[63].

Szukając dróg dojścia w internecie do możliwie wielu potencjalnych klientów, platformy komunikacyjne nie zapominają o ciemnej stronie człowieka i adresują swoją ofertę również do ludzi mających – nazwijmy to oględnie – niestandardowe potrzeby. Obcowanie w świecie wirtualnym z najróżniejszymi patologiami, w tym z agresją i przemocą, sprawia, że te groźne zjawiska łatwiej się szerzą w świecie realnym, a co najmniej przyczynia się do zobojętnienia

---

61 https://www.iso.org/news/ref2360.html.

62 https://www.dni.gov/index.php/ctiic-newsroom/item/1899-statement-for-the-record-mr-michael-moss-for-confirmation-before-the-senate-select-committee-on-crime-and-terrorism-to-be-deputy-director-of-the-cyber-threat-intelligence-integration-center.

63 https://www.theguardian.com/technology/2019/aug/08/chinese-cyberhackers-blurring-line-between-state-power-and.

na ich występowanie. Funkcjonowanie darknetu, czyli ukrytej (ciemnej) sieci internetowej, której użytkownicy – trudniej identyfikowalni – wyrażają bez zahamowań swoje postawy i pragnienia, jest wykorzystywane do tworzenia różnych przestępczych wspólnot elektronicznych. Za pomocą tej sieci jest prowadzony obrót bronią, materiałami wybuchowymi, narkotykami, odbywa się też kontraktowanie usług płatnych przestępców i kontaktowanie się osób o zaburzonych preferencjach seksualnych[64]. Nie da się łatwo rozwiązać problemu ograniczania zjawisk patologicznych w sieci. Okazuje się bowiem, że bardziej „proaktywne" podejście Facebooka do wykrywania problematycznych treści w zamkniętych grupach, którego celem ma być uczynienie aktywności tych grup przejrzystszą oraz usuwanie z przestrzeni komunikacji publicznej treści szkodliwych, może w praktyce prowadzić do głębszego zakonspirowania tych treści w ramach zamkniętych wspólnot internautów. Utrudni to wykrywanie przez podmioty zewnętrzne naruszeń standardów w komunikacji w tym segmencie internetu[65].

9.6. Rozwój technologii cyfrowych jako przesłanka zmian w systemach bezpieczeństwa

Proces tworzenia wyspecjalizowanych instytucji odpowiedzialnych za przeciwdziałanie zagrożeniom cybernetycznym • Wykorzystanie narzędzi sztucznej inteligencji w walce z zagrożeniami bezpieczeństwa

Zapewnienie cyberbezpieczeństwa stało się jednym z kluczowych zadań wszystkich państw. Dotyczy to także państw europejskich, w których są wypracowywane specjalne rozwiązania systemowe służące wykonywaniu tych zadań[66]. Dość powszechnie, chociaż nie zawsze w sposób otwarty, przyjmuje się, że: „Skuteczna obrona – nie tylko w ujęciu cybernetycznym – wymaga posiadania również środków ofensywnych, umożliwiających zarówno prowadzenie aktywnych działań obronnych, jak i przeprowadzenie kontruderzenia lub – jak kto woli – odwetowego «zhakowania» systemów przeciwnika, a w razie konieczności również przeprowadzenie wyprzedzającego ataku cybernetycznego"[67].

---

64 Zob. E. Ormsby, *Darknet*, Kraków 2019; N. Bilton, *Król darknetu. Polowanie na genialnego cyberprzestępcę*, Sękowa 2020.

65 https://www.theguardian.com/technology/2019/aug/14/facebook-private-groups-rules-extremist-fake-news.

66 Zob. P. Mickiewicz, *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, nr 1, s. 65 i nast.

67 W. Goździewicz, *Cyberobrona i nie tylko. Rola wojska w budowaniu ekosystemu cyberbezpieczeństwa w kraju*, w: W. Goździewicz i in., *Bezpieczeństwo poprzez innowacje. Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego*, Kraków 2017, s. 20.

Wyzwania związane z rozwojem technologii cyfrowych stały się impulsem do wprowadzania istotnych zmian w siłach zbrojnych poszczególnych państw oraz w rozwiązaniach instytucjonalnych i procedurach systemu bezpieczeństwa. Podejmowane są działania zmierzające do uodpornienia na zagrożenia atakiem cybernetycznym systemów dowodzenia, baz danych, technik przetwarzania i dystrybucji danych, identyfikacji obiektów nieprzyjaciela i funkcjonowania mechanizmów współpracy sojuszniczej oraz do podjęcia, jeśli zajdzie taka potrzeba, działań ofensywnych w cyberprzestrzeni. Z danych wywiadowczych wynika, że w państwach, które wpisały wykorzystanie operacji cybernetycznych do planów strategicznych, w strukturach wojska są tworzone jednostki przeznaczone do wspomagania lub prowadzenia takich operacji. Źródła amerykańskie wskazują w tym kontekście m.in. na integrację od 2015 r. narzędzi cybernetycznego ataku i wywiadu wojskowego w Chinach[68].

W instytucjach państwowych, w tym bardzo często w ramach służb specjalnych, powstają wyspecjalizowane podmioty odpowiedzialne za przeciwdziałanie zagrożeniom cybernetycznym. Obok instytucji o charakterze operacyjnym, których zadaniem jest ochrona sieci i reagowanie w przypadku incydentów – lub prób – naruszenia bezpieczeństwa sieci, coraz częściej rozbudowuje się specjalne struktury odpowiedzialne za analityczną koordynację informacji o atakach i zagrożeniach cybernetycznych oraz tendencjach w ich występowaniu. Odnosi się to do monitorowania i analizy zarówno destrukcyjnych oddziaływań w komunikacji internetowej, jak i zakłóceń w funkcjonowaniu urządzeń i sieci informatycznych. Umacnia się bowiem przekonanie, że w obecnych warunkach zasadniczym zadaniem państwa i jego służb specjalnych staje się rozpoznanie oraz zrozumienie strategii i taktyki potencjalnych agresorów, gotowych do przeprowadzenia ataków w cyberprzestrzeni.

Przykładowo w USA zadania związane z informacjami o destrukcyjnych działaniach w cyberprzestrzeni wykonuje funkcjonujące w strukturze Wspólnoty Wywiadowczej od 2016 r. – wspomniane już wyżej – centrum wywiadowcze (CTIIC). Misją tej instytucji jest rozpoznawanie zagranicznych zagrożeń cybernetycznych oraz wspomaganie w tej dziedzinie innych podmiotów federalnych i stanowych, m.in. przez koordynację i analizę informacji wojska, wywiadu, organów bezpieczeństwa wewnętrznego i ścigania oraz wymiaru sprawiedliwości. W CTIIC pracują analitycy pochodzący z wszystkich innych podmiotów biorących udział w zwalczaniu zagrożeń cybernetycznych, w tym przede wszystkim z Departamentu Bezpieczeństwa Krajowego (DHS), Biura Dyrektora Wywiadu Narodowego (ODNI), Agencji Wywiadu Obronnego (DIA),

[68] https://www.dni.gov/index.php/ctiic-newsroom/item/1899-statement-for-the-record-mr-michael-moss-for-confirmation-before-the-senate-select-committee-on-crime-and-terrorism-to-be-deputy-director-of-the-cyber-threat-intelligence-integration-center.

Agencji Bezpieczeństwa Narodowego (NSA), Federalnego Biura Śledczego (FBI), Centralnej Agencji Wywiadowczej (CIA) oraz Departamentu Energii[69].

W Niemczech w przyjętej w 2011 r. strategii bezpieczeństwa cybernetycznego rząd określił przeciwdziałanie atakom cybernetycznym jako zadanie o największym znaczeniu. Odrębnie wskazano na ataki o podłożu kryminalnym, terrorystycznym i wywiadowczym oraz ataki cybernetyczne na sieci informatyczne administracji federalnej, które mogą zagrozić krytycznej infrastrukturze informatycznej państwa. Utworzono Narodowe Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni, którego zadaniem jest koordynowanie działań wszystkich struktur rządowych zajmujących się problemem cyberbezpieczeństwa. Wypracowano także mechanizmy współdziałania w sprawach cyberbezpieczeństwa podmiotów publicznych i prywatnych[70].

W pochodzącej z 2017 r. strategii cyberbezpieczeństwa Wielkiej Brytanii założono aktywną rolę państwa w zapewnieniu ochrony przed zagrożeniami w cyberprzestrzeni. Tym samym odstąpiono od wcześniejszego modelu, w którym kluczową rolę w tym zakresie odgrywały podmioty prywatne. Zgodnie z nowymi rozwiązaniami, partnerstwo publiczno-prywatne ma stanowić tylko dopełnienie systemu państwowego, na którego funkcjonowanie w ciągu 5 lat mają być wydatkowane prawie 2 miliardy funtów. W celu koordynowania działań państwa powołano Narodowe Centrum Cyberbezpieczeństwa (NCSC). Kwestie cyberbezpieczeństwa połączono z programem rozwoju zdolności cyfrowych państwa i społeczeństwa[71].

W walce z zagrożeniami bezpieczeństwa, w tym zagrożeniami związanymi z rozwojem cywilizacji cyfrowej, wykorzystuje się coraz częściej narzędzia sztucznej inteligencji. Stają się one jednym z głównych instrumentów służb specjalnych, m.in. służb wywiadowczych. Przykładowo, w strategii służb wywiadu amerykańskiego z 2019 r. (określonej jako AIM Initiative)[72] przyjęto, że zadaniem narzędzi sztucznej inteligencji jest analizowanie danych, łączenie różnych zestawów danych, wybór odpowiedniego kontekstu danych, wnioskowanie znaczenia z danych i ostatecznie dokonywanie ocen analitycznych na

---

69 https://www.dni.gov/index.php/ctiic-what-we-do; https://www.dni.gov/index.php/ctiic-newsroom/item/1899-statement-for-the-record-mr-michael-moss-for-confirmation-before-the-senate-select-committee-on-crime-and-terrorism-to-be-deputy-director-of-the-cyber-threat-intelligence-integration-center.

70 K. Sacewicz, *Niemiecka strategia ochrony cyberprzestrzeni*, Agencja Bezpieczeństwa Wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7, s. 129 i nast.

71 https://www.cyberdefence24.pl/wielka-brytania-nowa-strategia-cyberbezpieczenstwa-zmiana-czy-kontynuacja; file:///C:/Users/UW/Downloads/systemowe_wsparcie_dla_cyfryzacji_gospodarki_-_przyklad_wielkiej_brytani.pdf.

72 *The AIM Initiative: A Strategy for Augmenting Intelligence using Machines*, https://www.dni.gov/index.php/newsroom/reports-publications/item/1940-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines.

podstawie wszystkich dostępnych danych. Uznano, że tempo, w jakim dane są generowane, przekroczyło zbiorową zdolność do ich wyszukania i zrozumienia. W tych warunkach wskazano technologie AIM AAA (Artificial intelligence, process Automation, IC officer Augmentation) jako kluczowy element transformacyjny w działaniu służb wywiadowczych[73]. W tej dziedzinie korzysta się także z partnerstwa publiczno-prywatnego. Przykładowo, celem zwiększenia koordynacji w zakresie analizy dużych zbiorów danych, które są istotne dla amerykańskiego wywiadu skupiającego kilkanaście różnych agencji, wykorzystuje się, poczynając od 2013 r., możliwości wynikające z potencjału chmury elektronicznej (C2S) udostępnionej przez komercyjnego dostawcę[74].

9.7. Problemy cywilizacji cyfrowej w strategiach i praktyce działania w sferze bezpieczeństwa w Polsce

Potwierdzenie ogólnych tendencji w zakresie zagrożeń informatycznych, cyberprzestępczości oraz bezpieczeństwa informacyjnego • Podstawowe kategorie przestępstw w cyberprzestrzeni rejestrowanych w Polsce • Strategia Cyberbezpieczeństwa RP na lata 2019–2024 • System cyberbezpieczeństwa w Polsce • Projekty ujęcia kwestii bezpieczeństwa informacyjnego w Polsce • Strategia Bezpieczeństwa Narodowego z 2020 r.

W Polsce znajdują odbicie światowe tendencje w zakresie zagrożeń informatycznych, cyberprzestępczości i bezpieczeństwa informacyjnego. Problemy związane z rozwojem cywilizacji cyfrowej zajmują coraz więcej miejsca w strategiach bezpieczeństwa. W kraju powstał system cyberbezpieczeństwa[75], podejmuje się też próby stworzenia mechanizmów bezpieczeństwa informacyjnego, jednak w tym przypadku nie ma jeszcze całościowych rozwiązań systemowych. Z uwagi na nieskuteczność działań w sprawach cyberbezpieczeństwa podejmowanych w granicach jednego państwa, tworzone są systemowe mechanizmy współpracy w tej dziedzinie na forum międzynarodowym.

Jak wynika z danych udostępnionych przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV)[76], w 2018 r. odnotowano 31 865 zgłoszeń incydentów komputerowych w sieciach znajdujących się

---

[73] https://www.dni.gov/index.php/newsroom/reports-publications/item/1940-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines.

[74] https://www.dni.gov/index.php/newsroom/news-articles/item/2007-top-u-s-intelligence-official-says-cloud-one-of-best-decisions-we-made.

[75] I. Oleksiewicz, *Transformacja polityki cyberbezpieczeństwa RP w XXI wieku*, Warszawa 2020.

[76] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku*, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, kwiecień 2019 r., https://www.csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi. Zespół nazwą nawiązuje do podobnych jednostek tworzonych

w obszarze kompetencyjnym Zespołu (w 2017 r. takich zgłoszeń było 28 281). Po weryfikacji danych i wyeliminowaniu tych samych incydentów ustalono, że faktyczne naruszenie bezpieczeństwa teleinformatycznego miało miejsce w 6236 przypadkach (w 2017 r. – 5819). Przeważnie chodziło tu o zainfekowanie wirusami, błędną konfigurację, nieuprawnione skanowanie, *botnet*, *phishing*, spowodowanie niedostępności. Równocześnie w ramach ARAKIS 3.0 GOV[77] – systemu wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią internetu – na 319 943 424 zarejestrowane przepływy, 454 207 zakwalifikowano do kategorii alarmów, z których 62 365 alarmów miało pilny priorytet i wymagało natychmiastowej reakcji, gdyż niosło duże ryzyko przełamania zabezpieczeń. Najczęściej były to ataki na usługę Secure Shell (SSH) zapewniającą zdalny dostęp do danego zasobu teleinformatycznego. Najczęstszym zaś sposobem przełamania zabezpieczeń są ataki słownikowe zbliżone do metody *brute-force*. Warto tutaj zaznaczyć, że w 2018 r. aż 22% wszystkich odnotowanych przepływów pochodziło z Chin, a 13% z Rosji.

Zgodnie z raportem Ministerstwa Spraw Wewnętrznych i Administracji o stanie bezpieczeństwa w Polsce za 2016 r. (to ostatni dostępny raport)[78], stałą tendencją jest wzrost liczby ujawnionych przestępstw w cyberprzestrzeni. Jak wskazano w tym raporcie, sprawcy przestępstw coraz częściej wykorzystują specjalne oprogramowanie umożliwiające kamuflowanie miejsca, z którego operują w internecie. Odnotowano też, że poza atakami wymierzonymi w funkcjonowanie systemów teleinformatycznych, w cyberprzestrzeni mają miejsce tradycyjne przestępstwa – popełniane jednak za pomocą nowych narzędzi.

W cyberprzestrzeni dochodzi do różnego typu przestępstw. Są to m.in.: oszustwa, przestępstwa z wykorzystaniem elektronicznych instrumentów płatniczych, pedofilia i pornografia dziecięca, przestępstwa na szkodę właścicieli dóbr intelektualnych, nielegalny handel towarami licencjonowanymi, nielegalny handel towarami akcyzowymi, handel przedmiotami pochodzącymi z przestępstw i obrót dobrami dziedzictwa narodowego, handel ludźmi i narządami ludzkimi, wymuszenia i groźby karalne, nieuprawnione uzyskiwanie informacji (*hacking*), podsłuch komputerowy (*sniffing*), udaremnianie dostępu do informacji przez zaszyfrowanie danych i żądanie otrzymania określonej sumy pieniędzy za ich ponowne udostępnienie (*ransomware*), przełamywanie zabezpieczeń komputerowych, wprowadzanie złośliwego oprogramowania, nielegalny hazard.

---

przez rządy na całym świecie (CSIRT jest akronimem angielskiej nazwy Computer Security Incident Response Team).

77 ARAKIS jest akronimem nazwy: AgRegacja, Analiza i Klasyfikacja Incydentów Sieciowych.

78 https://archiwumbip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html.

Wśród podstawowych zagrożeń, które pozostają w zasięgu zainteresowań Agencji Bezpieczeństwa Wewnętrznego, w 2016 r. odnotowano: szpiegostwo komputerowe (w tym wykradanie istotnych danych prywatnych, m.in. kradzież tożsamości, oraz działania mające znamiona szpiegostwa przemysłowego i wywiadowczego); wykorzystywanie internetu przez ekstremistyczne środowiska polityczne, organizacje terrorystyczne oraz obce służby specjalne w celu dezinformacji, propagowania skrajnych poglądów i zachęcania do udziału w organizowanych przez nie przedsięwzięciach; działania o charakterze cybernetycznej wojny dezinformacyjnej (obejmujące masową dystrybucję fałszywych informacji); cyberataki mające na celu zastraszenie lub wymuszenie spełnienia pewnych żądań.

Szczególne zagrożenia cyberprzestrzeni stwarzają ataki o znacznym stopniu zaawansowania informatycznego skierowane przeciwko sieciom i systemom teleinformatycznym państwa. Ich zadaniem jest pozyskiwanie wrażliwej wiedzy z systemów i sieci teleinformatycznych (np. uczelni oraz agend rządowych i podmiotów infrastruktury krytycznej)[79]. Do równie dużych zagrożeń należy zaliczyć: działania propagandowe, działania paraliżujące infrastrukturę krytyczną (głównie ataki DDoS), prowadzenie inwigilacji krytycznych sieci za pomocą złośliwego oprogramowania.

W omawianym raporcie MSWiA mówi się także o działalności grup internetowych zwanej haktywizmem, wykorzystywaniu internetu jako narzędzia szantaży i wyłudzeń, działaniach werbunkowych prowadzonych przez organizacje terrorystyczne. Nie ulega wątpliwości, że wszystkie te zagrożenia muszą podlegać ścisłemu monitorowaniu.

Poczynając od pierwszej dekady XXI wieku, problemy wiążące się z rozwojem cywilizacji cyfrowej zajmują w Polsce coraz więcej miejsca w kolejnych strategiach bezpieczeństwa. Zaczęto je rozpatrywać nie tylko w związku z systemami łączności, lecz także jako samoistny element bezpieczeństwa. Toruje też sobie drogę pogląd, że narzędzia cybernetyczne powinny być śmielej i na większą skalę wykorzystywane przez instytucje państwa.

W Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2007 r.[80] ustalono zadania w zakresie informatyzacji w Polsce związane z powszechną implementacją rozwiązań, które miały podnieść stan techniczny systemów i sieci teleinformatycznych oraz jakość świadczenia usług drogą elektroniczną do przeciętnego poziomu notowanego w krajach UE. Tak więc, stwierdzono konieczność rozwijania sieci telekomunikacyjnej pań-

---

[79] D. Mider, J. Garlicki, W. Mincewicz, *Pozyskiwanie informacji z Internetu metodą Google Hacking – biały, szary czy czarny wywiad?*, Agencja Bezpieczeństwa Wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 20.

[80] Strategia Bezpieczeństwa Narodowego RP, przyjęta przez Radę Ministrów, zatwierdzona przez Prezydenta RP w dniu 13 listopada 2007 r., http://192.168.0.116/dokumenty/SBN_RP.pdf.

stwa, powiększania zasobów polskiego internetu, wprowadzania powszechnie dostępnych usług elektronicznych, kształtowania umiejętności niezbędnych do aktywnego i twórczego uczestnictwa w usługach społeczeństwa informacyjnego. Szeroko ujęto kwestie bezpieczeństwa informacyjnego i telekomunikacyjnego. Wskazano na konieczność skutecznego zapobiegania próbom destrukcyjnego oddziaływania na infrastrukturę telekomunikacyjną państwa, potrzebę tworzenia długofalowych planów ochrony kluczowych systemów teleinformatycznych oraz nieodzowność poddawania stałej ocenie możliwości wtargnięcia do systemów teleinformatycznych. Za priorytety w działaniu państwa uznano wspieranie narodowych programów i technologii informacyjnych, zwalczanie zagrożeń rządowych systemów teleinformatycznych i sieci telekomunikacyjnych oraz ograniczanie przestępczości komputerowej. Szczególne znaczenie nadano ochronie informacji niejawnych przechowywanych lub przekazywanych w postaci elektronicznej. W sprawach bezpieczeństwa infrastruktury telekomunikacyjnej zapowiedziano współpracę z państwami członkowskimi NATO i UE, z producentami i dostawcami urządzeń informatycznych oraz oprogramowania, krajowymi operatorami telekomunikacyjnymi, dostawcami usług internetowych, ośrodkami badawczymi i szkoleniowymi. Podkreślono znaczenie uczestnictwa w pracach NATO mających na celu przeciwdziałanie próbom destrukcji infrastruktury informacyjnej państwa. Uznano, że bezpieczeństwo państwa jest uzależnione od zapewnienia nowoczesnego i bezpiecznego systemu łączności dla administracji rządowej, sił zbrojnych oraz innych kluczowych instytucji państwowych, i że Polska powinna jak najszybciej zbudować własny system łączności satelitarnej.

W Strategii Obronności Rzeczypospolitej Polskiej z 2009 r.[81], która była dokumentem implementacyjnym do Strategii Bezpieczeństwa Narodowego z 2007 r., problemy zagrożeń cyfrowych nie zostały szerzej podjęte. Poprzestano na ogólnych uwagach na temat walki elektronicznej. W dokumencie tym wspomniano tylko o zadaniach informacyjnych służących ochronie i propagowaniu polskich interesów. Kwestie informatyki osadzono w kontekście zadań związanych z doskonaleniem łączności w systemie obrony.

Zasadniczy postęp w zakresie regulacji strategicznych dotyczących bezpieczeństwa sfery cyfrowej dokonał się w drugiej dekadzie XXI wieku. W przyjętej przez Radę Ministrów w kwietniu 2013 r. „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022”[82] jako

---

[81] Strategia Obronności Rzeczypospolitej Polskiej. Strategia sektorowa do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Ministerstwo Obrony Narodowej, Warszawa 2009, https://biblioteka.womczest.edu.pl/new/wp-content/uploads/2013/09/webowa_biblioteka_edukacja_dla_bezpieczenstwa_strategia_obronnosci_rzeczypospolitej_polskiej.pdf.

[82] Uchwała nr 67 Rady Ministrów z dnia 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022”, M.P. z 2013 r., poz. 377.

odrębne zadanie w ramach tworzenia warunków rozwoju zintegrowanego systemu bezpieczeństwa narodowego wskazano zapewnienie bezpieczeństwa informacyjnego i telekomunikacyjnego. Podkreślono potrzebę podwyższenia stopnia zabezpieczeń zasobów teleinformatycznych administracji publicznej i państwowej, m.in. zabezpieczeń przed zagrożeniami sieci internetu oraz cyberterroryzmem, który „(…) stanowi obecnie jedno z głównych zagrożeń dla bezpieczeństwa teleinformatycznego państw, w tym Polski. Spowodowane jest to między innymi rosnącą liczbą użytkowników sieci internetowej, niewielkimi kosztami związanymi z przeprowadzeniem ataku cyberterrorystycznego, a także możliwością zachowania praktycznie pełnej anonimowości przez odpowiedzialne za niego osoby bądź podmioty". Zapowiedziano, że stosowne działania będą także podejmowane w reakcji na zagrożenia związane z cyberwywiadem. Wśród głównych działań przewidzianych w „Strategii…" wymieniono: przyjęcie polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, umocnienie mechanizmów koordynacji i współdziałania na poziomie państwa poprzez działania Komitetu Rady Ministrów ds. Cyfryzacji, zwiększenie zasięgu działania systemu ARAKIS.GOV (o którym była tu już mowa) poprzez objęcie nim wszystkich urzędów i instytucji państwowych, prowadzenie prac naukowych mających za przedmiot reagowanie na incydenty komputerowe w Systemie Zarządzania Bezpieczeństwem Informacji oraz rozwijanie Systemu Reagowania na Incydenty Komputerowe.

Kwestie cyberbezpieczeństwa uwzględniono w Strategii Bezpieczeństwa Narodowego RP z 2014 r.[83]. W dokumencie tym za jeden ze strategicznych celów w dziedzinie bezpieczeństwa uznano „zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni", co uzasadniono w następujący sposób: „Wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci Internet pojawiły się nowe zagrożenia, takie jak cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych i cyberwojna, rozumiana jako konfrontacja w cyberprzestrzeni między państwami. Obecne trendy rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju. Przy rosnącym uzależnieniu od technologii teleinformatycznych konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw". Autorzy tego dokumentu uważają też, że „Znaczenie bezpieczeństwa w cyberprzestrzeni będzie rosło, podobnie jak odpowiedzialność państw za jej ochronę i obronę. Istotne znaczenie dla zwiększenia poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni ma polityka organizacji

[83] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej zatwierdzona przez Prezydenta Rzeczypospolitej Polskiej 5 listopada 2014 r. na wniosek Prezesa Rady Ministrów, Warszawa 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf.

i struktur współpracy międzynarodowej, w pracach których Polska uczestniczy, oraz współpraca dwustronna z wybranymi państwami, w szczególności z państwami NATO i UE". W myśl tego dokumentu, zadanie zapewnienia bezpieczeństwa Polski w cyberprzestrzeni – jako jedno z podstawowych zadań w sferze bezpieczeństwa państwa – powinno być realizowane poprzez rozwój zdolności do działań defensywnych i ofensywnych. Szczególnie ważne są w tym przypadku: współpraca i koordynacja działań ochronnych z podmiotami sektora prywatnego, prowadzenie działań o charakterze prewencyjnym i profilaktycznym, wypracowanie właściwych procedur komunikacji społecznej, rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców, prowadzenie walki informacyjnej w cyberprzestrzeni, współpraca sojusznicza (także na poziomie działalności operacyjnej). Zgodnie ze stanowiskiem wyrażonym w Strategii z 2014 r., konieczne będzie rozwijanie w Siłach Zbrojnych RP zdolności do działań w cyberprzestrzeni, w tym stworzenie mechanizmów cyberobrony i wzmocnienie zajmujących się nią jednostek oraz rozwijanie narodowych zdolności w zakresie kryptologii dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych.

W Strategii Bezpieczeństwa Narodowego RP z 2020 r.[84] rozwój nowych technologii cyfrowych – zarówno cywilnych, jak i wojskowych – uznano za uwarunkowanie znacznego wzrostu wykorzystania „bezzałogowych i autonomicznych systemów, zautomatyzowanych i zrobotyzowanych platform uzbrojenia wykorzystujących sztuczną inteligencję, a także systemów broni precyzyjnego rażenia na dalekie odległości, w tym rakiet balistycznych i manewrujących". Mając na uwadze zadanie wzmocnienia zdolności operacyjnych Sił Zbrojnych Rzeczypospolitej Polskiej do odstraszania i obrony przed zagrożeniami bezpieczeństwa oraz podniesienia poziomu odporności na cyberzagrożenia, w dokumencie tym wskazano, że należy uzyskać „zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni".

Po 2015 r. politykę cyberbezpieczeństwa regulowały początkowo Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. W dokumencie tym określono cele i zadania, głównie administracji rządowej, związane z podniesieniem poziomu bezpieczeństwa w cyberprzestrzeni RP. Zaliczono do nich: „osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa"; „wzmocnienie zdolności do przeciwdziałania zagrożeniom"; „zwiększanie potencjału naro-

[84] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, załącznik do postanowienia Prezydenta Rzeczypospolitej Polskiej z dnia 12 maja 2020 r. w sprawie zatwierdzenia „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej", M.P. z 2020 r., poz. 413.

dowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni"; „zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa". Szczególną uwagę zwrócono w tym dokumencie na „zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych"[85].

W 2019 r. Rada Ministrów przyjęła nowe regulacje strategiczne dotyczące celów i zadań oraz środków działania w dziedzinie cyberbezpieczeństwa na lata 2019–2024[86]. W strategii rządowej cyberprzestrzeń została zdefiniowana jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (…) wraz z powiązaniami między nimi oraz relacjami z użytkownikami". Za cel główny uznano minimalizowanie podatności na cyberzagrożenia, zwiększenie ochrony informacji w sektorach publicznym (w tym samorządu terytorialnego), militarnym i prywatnym, a także poprawę efektywności zwalczania skutków incydentów w sieci oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Zgodnie z regulacjami Unii Europejskiej[87], cyberzagrożenie określono jako „wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów teleinformatycznych, użytkowników takich systemów oraz innych osób". W strategii uwzględniono w szczególności: cele i priorytety cyberbezpieczeństwa; podmioty zaangażowane we wdrażanie i realizację strategii; środki służące osiąganiu celów strategii; środki w zakresie gotowości i reagowania na incydenty oraz przywracania stanu normalnego (w tym zasady współpracy między sektorem publicznym i prywatnym; podejście do oceny ryzyka; działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa; działania odnoszące się do planów badawczo-rozwojowych z obszaru cyberbezpieczeństwa). Cel główny powiązano z pięcioma celami cząstkowymi, do których zaliczono: rozwój krajowego systemu cyberbezpieczeństwa; podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz uzyskanie zdolności do skutecznego zapobiegania incyden-

---

85 Uchwała nr 52 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa.

86 Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 przyjęta przez Radę Ministrów w uchwale nr 125 z dnia 29 października 2019 r., M.P. z 2019 r., poz. 1037.

87 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. L 151 z 7.06.2019, s. 15.

tom i reagowania na nie; zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni; budowanie świadomości i kompetencji społecznych w dziedzinie cyberbezpieczeństwa; zapewnienie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

W tejże strategii zapowiedziano rozwój systemowych rozwiązań dotyczących szacowania ryzyka i ostrzegania przed zagrożeniami cybernetycznymi, standaryzację zabezpieczeń urządzeń i systemów informatycznych, wzmocnienie systemu rejestrowania i analizowania incydentów, zwiększenie potencjału narodowego w dziedzinie technologii cyberbezpieczeństwa oraz działania służące kształtowaniu świadomości i kompetencji społecznych w sprawach cyberbezpieczeństwa, zwłaszcza – w sprawach bezpiecznego korzystania z wirtualnej przestrzeni. Przyjęto założenie, że Polska musi być przygotowana do wykorzystania narzędzi cybernetycznych także w ramach działań ofensywnych. Zapowiedziano tworzenie warunków do rozwoju polskich zasobów naukowych i przemysłowych na potrzeby cyberbezpieczeństwa, sprzyjanie działalności przedsiębiorstw i ośrodków badawczych pracujących nad innowacyjnymi rozwiązaniami w tym obszarze. Uznano, że niezbędne jest opracowanie Narodowych Standardów Cyberbezpieczeństwa, rozbudowanie kadr systemu, wzmocnienie wymiany informacji oraz współpracy między sektorem publicznym i prywatnym. Dokument zakłada zwiększenie udziału Polski w międzynarodowej współpracy na polu technologii cyberbezpieczeństwa.

W ślad za nadaniem działaniom związanym z cyberbezpieczeństwem charakteru strategicznego w systemie bezpieczeństwa, dla lepszej koordynacji działań państwa wyodrębniono w 2018 r. system cyberbezpieczeństwa[88]. Przyjęto, że celem funkcjonowania krajowego systemu cyberbezpieczeństwa jest w szczególności zapewnienie „niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów". Cyberbezpieczeństwo zdefiniowano w ustawie jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". Ustalono kryteria wartościowania incydentów w sferze cybernetycznej i wskazano odrębne mechanizmy reagowania na incydenty zakwalifikowane jako krytyczne, poważne lub istotne. Działaniami systemu objęto czynności umożliwiające wykrywanie incydentów, ich rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, a także podejmowanie prac naprawczych i ograniczenie skutków incydentów. Ustalono również kryteria i procedury oceniania podatności systemów na zagrożenia

[88] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560 z późn. zm.

oraz rodzaje ryzyka wystąpienia zdarzenia niepożądanego. Określono zasady i procedury świadczenia usług drogą elektroniczną oraz dostarczania usług cyfrowych, w tym obowiązki podmiotów świadczących takie usługi. Istotne znaczenie przypisano współpracy podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa. Do obszernego katalogu podmiotów współtworzących ten system należą m.in.: operatorzy usług kluczowych i dostawcy usług cyfrowych; zespoły reagowania na incydenty bezpieczeństwa komputerowego prowadzone przez ministra obrony narodowej (CSIRT MON), szefa Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV) oraz Naukową i Akademicką Sieć Komputerową (CSIRT NASK); sektorowe zespoły cyberbezpieczeństwa; wskazane w ustawie jednostki sektora finansów publicznych, instytucje finansowe, urzędy administracji, fundusze oraz spółki prawa handlowego; podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz organy właściwe do spraw cyberbezpieczeństwa, w tym punkt kontaktowy do spraw cyberbezpieczeństwa, pełnomocnik rządu i Kolegium do Spraw Cyberbezpieczeństwa. Monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej powierzono ministrowi właściwemu do spraw informatyzacji.

W strukturach wojskowych kluczową rolę w systemie cyberbezpieczeństwa przypisano w 2019 r. Narodowemu Centrum Bezpieczeństwa Cyberprzestrzeni, powołanemu na bazie utworzonego w 2013 r. Narodowego Centrum Kryptologii. Do zadań NCBC należy konsolidacja kompetencji i zasobów Ministerstwa Obrony Narodowej w dziedzinie cyberprzestrzeni i kryptologii, w szczególności „realizacja zadań związanych z prowadzeniem badań, projektowaniem, budową, wdrażaniem, użytkowaniem oraz ochroną narodowych technologii kryptologicznych", a także „wytwarzanie nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych"[89].

W ramach Sił Zbrojnych RP zaczęto formować specjalistyczne Wojska Obrony Cyberprzestrzeni, które zgodnie z zatwierdzoną w 2019 r. koncepcją mają osiągnąć gotowość działania w 2024 r. Utworzono Zespół Działań Cyberprzestrzennych w obrębie Wojsk Obrony Terytorialnej. W Ministerstwie Obrony dokonano konsolidacji instytucji zajmujących się sprawami cyberprzestrzeni. Zadaniom z tym związanym nadano w planie modernizacji technicznej wojska do 2026 r. rangę jednego z priorytetów programu cyber.mil.pl, na który zarezerwowano 3 miliardy złotych[90]. Program ten ma na celu: kompleksowe wsparcie procesu formowania Wojsk Obrony Cyberprzestrzeni; konsolidację potencjału i zasobów jednostek Ministerstwa Obrony, które są zaangażowane

[89] https://www.gov.pl/web/obrona-narodowa/narodowe-centrum-kryptologii. Zob. też: https://ncbc.wp.mil.pl/pl.; https://ncbc.wp.mil.pl/u/Realizacja_Cyber.mil.pl_w_I_kwartale_2020_folder_1.pdf.

[90] https://www.wojsko-polskie.pl/u/pages/atts/2019/5/PLAN_MODERNIZACJI_TECHNICZNEJ_DO_2026_r.pdf.

w zapewnienie bezpieczeństwa w cyberprzestrzeni; stworzenie jednolitego systemu zarządzania obszarem informatyki, teleinformatyki i cyberbezpieczeństwa, z precyzyjnie określonymi zakresami odpowiedzialności; edukację i rekrutację wykwalifikowanej kadry; wdrożenie efektywnych systemów łączności zapewniających łączność międzyresortową oraz bezpieczne przekazywanie informacji niejawnych[91].

Podejmowane są działania w sferze kształcenia zmierzające do przygotowania kwalifikowanych kadr dla systemu cyberbezpieczeństwa. Zwiększono m.in. liczbę studentów na kierunkach informatycznych.

W Biurze Bezpieczeństwa Narodowego funkcjonuje zespół ds. cyberbezpieczeństwa, którego zadaniem jest wspomaganie Prezydenta RP w sprawach polityki państwa dotyczących ochrony cyberprzestrzeni oraz przygotowywanie rekomendacji odnośnie do zmian prawnych i programowych w tej dziedzinie[92].

Przeciwdziałanie zagrożeniom w cyberprzestrzeni zostało wpisane do katalogu działań w systemie zarządzania kryzysowego. Szczególną uwagę poświęcono działaniom służącym ochronie przed tymi zagrożeniami infrastruktury krytycznej, w tym publicznej sieci telekomunikacyjnej oraz stacji nadawczych i odbiorczych używanych do zapewnienia bezpieczeństwa systemu łączności i sieci teleinformatycznych.

Tworzone są systemowe mechanizmy współdziałania w sprawach cyberbezpieczeństwa w relacjach międzynarodowych, m.in. w ramach NATO – organizacji, w której od 2014 r. cyberprzestrzeń jest uznawana za domenę operacyjną. W 2019 r. podpisano z Sojuszem Północnoatlantyckim umowę o współpracy w sprawach cyberbezpieczeństwa. Ustanowiono m.in. system całodobowych punktów kontaktowych, a także zasady i procedury wczesnego ostrzegania o zagrożeniach w cyberprzestrzeni oraz wspólnego reagowania na incydenty informatyczne, w tym przy użyciu Zespołów Szybkiego Reagowania (Rapid Reaction Teams) funkcjonujących w NATO[93]. W 2019 r. podpisano też polsko-amerykańskie porozumienie wojskowe o współpracy w cyberprzestrzeni, obejmującej m.in. wymianę informacji, szkolenia i koordynację działań obronnych[94].

W omawianej już Strategii Bezpieczeństwa Narodowego RP z 2020 r. wskazano następujące cele i zadania: „Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych prak-

---

91 https://www.cyber.mil.pl/misja-i-wizja.

92 https://www.bbn.gov.pl/pl/prace-biura/glowne-inicjatywy/zespol-ds-bezpieczenstw/7266,W-BBN-powstal-Zespol-ds-cyberbezpieczenstwa.html.

93 https://www.gov.pl/web/obrona-narodowa/cyberbezpieczenstwo-wymaga-szerokiej-wspolpracy.

94 https://www.gov.pl/web/obrona-narodowa/zaciesniamy-wspolprace-polsko-amerykanska-w-obszarze-cyber.

tyk umożliwiających obywatelom lepszą ochronę ich informacji". W związku z tym w dokumencie zalecono: zwiększać poziom odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej; osiągnąć zdolność do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia; wzmacniać defensywny potencjał państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa; rozwijać krajowe zdolności do testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa; rozwijać wśród kadr administracji publicznej i w społeczeństwie kompetencje, wiedzę oraz świadomość zagrożeń i wyzwań cyberbezpieczeństwa; wzmacniać i rozbudowywać potencjał państwa m.in. poprzez rozwój rodzimych rozwiązań w zakresie cyberbezpieczeństwa oraz prowadzenie finansowanych przez państwo prac badawczo-rozwojowych nad nowoczesnymi technologiami.

Na tle rozbudowanych regulacji strategicznych oraz rozwiązań instytucjonalnych i funkcjonalnych związanych z działaniami na rzecz bezpieczeństwa informatycznego w Polsce – zdecydowanie skromniej prezentują się efekty prac nad systemowymi gwarancjami bezpieczeństwa informacyjnego[95]. Należy dążyć do większego zaawansowania tych prac, do nadania im większego tempa. Trzeba bowiem pamiętać, że w dzisiejszych czasach klasyczne, tj. pochodzące z epoki przedcyfrowej, militarne czy siłowe sposoby walki między państwami (np. o sporne terytoria) ustępują coraz częściej miejsca akcjom mającym na celu nie tylko podporządkowanie sobie funkcjonowania infrastruktury informatycznej obcego państwa, lecz także uzyskanie wpływu na świadomość społeczną i mentalność żyjących w nim ludzi. Agresorzy podejmują próby ataku za pomocą fałszywych wiadomości upowszechnianych w cyberprzestrzeni. W niektórych przypadkach są to zorganizowane operacje prowadzone w sposób niejawny, przy wykorzystaniu możliwości ukrycia swojej tożsamości. Jest to rodzaj agresji nie mniej groźnej niż interwencja zbrojna – i nie ma w tym stwierdzeniu przesady. W tych warunkach zagwarantowanie bezpieczeństwa informatycznego i informacyjnego staje się sprawą najwyższej rangi. Wszystkie działania podejmowane w tej sferze muszą być wartościowane z punktu widzenia zdolności do zapewnienia suwerenności oraz bezpieczeństwa społecznego, politycznego, ekonomicznego i kulturowego.

Próbę systemowego ujęcia spraw bezpieczeństwa informacyjnego w Polsce należy wiązać zwłaszcza z opracowanym w 2015 r. w Biurze Bezpieczeństwa Narodowego projektem Doktryny Bezpieczeństwa Informacyjnego RP[96]. W dokumencie tym w sposób uporządkowany i całościowy przedstawiono cele strategiczne RP w dziedzinie bezpieczeństwa informacyjnego, wewnętrzny

[95] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2011.

[96] Doktryna bezpieczeństwa informacyjnego RP. Projekt, Warszawa 2015, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf.

i zewnętrzny wymiar tego bezpieczeństwa (w tym zagrożenia, wyzwania i ryzyka) oraz koncepcję zadań operacyjnych i przygotowawczych związanych z utrzymaniem i rozwojem systemu bezpieczeństwa informacyjnego. Przedstawiono również rozwiązania dotyczące systemu kierowania i aktywności operacyjnej w działaniach na rzecz bezpieczeństwa informacyjnego, a także publicznego i prywatnego wsparcia tych działań. Punktem wyjścia tego dokumentu było założenie, że „Bezpieczeństwo informacyjne – wraz z jego integralną częścią, jaką jest cyberbezpieczeństwo – jest jednym z najbardziej wrażliwych obszarów bezpieczeństwa narodowego i międzynarodowego, mającym charakter transsektorowy i wpływającym na efektywność funkcjonowania całego systemu bezpieczeństwa". Jak czytamy w tym projekcie, „Działania na rzecz bezpieczeństwa informacyjnego muszą być podejmowane z uwzględnieniem ochrony praw człowieka i obywatela, a szczególnie poszanowaniem prawa do wolności słowa oraz prywatności. Proporcjonalność środków bezpieczeństwa w stosunku do zagrożeń powinna być oparta na efektywnej i wiarygodnej analizie ryzyka". Zgodnie z przyjętą w przywołanym projekcie definicją, przez bezpieczeństwo informacyjne państwa należy rozumieć „transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa; proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze. Osiąga się to poprzez realizację takich zadań, jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze. Zadania te konkretyzowane są w strategii (doktrynie) bezpieczeństwa informacyjnego (operacyjnej i preparacyjnej), a do ich realizacji utrzymuje się i rozwija odpowiedni system bezpieczeństwa informacyjnego". Środowisko bezpieczeństwa informacyjnego zdefiniowano jako przestrzeń informacyjną (infosferę), tj. „zewnętrzne i wewnętrzne, militarne i niemilitarne (cywilne), osobowe, technologiczne i organizacyjne warunki bezpieczeństwa (warunki realizacji interesów danego podmiotu w dziedzinie bezpieczeństwa informacyjnego i osiągania ustalonych przezeń celów w tym zakresie), charakteryzowane za pomocą takich kategorii, jak zagrożenia, wyzwania oraz szanse i ryzyka". Komunikację społeczną zdefiniowano jako „proces wytwarzania, przekształcania i przekazywania informacji między jednostkami, grupami i organizacjami społecznymi, mający na celu dynamiczne kształtowanie, modyfikację bądź zmianę wiedzy, postaw i zachowań w kierunku zgodnym z wartościami i interesami oddziałujących na nie podmiotów", podkreślając, że w komuni-

kacji społecznej nadawca w przekazie może wykorzystywać środki perswazji lub manipulacji medialnej, aby wywołać określone zachowanie u odbiorcy. W treści dokumentu zostały też uwzględnione operacje informacyjne (zwane również walką informacyjną), tzn. „czynności polegające na oddziaływaniu na informacje i/lub systemy informacyjne w celu kształtowania i przejmowania procesów decyzyjnych przeciwnika (zautomatyzowanych oraz z udziałem czynnika ludzkiego), przy jednoczesnej ochronie własnych procesów decyzyjnych; w wymiarze wojskowym także działalność mająca na celu wywarcie pożądanego wpływu na wolę, rozumienie i zdolności przeciwników, potencjalnych przeciwników lub innych stron konfliktu, wspierających cele danej misji". Zaproponowano uporządkowany sposób rozumienia i wartościowania takich zjawisk ze świata walki informacyjnej, jak: operacje psychologiczne, inżynieria społeczna, propaganda i dezinformacja, manipulacja informacją, trollowanie (trolling).

Do przywołanej wyżej propozycji doktryny bezpieczeństwa informacyjnego nie powrócono już wprost po zmianach politycznych w Polsce, które nastąpiły po wyborach prezydenckich i parlamentarnych w 2015 r. Podejmowano próby stworzenia mechanizmów bezpieczeństwa informacyjnego w ramach ogólnych regulacji. W sprawie eliminowania z internetu profili i treści naruszających standardy prawne i etyczne przyjęto zasadę rozstrzygania maksymalnie dużej liczby problemów w kontakcie z przedstawicielami portali społecznościowych[97]. W Strategii Bezpieczeństwa Narodowego RP z 2020 r. zapisano, że w kontekście rewolucji cyfrowej należy uwzględnić szczególną rolę przestrzeni informacyjnej, zauważając równocześnie, iż obecna sytuacja stwarza pole do dezinformacji i manipulacji informacją, „co wymaga prowadzenia skutecznych działań z zakresu komunikacji strategicznej". W dokumencie tym nadano przestrzeni informacyjnej status jednego z kluczowych czynników w pierwszym filarze bezpieczeństwa narodowego, obejmującym „strzeżenie niepodległości, nienaruszalności terytorialnej, suwerenności oraz zapewnienie bezpieczeństwa państwa i obywateli". Jako wyzwanie strategiczne potraktowano: po pierwsze – zbudowanie „zdolności do ochrony przestrzeni informacyjnej (w tym do systemowego zwalczania dezinformacji), rozumianej jako przenikające się warstwy przestrzeni: wirtualnej (warstwa systemów, oprogramowania i aplikacji), fizycznej (infrastruktury i sprzętu) i poznawczej (kognitywnej)"; po drugie – stworzenie jednolitego systemu komunikacji strategicznej państwa, „którego zadaniem powinno być prognozowanie, planowanie i realizowanie spójnych działań komunikacyjnych, przy wykorzystaniu szerokiej gamy kanałów komunikacji i mediów"; po trzecie – aktywne przeciwdziałanie dezinformacji

[97] http://centrumprasowe.pap.pl/cp/pl/news/info/144846,36,mc-ministerstwo-cyfryzacji-w-kontakcie-z-przedstawicielami-portali-spolecznosciowych(komunikat).

„poprzez budowę zdolności i stworzenie procedur współpracy z mediami informacyjnymi oraz społecznościowymi, przy zaangażowaniu obywateli i organizacji pozarządowych"; po czwarte – zwiększenie w społeczeństwie świadomości zagrożeń związanych z manipulacją informacją „poprzez edukację w zakresie bezpieczeństwa informacyjnego".

Rozdział dziesiąty

Cywilizacja cyfrowa jako narzędzie polityki, rządzenia i administrowania w Polsce

10.1. Miejsce technologii cyfrowych wśród narzędzi zrównoważonego i odpowiedzialnego rozwoju

Świadomość uzależnienia rozwoju państwa od postępu w dziedzinie informatyzacji i cyfryzacji • Miejsce cyfryzacji w strategiach rozwojowych państwa • Świadomość niebezpieczeństw związanych z nowymi inteligentnymi technologiami cyfrowymi • Koncepcja nowoczesnego „cyfrowego państwa usługowego"

Już w pierwszych latach drugiej dekady XXI wieku w dokumentach rządowych jednoznacznie wskazywano w Polsce na znaczenie możliwości, jakie niesie ze sobą ekspansja cyfrowa, dla rozwoju państwa, w tym zwiększania konkurencyjności i innowacyjności gospodarki. Zwracano w szczególności uwagę na potencjał innowacyjny cyfryzacji, który należy wyzwolić.

W Strategii Rozwoju Kraju 2020, przyjętej przez Radę Ministrów we wrześniu 2012 r.[1], zwiększeniu wykorzystania technologii cyfrowych poświęcono odrębny fragment. Oddzielnie wskazano zadania związane z zapewnieniem powszechnego dostępu do internetu, upowszechnieniem stosowania technologii cyfrowych oraz zagwarantowaniem odpowiedniej jakości treści i usług cyfrowych. Podkreślono, że czynnikiem o rosnącym strategicznym znaczeniu dla rozwoju będzie właściwe spożytkowanie przez gospodarkę efektów cyfryzacji i możliwości stwarzanych przez ewolucję przebiegającą od społeczeństwa informacyjnego do sieciowego społeczeństwa cyfrowego. Wprowadzenie jednolitych zasad e-gov w administracji (e-administracja) usytuowano wśród zadań związanych ze zwiększeniem sprawności i efektywności administracji oraz poprawą dostępu do usług publicznych, m.in. poprzez budowę elektro-

[1] Uchwała nr 157 Rady Ministrów z dnia 25 września 2012 r. w sprawie przyjęcia Strategii Rozwoju Kraju 2020. Aktywne społeczeństwo, konkurencyjna gospodarka, sprawne państwo, M.P. z 2012 r., poz. 882.

nicznej platformy usług administracji publicznej (ePUAP) i podjęcie innych działań wynikających z unijnej strategii „Europa 2020".

W Długookresowej Strategii Rozwoju Kraju przyjętej przez Radę Ministrów w lutym 2013 r.[2] podkreślono możliwość swoistego „turbodoładowania", czyli zwiększenia efektu i uzyskania wartości dodanej wynikającej z uruchomienia cyfryzacji, wykorzystania potencjału e-państwa, rozwoju infrastruktury teleinformatycznej, budowy otwartych zasobów publicznych i – co uznano za warunek powodzenia tego kierunku działań – przyspieszenia rozwoju kompetencji cyfrowych społeczeństwa. W dokumencie tym zapowiedziano ukierunkowanie działań na rozwój infrastruktury informatycznej, powszechny dostęp do internetu, podniesienie poziomu badań i prac rozwojowych oraz stworzenie niezbędnych regulacji. Założenia programowe ujęto w następujący sposób: „Cyfryzacja ma sens tylko jako podejście kompleksowe. Aby jednak zapewnić takie podejście konieczne jest: zwiększenie dostępności do Internetu (…), zwiększenie potrzeby używania Internetu poprzez rozwój i udostępnianie treści – zasobów publicznych (…) oraz zwiększenie kompetencji cyfrowych społeczeństwa – promocja i edukacja, co wpływa na innowacyjny rozwój Polski". Odnotowano przy tym, że w Polsce wskaźnik e-government, usług online i infrastruktury telekomunikacyjnej pozostaje poniżej średniej europejskiej.

W przyjętej w lutym 2013 r. przez Radę Ministrów strategii „Sprawne Państwo 2020"[3] ogólne cele i zadania programowe dotyczące cyfryzacji, które były zawarte w dwóch wskazanych wyżej dokumentach, ujęto w ramach działań związanych z realizacją w Polsce Europejskiego Planu Działań na Rzecz Administracji Elektronicznej na lata 2011–2015, Europejskiej Agendy Cyfrowej oraz Europejskiej Strategii Otwartych Danych. Szczególną uwagę poświęcono informatyzacji urzędów państwowych i samorządu terytorialnego, wzmocnieniu kompetencji cyfrowych urzędników oraz stworzeniu mechanizmów wymiany w trybie elektronicznym danych między urzędami.

Orientacja na sięganie w działaniach rozwojowych po narzędzia cyfrowe umocniła się po zmianach politycznych w Polsce w 2015 r. Zwrócono równocześnie większą uwagę na potencjalne niebezpieczeństwa związane z nowymi inteligentnymi technologiami cyfrowymi. W uchwalonej przez Radę Ministrów w lutym 2017 r. Strategii na Rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)[4], która zastąpiła strategię z 2012 r., znalazły się znamienne zdania: „Świat wchodzi w etap czwartej rewolucji przemysłowej

---

[2] Uchwała nr 16 Rady Ministrów z dnia 5 lutego 2013 r. w sprawie Długookresowej Strategii Rozwoju Kraju. Polska 2030. Trzecia fala nowoczesności, M.P. z 2013 r., poz. 121.

[3] Uchwała nr 17 Rady Ministrów z dnia 12 lutego 2013 r. w sprawie przyjęcia strategii „Sprawne Państwo 2020", M.P. z 2013 r., poz. 136.

[4] Uchwała nr 8 Rady Ministrów z dnia 14 lutego 2017 r. w sprawie przyjęcia Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.), M.P. z 2017 r., poz. 260.

opartej na rozwiązaniach cyfrowych. Postęp naukowy i technologiczny w obszarze robotyzacji, mechanizacji, automatyzacji, magazynowania energii, programy rozwoju sztucznej inteligencji i programy rozwoju gospodarki cyfrowej mogą głęboko przeobrazić gospodarkę światową". Przy kształtowaniu strategii wzięto pod uwagę fakt, że „Czwarta rewolucja przemysłowa skutkować będzie wprowadzeniem technologii umożliwiających komunikację między maszynami, upowszechnieniem cyfrowych procesów w zarządzaniu produktami i robotyzacją na nieznaną dotąd skalę. Będzie to w istotny sposób wpływało na edukację, rynek pracy oraz kreowało nowe potrzeby konsumentów". Wskazano równocześnie, że „(…) istnieje duże prawdopodobieństwo niekorzystnego oddziaływania rozwoju technologicznego na rynek pracy w kolejnych latach, w wyniku zastępowania czynnika pracy ludzkiej rozwiązaniami z zakresu robotyzacji i automatyzacji", co oznacza, iż należy dążyć do minimalizowania potencjalnych negatywnych skutków społecznych tej sytuacji. Jako kierunek działań przyjęto „(…) inteligentną reindustrializację, polegającą na wdrażaniu nowych cyfrowych rozwiązań techniczno-technologiczno-organizacyjnych, jak również rozwoju nowych gałęzi przemysłu opartych na technologiach cyfrowych, zdolnych do tworzenia produktów przełomowych". Dalsze postępy w cyfryzacji państwa powiązano z koncepcją kształtowania „cyfrowego państwa usługowego". Ma to przynieść wymierne korzyści, bowiem elektronizacja obsługi obywateli i przedsiębiorców przyczyni się do poprawy funkcjonowania administracji, obniżenia jej kosztów oraz uproszczenia działalności przedsiębiorstw. Ale nie tylko takie efekty są oczekiwane, gdyż „Wysokiej jakości usługi na rzecz obywateli, w tym również przedsiębiorców, (…) dostarczane przez nowoczesne rozwiązania informatyczne", będą wspierać logiczny i spójny system informacyjny państwa, zaś wskutek podjętych działań zwiększy się odsetek osób korzystających z internetu w kontaktach z administracją publiczną (z 16% w 2015 r. do 25% w 2020 r. i 40% w 2030 r.)[5]. Jak wynika z dokumentu, rządzący zdają sobie sprawę z tego, że cyfryzacja i innowacyjność potrzebują odpowiedniej infrastruktury telekomunikacyjnej, w tym dostępu do szerokopasmowego internetu.

10.2. Postęp informatyzacji: podstawowy warunek wdrożenia rozwiązań cyfrowych do realizacji polityk publicznych

Proces informatyzacji w Polsce w perspektywie porównawczej • Priorytetowe znaczenie dostępu do szerokopasmowego internetu • Odległe miejsce Polski w europejskiej statystyce cyfryzacji

[5] Zob. M. Ganczar, *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009.

Większość nowych możliwości działania w przestrzeni publicznej, w tym także w sferze administracyjnej, jest współcześnie uwarunkowana właściwą realizacją podstawowych zadań dotyczących informatyzacji. Po pierwsze – należy zapewnić powszechną dostępność szybkiej, interaktywnej, uwolnionej od nadmiernych kosztów komunikacji internetowej. Po drugie – niezbędne jest upowszechnienie na odpowiednim poziomie zdolności do posługiwania się narzędziami komunikacji internetowej przez obywateli (a także wyrobienie w nich skłonności do sięgania po te narzędzia). Po trzecie – muszą być wypracowane regulacje normatywne odnośnie do e-administracji. Po czwarte – konieczne jest zapewnienie technologicznych gwarancji bezpieczeństwa komunikacji elektronicznej. W tym przypadku podstawowe znaczenie ma też wprowadzenie niezawodnych narzędzi potwierdzania tożsamości podmiotów prawnych i fizycznych, co stanowi nieodzowny warunek bezpieczeństwa elektronicznego obrotu prawnego i finansowego. Po piąte – należy stworzyć ogólnodostępne, zintegrowane zbiory danych publicznych.

Polska jest znacznie opóźniona w dziedzinie informatyzacji w stosunku do innych państw europejskich. Pierwsze próby używania narzędzi elektronicznych w przestrzeni działania państwa miały miejsce w połowie lat siedemdziesiątych XX wieku. Wiązały się one przede wszystkim z budowaniem – w ramach Krajowego Systemu Informatycznego – państwowych rejestrów danych osobowych wykorzystywanych do celów administracyjnych. W 1974 r. uruchomiono system MAGISTER zawierający elektroniczny zbiór danych absolwentów wyższych uczelni. W drugiej połowie lat siedemdziesiątych zaczęto sukcesywnie wdrażać system ewidencji obywateli PESEL (Powszechny Elektroniczny System Ewidencji Ludności). Było to jednak w głównej mierze tworzenie mechanizmów wspomagających działanie instytucji państwowych i nie przekładało się na kształtowanie systemu usług elektronicznych, którego powstanie wymagało zasadniczego postępu w informatyzacji kraju. Do połowy pierwszej dekady XXI wieku w tej dziedzinie brakowało całościowych programów i działań. Zostały one wyraźniej zarysowane dopiero w 2007 r. w Planie Informatyzacji Państwa na lata 2007–2010[6]. W następnych latach opracowywano liczne raporty o stanie realizacji projektów informatyzacji i cyfryzacji oraz przyjmowano kolejne programy działań, m.in. w 2012 r. opracowano raport *Państwo 2.0. Nowy start dla e-administracji*, w 2013 r. przygotowano Program Operacyjny Polska Cyfrowa, w którym zestawiono kierunki działań uwzględnione w rządowych strategiach rozwojowych Polski do roku 2020 i 2030. Równocześnie w kolejnych raportach stale są moni-

[6] Rozporządzenie Rady Ministrów z dnia 28 marca 2007 r. w sprawie Planu Informatyzacji Państwa na lata 2007–2010, Dz.U. z 2007 r. nr 61, poz. 415.

torowane i analizowane postępy w kształtowaniu w Polsce społeczeństwa informacyjnego[7].

W dokumencie poświęconym programowi Polska Cyfrowa określono priorytety związane z informatyzacją. Pierwszym z nich było zapewnienie powszechnego dostępu do szybkiego internetu, połączone z ograniczeniem zróżnicowania terytorialnego pod tym względem. Jako wskaźnik realizacji tego priorytetu przyjęto liczbę gospodarstw domowych mających dostęp do internetu o przepustowości co najmniej 30 MB/s. Drugim priorytetem uczyniono poprawę sytuacji w zakresie e-administracji i otwartości rządzenia. W tej dziedzinie wyznaczono następujące zadania: podniesienie jakości i dostępności e-usług (jako wskaźnik rezultatu przyjęto w tym przypadku odsetek osób korzystających z internetu w relacjach z administracją publiczną oraz odsetek przedsiębiorców korzystających z internetu w kontaktach z administracją publiczną w ramach kompletnych procedur); poprawienie cyfrowej efektywności urzędów (wskaźnik rezultatu: udział ilościowy dokumentów elektronicznych w korespondencji wychodzącej z urzędu przy wykorzystaniu elektronicznej skrzynki podawczej); zwiększenie dostępności informacji sektora publicznego (wskaźnik rezultatu: odsetek internautów pozytywnie oceniających łatwość dostępu do informacji zamieszczanych na stronach internetowych urzędów administracji publicznej i użyteczność tych informacji). Trzecim priorytetem stała się cyfrowa aktywizacja społeczeństwa. Jako wskaźniki rezultatu przyjęto w tym przypadku odsetek osób regularnie korzystających z internetu oraz odsetek osób w wieku 16–74 lat, które prezentują średni lub wysoki poziom umiejętności internetowych, a także liczbę uzdolnionych studentów przygotowywanych do stosowania rozwiązań cyfrowych w gospodarce i administracji.

Wiele konkretnych zamierzeń w dziedzinie informatyzacji sfery publicznej przedstawiono w kolejnych dokumentach strategicznych dotyczących rozwoju społeczno-gospodarczego. Liczne rozwiązania idące w kierunku upowszechnienia i poprawy jakości rozwiązań e-administracji znalazły bardziej szczegółowe ujęcie w dokumentach regulujących planowanie i koordynację informatyzacji działalności podmiotów publicznych[8].

W przyjętym przez Radę Ministrów w 2014 r. Programie Zintegrowanej Informatyzacji Państwa do 2020 r. zawarto cele i spodziewane efekty e-usług.

---

[7] Zob. m.in. raporty pt. *Społeczeństwo obywatelskie w liczbach*, przygotowywane początkowo przez Ministerstwo Spraw Wewnętrznych i Administracji (raport z 2009 r., www.mswia.gov.pl), a następnie – po zmianach w przyporządkowaniu działu administracji rządowej pod nazwą „informatyzacja" – przez Ministerstwo Administracji i Cyfryzacji (raporty z 2012 i 2014 r., www.mac.gov.pl).

[8] Uchwała Rady Ministrów nr 1 z dnia 8 stycznia 2014 r. w sprawie przyjęcia programu rozwoju „Program Zintegrowanej Informatyzacji Państwa", www.mac.gov.pl; uchwała Rady Ministrów nr 2 z dnia 8 stycznia 2014 r. w sprawie przyjęcia programu rozwoju pod nazwą „Narodowy Plan Szerokopasmowy", www.mac.gov.pl oraz komunikat M.P. z 2015 r., poz. 279.

Zgodnie z tym dokumentem, zadaniem administracji publicznej powinno być (na zasadach: logicznego i skutecznego obiegu informacji, koncentracji na procesach i usługach, przejrzystości i efektywności w wydatkowaniu środków publicznych, neutralności technologicznej) budowanie nowych i modernizacja istniejących systemów teleinformatycznych w taki sposób, aby były one ze sobą spójnie i logicznie powiązane oraz zorientowane na potrzeby użytkownika. Podstawowym założeniem programu było stworzenie elektronicznej Platformy Usług Administracji Publicznej (ePUAP), jako miejsca, z którego można mieć dostęp przez internet do e-usług po zweryfikowaniu tożsamości za pomocą profilu zaufanego ePUAP (czyli darmowego e-podpisu).

W ostatnich latach w Polsce odnotowano w dziedzinie informatyzacji znaczne przyspieszenie. Nadal jednak dawały o sobie znać czynniki, które opóźniały osiągnięcie wyznaczonych celów. W 2012 r. administracja publiczna w Polsce prowadziła kilkaset projektów informatycznych, z których 29 znajdowało się na liście priorytetowej i uzyskało finansowanie w ramach siedmiu osi Programu Operacyjnego Innowacyjna Gospodarka. Projekty informatyczne znajdowały się w gestii 14 ministerstw i urzędów. W realizacji licznych projektów występowały opóźnienia, naruszenia ustawy o zamówieniach publicznych, a także nieprawidłowości o charakterze korupcyjnym. Przeprowadzona wówczas analiza pokazała, że: „W przypadku bardzo wielu przedsięwzięć cele i korzyści – nawet jeśli osiągnięte – nie zostały podporządkowane szerszej strategicznej wizji. Widoczny jest brak koncentracji na funkcjach i przyjaznych usługach dla obywateli, a dominuje orientacja na zakup sprzętu i technologii. Brakowało do tej pory możliwości wymiany danych zgromadzonych w «silosowych» systemach poszczególnych ministerstw i urzędów, wobec czego rozwijały one osobne niezależne rejestry, a także niezależne systemy autoryzacji, a obywatel czy przedsiębiorca wielokrotnie podawał te same dane potrzebne różnym instytucjom”[9]. W prezentacji, która towarzyszyła ogłoszeniu przywołanego wyżej raportu, ówczesny minister administracji i cyfryzacji Michał Boni podkreślił, że zasadniczo daje się odczuć brak wielowymiarowego i perspektywicznego podejścia do informatyzacji, w tym brak kompleksowego nastawienia na użytkownika. Istotnym mankamentem jest nieprzejrzystość podejmowanych w tej dziedzinie decyzji oraz niewystarczająca współpraca z interesariuszami. Występują też braki w zakresie: koordynacji na poziomie rządowym; logicznej sekwencyjności w opracowywaniu i realizacji projektów; etapowości w planowaniu oraz wdrażaniu projektów; odpowiednio zaplanowanego w projektach czasu na testowanie; dopasowania rozwiązań do realnych i zmiennych w czasie potrzeb użytkowników oraz zmian w aktach prawnych;

[9] Raport pt. *Państwo 2.0. Nowy start dla e-administracji*, www.mac.gov.pl, s. 1.

analiz kosztów utrzymania. Należy się też liczyć z ryzykiem kumulacji w czasie rozliczeń projektów oraz konsekwencjami braku kompatybilności.

Doświadczenia innych państw pokazują, że o stopniu wykorzystania narzędzi cyfrowych decyduje przede wszystkim poziom dostępu do szerokopasmowego internetu. Korzystający z internetu za pośrednictwem łączy szerokopasmowych znacznie pełniej i aktywniej spożytkowują jego możliwości w kontaktach z urzędami, stymulując tym samym rozwój nowych usług informatycznych w administracji publicznej. Według danych Eurostatu z 2009 r., w 27 państwach UE aż 42% osób posiadających dostęp do internetu szerokopasmowego korzystało z internetu do kontaktowania się z administracją publiczną, zaś wśród osób, które nie miały do niego dostępu, ów wskaźnik wynosił 27%. W Polsce wskaźniki te wynosiły wówczas odpowiednio: 28% i 17%[10]. W kolejnych latach dokonywał się w Polsce w tej dziedzinie postęp, co nie doprowadziło jednak do osiągnięcia takiego stopnia rozwoju, jaki odnotowują liczne państwa członkowskie UE. W diagnozie rządowej z 2014 r. stwierdzono, że: „stan rozwoju infrastruktury szerokopasmowej, a także poziom jej wykorzystania, jest relatywnie niski w porównaniu z większością pozostałych krajów Unii Europejskiej, a także odległy od przyjętych w ramach NPS celów”[11]. W dokumencie tym wskazano, że: po pierwsze – w 2012 r. możliwość stacjonarnego dostępu do internetu uzyskało 69,1% gospodarstw domowych (przy 95,5% w całej UE), przy czym 96,5% populacji miało możliwość korzystania z szerokopasmowego dostępu za pośrednictwem sieci mobilnych (96,3% w UE); po drugie – na koniec 2012 r. zapewniono możliwość dostępu do internetu o przepustowości co najmniej 30 Mb/s w 44,5% gospodarstw domowych (53,8% w UE); po trzecie – na koniec 2012 r. około 1,3% łączy stacjonarnych miało prędkość co najmniej 100 Mb/s (3,4% w UE). W tym samym dokumencie poinformowano, że na koniec 2011 r. przedsiębiorcy telekomunikacyjni w Polsce świadczyli usługę szerokopasmowego dostępu do internetu dla ponad 10 milionów użytkowników, a na koniec 2012 r. dla 11,6 miliona użytkowników, co oznacza przyrost wynoszący 10,7%. Podkreślono, że przełożyło się to na dostęp do szerokopasmowego internetu w gospodarstwach domowych na poziomie 83,5% (przy wzroście o ponad 8% w przypadku usług stacjonarnych i aż o 21% w odniesieniu do dostępu mobilnego). Ponadto poinformowano, że w 2012 r. wskaźnik penetracji internetu kształtował się w Polsce na poziomie 83,5% gospodarstw domowych oraz 29,33% na 100 mieszkańców.

---

[10] Zob. *Internet szerokopasmowy w Polsce – najnowsze dane KE*, www.mswia.gov.pl.

[11] Załącznik do uchwały Rady Ministrów nr 2 z dnia 8 stycznia 2014 r. w sprawie przyjęcia programu rozwoju pod nazwą „Narodowy Plan Szerokopasmowy”, www.mac.gov.pl, s. 6, oraz M.P. z 2015 r., poz. 279.

W marcu 2020 r. Rada Ministrów zaktualizowała Narodowy Plan Szerokopasmowy, ustalając w polityce cyfrowej państwa na kolejne 5 lat nowe cele w zakresie powszechnego dostępu obywateli i przedsiębiorców do szybkiego internetu i rozwoju sieci 5G. Za kluczowe wyzwanie uznano zapewnienie do 2025 r. powszechnego dostępu do internetu o przepustowości co najmniej 100 Mb/s (z możliwością modyfikacji do przepustowości mierzonych w Gb/s), przy wyższej przepustowości (co najmniej 1 Gb/s) w przypadku szkół, węzłów transportowych i miejsc świadczenia usług publicznych oraz przedsiębiorstw prowadzących intensywną działalność w internecie. W 2025 r. ma być także w pełni rozwinięta łączność 5G na wszystkich najważniejszych szlakach komunikacyjnych i w głównych ośrodkach miejskich[12].

Trzeba zauważyć, że sama dostępność sieci internetowych za pośrednictwem łączy szerokopasmowych nie wystarczy do rozwoju usług e-administracji. Efektywna i bezpieczna e-administracja wymaga spełnienia standardów w zakresie: interoperacyjności, bezpieczeństwa teleoperacyjnego, ochrony cyberprzestrzeni, identyfikacji elektronicznej i usługi zaufania, zarządzania infrastrukturą, informacji zarządczej, zarządzania mechanizmami kontrolnymi, kompetencji kadr urzędniczych.

W świetle – przywołanego już w rozdziale trzecim – sprawozdania na 2019 r. przesłanego przez rząd do Unii Europejskiej na potrzeby sporządzanego od 2015 r. przez Komisję Europejską corocznego indeksu gospodarki cyfrowej i społeczeństwa cyfrowego (DESI), Polska, mimo stałego postępu, nadal miała w tej dziedzinie spore deficyty, w rezultacie zajmowała w rankingu cyfryzacji wśród 28 państw UE dopiero 25. pozycję. Przedmiotem analizy przy sporządzaniu tego zestawienia są dane dotyczące łączności szerokopasmowej, umiejętności cyfrowych, korzystania z internetu, cyfryzacji przedsiębiorstw, cyfrowych usług publicznych, sektora ICT i jego wydatków na badania i rozwój, a także wykorzystania przez państwo środków z programu „Horyzont 2020". Odrębnie są uwzględniane dane na temat łączności, korzystania z usług internetowych, cyfrowych usług publicznych, kapitału ludzkiego oraz integracji technologii cyfrowej. W indeksie DESI z 2020 r. niektóre wskaźniki cyfryzacji Polski uległy poprawie, ale równocześnie wzrosły wskaźniki wszystkich państw Unii Europejskiej, co spowodowało, że pozycja naszego kraju w rankingu gospodarki cyfrowej i społeczeństwa cyfrowego zmieniła się tylko nieznacznie: przesunęliśmy się z miejsca 25. na 23. Nadal w Polsce odnotowuje się najmniejszy postęp, jeśli chodzi o kompetencje cyfrowe społeczeństwa, korzystanie z usług internetowych, a także – co jest ważne w ujęciu strategicznym – integrację technologii cyfrowych oraz poziom cyfryzacji przedsiębiorstw. Aż 60% przedsiębiorstw charakteryzuje się bardzo słabym poziomem cyfryzacji

[12] https://www.gov.pl/web/cyfryzacja/narodowy-plan-szerokopasmowy---zaktualizowany.

(średnia w UE wynosi 39%), zaś tylko 11% przedsiębiorstw w Polsce odznacza się wysokim stopniem ucyfrowienia (w UE: 26%). Po stronie pozytywów można zapisać wysoki poziom wykorzystania mobilnych usług szerokopasmowych (z wynikiem 176 abonentów na 100 osób Polska zajmuje pod tym względem 1. miejsce w UE) oraz znaczny, przewyższający średnią UE, zasób danych otwartych. Nastąpił także widoczny postęp pod względem dostępności usług cyfrowych. Według danych z 2019 r., aż 54% użytkowników internetu złożyło formularze w systemie administracji elektronicznej, co w stosunku do 2018 r. stanowiło wzrost o 6%, ale nadal plasowało nas poniżej średniej UE wynoszącej 67%. Także w tej dziedzinie, w której zajmujemy 20. miejsce w UE, jest więc wiele do zrobienia[13].

W sprawozdaniu rządu złożonym w trakcie przygotowywania DESI na 2019 r. wskazano okoliczności wspomagające zmiany związane z cyfryzacją, ale także czynniki stojące na przeszkodzie włączeniu się polskiego społeczeństwa do światowej społeczności internetowej. Zwrócono uwagę na działania w ramach Programu Operacyjnego Polska Cyfrowa z 2014 r., w wyniku których w latach 2014–2019 osiągnięto istotny postęp w zakresie konsolidacji cyfrowych fundamentów rozwoju kraju, w tym upowszechnienia dostępu do szybkiego internetu oraz wprowadzania e-usług publicznych i zwiększania umiejętności cyfrowych. Jednakże pewne osiągnięcia, np. najwyższy w UE poziom wykorzystania mobilnych usług szerokopasmowych, nie upoważniały do mówienia o generalnej poprawie sytuacji, bowiem łączność, korzystanie z usług internetowych i integracja technologii cyfrowej stanowiły w Polsce duży problem. Zasięgiem stałych łączy szerokopasmowych nadal nie było w naszym kraju objętych 21% gospodarstw domowych (w UE wskaźnik ten wynosił 3%).

W ujęciu strategicznym problemem może się okazać w Polsce tempo wdrażania rozwiązań infrastrukturalnych dotyczących rozwoju sieci 5G. W 2020 r. Polska wykazywała zerową gotowość do tworzenia tej sieci (dla całej UE wskaźnik ten wynosił 14%), co miało w istocie podłoże polityczne, gdyż było konsekwencją wycofania się, w dużej mierze pod presją amerykańską, z możliwości skorzystania z oferty chińskiej. Poważną blokadą było też opieszałe tempo zwalniania przez Rosję, Ukrainę i Białoruś pasma 700 MHz, planowanego jako podstawa polskiej sieci 5G, które obecnie jest wykorzystywane przez te trzy państwa do transmisji telewizyjnej. Dodatkowym utrudnieniem stało się odwołanie, w związku z wątpliwościami prawnymi powstałymi w okresie walki z pandemią COVID-19, aukcji na rezerwację na potrzeby sieci 5G częstotliwości z pasma 3,6 GHz. Zapowiedziano ponowne ogłoszenie aukcji

[13] *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego* (DESI) *na 2020 r. – Polska*, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66953.

dopiero w drugiej połowie 2020 r. Sytuacja jest tym trudniejsza, że nie ma już wątpliwości, iż Polska nie osiągnie celu Europejskiej Agendy Cyfrowej, którym jest zagwarantowanie w 2020 r. łączności o przepustowości wynoszącej co najmniej 30 Mb/s dla wszystkich obywateli państw UE.

Optymizmem napawają natomiast perspektywy rozwoju w Polsce chmury informatycznej, niezwykle istotne dla procesu cyfryzacji państwa. Polska Chmura Krajowa, powołana przez PKO BP i Polski Fundusz Rozwoju, weszła w partnerstwo technologiczne z Microsoftem, która to firma zapowiedziała zainwestowanie rekordowej kwoty miliarda dolarów na stworzenie w naszym kraju nowoczesnego centrum danych, pierwszego takiego w Europie Środkowo-Wschodniej[14]. Można się spodziewać, że powodzenie tej inwestycji w Polsce przyczyni się do podniesienia kompetencji cyfrowych w branży IT oraz do cyfrowego włączenia także małych i średnich przedsiębiorstw. Znaczne, sięgające wysokości 1,5 miliarda dolarów, inwestycje w rozbudowę infrastruktury obliczeniowej i telekomunikacyjnej w regionie leżącym w Polsce zapowiedział też koncern Google. Niezależnie od związanych z tymi inwestycjami nadziei na przyspieszenie rozwoju cyfryzacji w Polsce, trzeba jednak pamiętać, że z wyborami strategicznymi odnoszącymi się do obliczeniowej chmury informatycznej wiąże się uzależnienie od technologii amerykańskiej. Niebezpieczeństwo takiego uzależnienia pojawia się wszędzie tam, gdzie nie stosuje się strategii dywersyfikacji partnerów. Należy przy tym zauważyć, że Polska zdaje się pomijać ostrzeżenia ze strony Francji i Niemiec, które dotyczą możliwości niejawnej kontroli przez służby specjalne USA danych zlokalizowanych w chmurach współtworzonych przez firmy amerykańskie. Brak też w postępowaniu decyzyjnym Polski zrozumienia znaczenia polityki przeciwdziałania dalszemu ograniczeniu „suwerenności technologicznej" Europy. Warto przypomnieć w tym kontekście, że Francja i Niemcy dążą do utworzenia odrębnej europejskiej chmury danych, a przynajmniej przyjęcia oferty usług hostingu w chmurze w ramach platformy Gaia-X – rozwiązania konkurencyjnego wobec Amazon Web Services oraz Microsoftu[15]. Unia Europejska z pewnością będzie coraz energiczniej promować w sprawach cyfryzacji rozwiązania europejskie, co może sprawić, że Polska – ze względu na powiązania z amerykańskimi gigantami cyfrowymi – znajdzie się na kursie kolizyjnym z innymi państwami naszego kontynentu.

---

14 https://businessinsider.com.pl/technologie/nowe-technologie/microsoft-zainwestuje-miliard-dolarow-w-polsce-na-centrum-danych-i-technologie/92le0vd.

15 https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty.

10.3. E-government: kluczowy element Cyfrowego Państwa

Pozyskiwanie i zarządzanie informacjami w trybie elektronicznym • Zmiany w zakresie polityk publicznych w warunkach ekspansji cyfrowej • Mechanizmy instytucjonalne i proceduralne w polskiej administracji publicznej związane z informatyzacją • Udostępnianie usług administracyjnych świadczonych drogą elektroniczną • Mechanizmy zintegrowanej informacji publicznej

W związku z ekspansją technologii cyfrowych, w organizacji i działaniach państw zachodzą nieuniknione jakościowe zmiany, które nie ograniczają się tylko do dziedziny bezpieczeństwa. W istocie stwarzają one we wszystkich obszarach działania państw zupełnie nową sytuację. Bodźcem do tych zmian – w pewnym sensie także ich treścią czy budulcem – są nieznane dotąd możliwości, jakie niesie ze sobą postęp naukowy i technologiczny. Razem wzięte, zmiany te prowadzą do kształtowania nowego, całościowego rozwiązania systemowego, które coraz częściej jest określane jako model Cyfrowego Państwa (Digital State). W obrębie tego modelu następuje integracja cyfrowej transformacji zachodzącej w poszczególnych segmentach sektora publicznego, powstaje nowa jakość cyfrowych usług publicznych oraz pojawia się nowa forma partycypacji obywatelskiej[16]. Programowanie i efektywne wdrażanie zmian inspirowanych nowymi technologiami stanowi współcześnie jedno z ważniejszych zadań w ramach rządzenia. Punktem wyjścia jest w tym przypadku informatyzacja, w tym informatyzacja administracji publicznej, oraz tworzenie w efekcie podstaw e-administracji (e-government) czy też, w bardziej zaawansowanej postaci, nowej cyfrowej administracji (digital government).

Informatyzacja radykalnie zmienia mechanizmy pozyskiwania i zarządzania informacjami oraz komunikowania się. Powstają tym samym nowe możliwości poprawy działania administracji publicznej oraz kształtowania e-administracji. Narzędzia cywilizacji cyfrowej wyznaczają nowe standardy w relacjach między administracją publiczną i obywatelami. W e-administracji wiele spraw wymagających dotychczas osobistych wizyt w urzędach można załatwiać w trybie elektronicznym, często w czasie rzeczywistym. Powstaje infrastruktura interaktywnych kontaktów elektronicznych, która może być użyta do rozwijania partycypacyjnych mechanizmów administrowania. Pojawiają się nowe formy organizacji pracy organów i urzędów administracji publicznej; odnosi się to

[16] Zob.: A. Sobczak, *Wizja Cyfrowego Państwa*, Ośrodek Studiów nad Cyfrowym Państwem, https://www.cyfrowepanstwo.pl/wizja-cyfrowego-panstwa/cyfrowa-transformacja-organizacji-publicznych; M. Kowalczyk, *Cyfrowe Państwo…*, s. 10 i nast.; M. Sitek, P.B. Zientarski (red.), *Wybrane aspekty informatyzacji w samorządach a zasada dobrej administracji*, Warszawa 2019.

również do procesu decyzyjnego, który może być wspomagany poprzez stosowanie narzędzi elektronicznych. Tradycyjne rozwiązania i relacje hierarchiczne mogą być dopełniane przez mechanizmy sieciowe. W istotny sposób zwiększają się możliwości dostępu do informacji publicznej, w tym w ramach systemu rejestrów publicznych, oraz powstają warunki wykorzystywania w relacjach administracyjnych zasobu ogólnie dostępnych danych.

Pokonywanie wyzwań związanych z informatyzacją stanowi niezbędną przesłankę efektywnego działania we wszystkich dziedzinach funkcjonowania państwa, struktur pozapaństwowych oraz pojedynczych obywateli. W przypadku administracji, wraz z rozwojem zdolności cyfrowych pojawiają się dodatkowe wyzwania związane z zagwarantowaniem zdolności działania w czasie rzeczywistym. Podobnie jak dawniej stało się to za sprawą upowszechnienia telegrafu, telefonii, maszyn do pisania, obecnie informatyzacja zdecydowanie zmienia też warunki wykonywania pracy biurowej. Chodzi tu przede wszystkim o pozyskiwanie informacji i zarządzanie nimi, organizację procesów decyzyjnych oraz standardy kontaktów między stronami stosunków administracyjnych. Ważnym zadaniem staje się wypracowanie i wdrożenie nowych rozwiązań w sferze informacji i zasobów danych. Dotyczy to zarówno strategii administracji otwartej informacyjnie[17], jak i zagwarantowania skutecznych zabezpieczeń informacji niejawnych (m.in. przy użyciu profesjonalnych procedur kryptograficznych) oraz niezakłóconego funkcjonowania elektronicznych rozwiązań systemowych (m.in. infrastruktury krytycznej państwa, baz danych, zbiorów danych osobowych i kanałów przepływu korespondencji elektronicznej).

Rozwój cywilizacji cyfrowej oraz sztucznej inteligencji zmienia zasadniczo sytuację w zakresie polityk publicznych. Powstają nowe obszary polityk publicznych – jako przykład można podać politykę cyberbezpieczeństwa. Równocześnie rzeczą nieodzowną jest dostosowanie dotychczasowych polityk publicznych do zmieniających się warunków. Chodzi tu m.in. o polityki w obszarze edukacji oraz stosunków pracy i gwarancji zatrudnienia.

Wiele faktów świadczy o tym, że narzędzia elektroniczne mogą w najbliższej przyszłości stać się ważnym elementem optymalizacji systemowych działań w politykach publicznych. Zwracałem już wcześniej uwagę na znaczenie tych narzędzi w działaniach na rzecz zagwarantowania bezpieczeństwa zewnętrznego i wewnętrznego. W tym miejscu można wskazać m.in. ochronę zdrowia jako obszar, gdzie zapewne dość szybko pojawią się nowe rozwiązania, które trzeba będzie uwzględniać w planowaniu i organizowaniu tej sfery polityki publicznej. Z informacji, które w 2019 r. dochodziły z pracowni badawczych, wynika, że algorytmy mogą się stać ważnym wsparciem w wykrywaniu zmian

[17] Zob. A. Sobczak, T. Kulisiewicz, *Otwarty Rząd i ponowne wykorzystanie informacji publicznej – inspirujące wzorce z Polski i ze świata*, Łódź 2013, s. 5 i nast.

nowotworowych i niektórych innych chorób na wczesnym etapie rozwoju, kiedy nie ma jeszcze możliwości ich zdiagnozowania tradycyjnymi metodami. Przykładowo, wstępne stadia ostrej niewydolności nerek, a nawet „jedynie" zagrożenie tą chorobą można będzie wykryć jeszcze przed pojawieniem się widocznych objawów, co znalazło potwierdzenie w projektach opracowanych przez należącą do koncernu Alphabet firmę DeepMind. W badaniach na pacjentach, niemal w 90% zidentyfikowano poważne schorzenia nerek, które na dalszych etapach rozwoju wymagałyby już dializy lub przeszczepu[18]. Również w 2019 r. poinformowano, że badacze z Massachusetts Institute of Technology opracowali narzędzia sztucznej inteligencji, dzięki którym można (ze stale wzrastającym wskaźnikiem prawdopodobieństwa) wykryć raka piersi, zanim da się on wychwycić w tradycyjnym badaniu. Modele zastosowane w tych narzędziach zostały już wyposażone w pamięć zawierającą informacje pobrane z ponad 90 tysięcy zdjęć mammograficznych pochodzących od pacjentek Massachusetts General Hospital[19].

Proces włączania narzędzi sztucznej inteligencji do procedur medycznych wyraźnie przyspiesza. Nie dotyczy to tylko diagnozowania online za pomocą inteligentnych rozwiązań. Roboty zaczynają zastępować człowieka w fazie leczenia. Przykładem są roboty chirurgiczne da Vinci. W Stanach Zjednoczonych jeden taki robot przypada na 100 tysięcy mieszkańców (dla porównania: w Polsce – na 6,5 miliona osób). Według informacji zawartych w materiale autorstwa Katarzyny Kucharczyk, na świecie przeprowadzono do tej pory ponad 6 milionów operacji przy wsparciu systemu robotycznego da Vinci, z czego około miliona w 2018 r.[20]. W tym samym materiale prasowym przedstawiono także opinie specjalistów, którzy zakładają, że liczba robotów chirurgicznych da Vinci będzie się zwiększała także w Polsce, zaś rynek robotyki chirurgicznej w naszym kraju ma szansę urosnąć w ciągu najbliższych czterech lat z obecnych 92 milionów złotych aż do 500 milionów. Dagmara Pomirska, szefowa sprzedaży w Axis Communications, przewiduje, że już niedługo w Polsce „inteligentne systemy wizyjne, zdolne do zaawansowanej analityki z wielu źródeł danych, będą gotowe do wstępnego diagnozowania, a także rozładowywania kolejek w szpitalnych oddziałach ratunkowych", a nawet „rozpoznają stan pacjenta i określą, czy potrzebuje natychmiastowego działania, np. podania określonego leku".

---

18 https://cyfrowa.rp.pl/technologie/36566-ai-ostrzeze-przed-niewydolnoscia-nerek?utm_source=rp&utm_medium=teaser_redirect.

19 https://www.msn.com/pl-pl/wiadomosci/nauka-i-technika/ai-wykryje-raka-piersi-zanim-pojawi%C4%85-si%C4%99-objawy/ar-AADDQ8R?li=AA51Z1.

20 https://cyfrowa.rp.pl/technologie/42233-zaufaj-robotom-wlasnie-wchodza-na-sale-operacyjne?utm_source=rp&utm_medium=teaser_redirect.

Zainteresowanie wykorzystaniem zdolności robotów do wykonywania zadań związanych z opieką nad chorymi wzrosło w okresie pandemii w 2020 r. Na przykład w Chinach, w jednym ze szpitali w Wuhan ograniczono kontakty personelu medycznego z zarażonymi pacjentami dzięki zastąpieniu go w niektórych czynnościach przez urządzenia cyfrowe. W szpitalu tym na większości oddziałów pacjenci zostali wyposażeni w elektroniczne bransolety, które w sposób ciągły mierzyły temperaturę ciała i rejestrowały pracę serca, zaś dane te w czasie rzeczywistym, za pośrednictwem centralnego rejestru elektronicznego wskazywały przypadki, w których potrzebna była interwencja lekarzy[21].

Informatyzacja stanowi współcześnie jedną z głównych proinnowacyjnych polityk administracyjnych w państwach europejskich. W Unii Europejskiej włączenie administracji publicznej do procesu rozwoju społeczeństwa informacyjnego stało się wyzwaniem strategicznym. Na obranie tego kierunku działań w zasadniczy sposób wpłynęły treści tzw. strategii lizbońskiej, przyjętej na unijnym szczycie w 2000 r., na podstawie których przystąpiono do kolejnych edycji planów „eEurope". W pierwszej dekadzie XXI wieku aktywność Unii Europejskiej w sprawach informatyzacji wpisywała się w realizację programu Europejskiej Agendy Cyfrowej, którą przyjęto w 2010 r. jako integralną część strategii „Europa 2020". Celem tego programu było stymulowanie wzrostu gospodarczego poprzez lepsze wykorzystanie potencjału technologii informacyjnych i komunikacyjnych oraz budowę jednolitego europejskiego rynku cyfrowego dla konsumentów i przedsiębiorstw[22].

W dzisiejszym świecie w istocie nie ma sensownej alternatywy dla rozwoju e-administracji. Poszczególne kraje są jednak w różnym stopniu zaawansowane w jej tworzeniu. Środowiskiem działania administracji publicznej jest w coraz większej mierze mobilne społeczeństwo informacyjne, w którym na masową skalę korzysta się z internetu, poczty elektronicznej, baz danych, wyszukiwarek i telefonii komórkowej. Informacja staje się w tych warunkach dobrem powszechnym, trudnym do reglamentowania przez podmioty państwowe, udostępnianym ponad granicami państw w czasie rzeczywistym. Opanowanie zdolności informatycznych bywa w wielu wypadkach niezbędną przesłanką dalszej kariery zawodowej. Obowiązkiem władz publicznych jest w tej sytuacji tworzenie warunków do rozwoju i popularyzacji rozwiązań informatycznych. Dotyczy to sfery normatywnej, instytucjonalnej, proceduralnej i kadrowej.

Rozwój środków i metod komunikacji elektronicznej rodzi oczekiwania społeczne co do świadczenia usług drogą elektroniczną także przez podmioty administracji publicznej. Informatyzacja jest przesłanką produktywnego i efektywnego funkcjonowania administracji i dostarczania przez nią usług

[21] https://cyfrowa.rp.pl/technologie/45471-w-gniezdzie-wirusa-dziala-szpital-5g-to-przyszlosc-medycyny?utm_source=rp&utm_medium=teaser_redirect.

[22] Europejska Agenda Cyfrowa, KOM(2010)245, http://eur-lex.europa.eu.

o możliwie najwyższej jakości, stanowi szansę lepszego wykonywania zadań. Współcześnie jest zarówno ważnym uwarunkowaniem, jak i istotnym elementem działania organów oraz urzędów administracji publicznej. Nowe możliwości i metody zdobywania informacji wiążą się z koniecznością ustalenia, w sposób zgodny z zasadami demokratycznego państwa prawnego, granic pozyskiwania, gromadzenia i udostępniania informacji o obywatelach. Nie da się tutaj ominąć problemu gwarancji wolności i praw jednostek.

Nowe, bardziej efektywne metody zarządzania informacjami w administracji pociągają za sobą obowiązek rozbudowy i integracji systemów informatycznych oraz standaryzacji i koordynacji oprogramowania, dokumentów elektronicznych i procedur. Niezbędne są działania ukierunkowane na bezpieczeństwo obrotu elektronicznego, w tym specjalne rozwiązania odnoszące się do infrastruktury krytycznej państwa oraz zabezpieczenia baz danych i kanałów przepływów. Jak już wcześniej sygnalizowałem, w działaniu e-administracji pojawiają się zagrożenia ze strony cyberprzestępczości, w tym cyberterroryzmu. Sprawą kluczową staje się więc zagwarantowanie autentyczności i rozliczalności użytkowników systemu informacyjnego oraz integralności danych, w tym szczególnie wykluczenie nieupoważnionej modyfikacji lub zniszczenia dokumentów, nieupoważnionego dostępu do dokumentów lub ujawniania ich treści oraz fizycznego zakłócenia funkcjonowania systemu. Nowe formy kontaktowania się stron stosunków administracyjnych w ramach e-administracji wymagają prowadzenia działań informacyjnych i edukacyjnych. Kształtowanie procesów decyzyjnych z wykorzystaniem narzędzi elektronicznych nie może się obyć bez specjalnej infrastruktury. Potrzeba działania „w czasie rzeczywistym" zmienia standardy w podejściu do czasu w funkcjonowaniu administracji, zwłaszcza w podejmowaniu decyzji. Dążenie do zwiększenia otwartości i przejrzystości działań administracji musi być poparte rozbudową bazy narzędzi informacyjno-komunikacyjnych. Wszelkie działania w sferze informatyzacji są możliwe tylko przy zagwarantowaniu odpowiednich kwalifikacji urzędników.

Kluczowe znaczenie dla zdolności wykonywania zadań państwa związanych z informatyzacją miało w Polsce stworzenie w administracji rządowej odrębnego działu, jakim jest informatyzacja. W 2011 r. w kompetencjach jednego ministra (i ministerstwa) znalazły się działy administracja, informatyzacja i łączność. W późniejszym okresie kwestie informatyzacji (wraz z działaniami z obszaru łączności) stały się przedmiotem kompetencji odrębnego ministra. Po 2015 r. w ramach działu informatyzacja skupiają się zadania i kompetencje dotyczące: informatyzacji administracji publicznej oraz podmiotów wykonujących zadania publiczne; systemów i sieci teleinformatycznych administracji publicznej; wspierania inwestycji w obszarze informatyzacji; realizacji zobowiązań międzynarodowych Polski w dziedzinie informatyzacji i telekomunikacji; udziału w kształtowaniu polityki Unii Europejskiej w zakresie informatyzacji; rozwo-

ju społeczeństwa informacyjnego i przeciwdziałania wykluczeniu cyfrowemu; rozwoju usług świadczonych drogą elektroniczną; kształtowania polityki państwa w zakresie ochrony danych osobowych; bezpieczeństwa cyberprzestrzeni w wymiarze cywilnym (właściwy w sprawach cyberbezpieczeństwa w wymiarze militarnym jest minister kierujący działem obrona narodowa); rejestru PESEL, Rejestru Dowodów Osobistych, Rejestru Stanu Cywilnego oraz Centralnej Ewidencji Wydanych i Unieważnionych Dokumentów Paszportowych; ewidencji pojazdów, ewidencji kierowców oraz ewidencji posiadaczy kart parkingowych; nadzoru nad świadczeniem usług zaufania; identyfikacji elektronicznej[23]. Minister właściwy w zakresie tego działu sprawuje także nadzór nad Prezesem Urzędu Komunikacji Elektronicznej – organem regulacyjnym w sprawach działalności telekomunikacyjnej, pocztowej oraz gospodarki zasobami częstotliwości i organem nadzoru rynku w zakresie kontroli wyrobów emitujących pole elektromagnetyczne lub podatnych na jego działanie, w tym urządzeń radiowych wprowadzonych do obrotu handlowego na terenie Polski.

Od kwietnia 2020 r. minister Marek Zagórski, kierujący działem administracji informatyzacja, jest równocześnie pełnomocnikiem rządu do spraw cyberbezpieczeństwa[24]. Dzięki temu nie powinno już dochodzić do sporu o to, który minister ma koordynować działania związane z cyberbezpieczeństwem. Do zadań pełnomocnika należy m.in. koordynacja, w porozumieniu z właściwymi ministrami, spraw związanych z analizą i oceną funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych z udziałem organów administracji publicznej, organów właściwych do spraw cyberbezpieczeństwa, krajowych zespołów reagowania na incydenty bezpieczeństwa: CSIRT MON, CSIRT NASK i CSIRT GOV. Do zadań tych należy także: nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa; upowszechnianie nowych rozwiązań i inicjowanie działań służących zapewnieniu cyberbezpieczeństwa na poziomie krajowym; inicjowanie krajowych ćwiczeń w zakresie cyberbezpieczeństwa; wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek krajowych zespołów reagowania na incydenty bezpieczeństwa CSIRT; współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi; podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa oraz podnoszenie świadomości i wiedzy społeczeństwa o zagrożeniach cyberbezpieczeństwa i bezpiecznym korzystaniu z internetu.

---

[23] Ustawa z dnia 4 września 1997 r. o działach administracji rządowej, tekst jedn. Dz.U. z 2020 r., poz. 945 z późn. zm.

[24] https://www.gov.pl/web/cyfryzacja/minister-marek-zagorski-pelnomocnikiem-rzadu-ds-cyberbezpieczenstwa. Urząd pełnomocnika rządu do spraw cyberbezpieczeństwa istniał już w strukturach administracji rządowej w latach 2018–2019.

Okolicznością istotną dla tworzenia infrastruktury funkcjonalnej informatyzacji było wpisanie wymagań związanych z tą dziedziną do rządowego procesu decyzyjnego. Projekty dokumentów rządowych są kierowane, jeszcze przed przedstawieniem ich stałemu Komitetowi Rady Ministrów, do Komitetu Rady Ministrów do Spraw Cyfryzacji. Organ ten został utworzony w 2012 r., w miejsce istniejącego od 2007 r. Komitetu Rady Ministrów do Spraw Informatyzacji i Łączności[25], i wyposażony w znaczne kompetencje, które dodatkowo wzmocniono jeszcze w 2014 r.[26]. Jako organ pomocniczy Rady Ministrów i Prezesa Rady Ministrów uczestniczy w rządowym procesie legislacyjnym. Stał się ważnym narzędziem koordynacji spraw związanych z informatyzacją, gdyż obligatoryjnie opiniuje wszystkie projekty dokumentów rządowych, które dotyczą: informatyzacji administracji publicznej; rozwoju społeczeństwa informacyjnego; sieci szerokopasmowych; wdrażania rozwiązań informatycznych (w szczególności w zakresie edukacji, ochrony zdrowia i podpisu elektronicznego); łączności; rejestrów publicznych; polityki audiowizualnej; zastosowania technologii informacyjnych w budowie gospodarki opartej na wiedzy; współpracy organów administracji państwowej z Systemem Informacyjnym Schengen i Wizowym Systemem Informacyjnym; zastosowania technologii informacyjnych w infrastrukturze transportowej.

W ostatnich kilku latach w Polsce zachodzą pozytywne zmiany w udostępnianiu usług administracyjnych świadczonych drogą elektroniczną[27]. Oceniając te zmiany, nie można zapominać, jak wielkie w punkcie wyjścia były zapóźnienia, które przyszło nam odrabiać. Warto tu odnotować, że w badaniach porównawczych gotowości sektora publicznego do zastosowania technik i technologii informatycznych Polska w 2004 r. sytuowała się dopiero na 93. miejscu wśród 104 badanych krajów[28]. W Europie postęp w udostępnianiu usług administracji publicznej drogą elektroniczną mierzono do 2013 r. za pomocą wskaźnika dostępności online 20 podstawowych usług administracji publicznej[29]. Usługę traktowano jako dostępną, gdy przez internet można było załatwić sprawę, przesłać wypełniony wniosek, pobrać formularz, a w naj-

---

25 M.P. z 2007 r. nr 52, poz. 604 z późn. zm.

26 Zarządzenie nr 1 Prezesa Rady Ministrów z dnia 5 stycznia 2012 r. w sprawie Komitetu Rady Ministrów do Spraw Cyfryzacji, M.P. z 2012 r., poz. 1; zarządzenie nr 37 Prezesa Rady Ministrów z dnia 30 maja 2014 r. w sprawie Komitetu Rady Ministrów do spraw Cyfryzacji, M.P. z 2014 r., poz. 395.

27 K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *E-obywatel. E-sprawiedliwość. E-usługi*, Warszawa 2017; M.K. Zwierżdżyński, M. Lakomy, K. Oświecimski (red.), *E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni*, Kraków 2016.

28 W. Sartorius, *Społeczeństwo informacyjne w Narodowym Planie Rozwoju*, „eAdministracja" 2005, nr 1, s. 31.

29 *Społeczeństwo informacyjne w liczbach 2014*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014, s. 165 i nast.

gorszym wypadku – uzyskać ze strony internetowej podmiotu administracji publicznej informację o sposobie załatwiania sprawy. W 2007 r. w naszej krajowej administracji było dostępnych zaledwie pięć z koszyka 20 badanych usług, a więc wówczas wskaźnik dla Polski wyniósł 25%. Gorszy wynik w Europie miała tylko Bułgaria. W tym czasie w trzech najlepszych w tej dziedzinie krajach UE (Austria, Malta, Słowenia) można było już skorzystać online z 19 spośród 20 badanych usług, co dawało średnią na poziomie 95%. W 2010 r. połowa krajów uczestniczących w badaniu osiągnęła już poziom co najmniej 90%, a sześć państw – 100%. Po modyfikacji metodologii pomiaru, wskaźniki odnoszące się do 20 usług publicznych w układzie resortowym zastąpiono wskaźnikami odnoszącymi się do zestawu usług publicznych, które są potrzebne w wybranych sytuacjach życiowych. Podejmowane działania rozwojowe dotyczące informatyzacji sfery publicznej spowodowały, że: „W okresie od 2007 do 2013 r. dystans w zakresie dostępności online usług publicznych dzielący Polskę od liderów europejskich z 70 punktów procentowych zmalał do 19 punktów. W 2013 r. wskaźnik dostępności online usług publicznych przydatnych w siedmiu (…) sytuacjach życiowych osiągnął w Polsce wartość 76% – 4 punkty powyżej średniej unijnej. W czołówce UE znalazły się: Malta z wynikiem 97%, Portugalia – 96% i Hiszpania – 91%. (…) Polska (…) uczyniła znaczny krok w kierunku nowoczesnej administracji, gdyż znalazła się w pierwszej piętnastce krajów, przed takimi potęgami jak Francja, Wielka Brytania czy Niemcy". W tym samym dokumencie podano, że już blisko co drugi urząd w Polsce udostępniał w 2013 r. usługi elektroniczne; w stosunku do 2012 r. był to wzrost o 45%[30].

Nie wolno jednak pomijać opinii krytycznych wobec rezultatów dotychczasowych działań. W programie uchwalonym przez Radę Ministrów w 2014 r. zaprezentowano – niewątpliwie znaczne – osiągnięcia na polu e-administracji, a jednocześnie podkreślono, że tylko nieliczne usługi elektroniczne dostarczane dzięki współpracy różnych resortów są świadczone w sposób satysfakcjonujący, zaś na budowę systemów teleinformatycznych administracji państwowej w większości składały się odseparowane od siebie i jedynie w niewielkiej mierze koordynowane centralnie działania poszczególnych resortów. W dokumencie tym stwierdzono, że „Niewystarczająca dojrzałość szeregu e-usług administracji w Polsce, w odniesieniu do oczekiwanego poziomu transakcyjności (np. dostępna jest informacja, a użytkownicy oczekują dwustronnej interakcji albo wręcz finalizacji transakcji), skutkuje niesatysfakcjonującym stopniem ich wykorzystania przez społeczeństwo (28% obywateli korzystało z usług e-administracji w 2011 r., natomiast w 2012 r. odsetek ten wyniósł już 32%). Nieporównywalnie lepiej wygląda korzystanie z usług online przez

[30] Tamże, s. 166–167.

przedsiębiorców – odsetek korzystający z internetu w relacjach z administracją osiągnął w 2012 r. poziom 90%"[31].

W diagnozie z 2014 r. Rada Ministrów przypomniała, że mimo wszystkich pojawiających się trudności i opóźnień, liczne e-usługi są już w Polsce dostępne dla obywateli w czasie rzeczywistym. W sprawach administracyjnych i obywatelskich były wówczas dostępne następujące e-procedury: potwierdzanie tożsamości w elektronicznych kontaktach z administracją w ramach bezpłatnego profilu zaufanego ePUAP; e-usługi poprzez platformę PUAP (obejmujące m.in. sprawdzanie stanu składek ubezpieczenia społecznego); elektroniczne sprawdzanie stanu realizacji złożonego wniosku paszportowego i weryfikacja dokumentów (np. prawa jazdy i dowodu rejestracyjnego). W sprawach rynku pracy – m.in. przeszukiwanie centralnej bazy krajowych ofert pracy zgłoszonych do powiatowych i wojewódzkich urzędów pracy oraz rejestracja online osoby bezrobotnej lub poszukującej pracy. W sprawach ochrony zdrowia – m.in. elektroniczne sprawdzanie prawa pacjenta do świadczeń opieki oraz dostęp do informacji o udzielonych pacjentowi świadczeniach opieki zdrowotnej. W sprawach dotyczących przedsiębiorców – m.in.: udostępnianie cyfrowych rejestrów medycznych, rejestracja i aktualizacja danych rejestrowych, pobieranie wypisów i zaświadczeń, dwustronna wymiana dokumentów z organami rejestrowymi, sprawdzanie stanu realizacji wniosków i automatyczne potwierdzanie odbioru dokumentu. W sprawach wymiaru sprawiedliwości i sądownictwa – m.in. dostęp do Krajowego Rejestru Sądowego (KRS), informacji z Monitora Sądowego i Gospodarczego oraz ksiąg wieczystych. W sprawach bezpieczeństwa i powiadamiania ratunkowego – system alarmowego numeru 112. W sprawach prowadzenia działalności gospodarczej – m.in.: rejestracja i dokonywanie zmian dotyczących działalności gospodarczej osób fizycznych; obsługa zgłoszeń identyfikacyjnych lub aktualizacyjnych, o których mowa w ustawie o zasadach ewidencji i identyfikacji podatników i płatników; obsługa wniosków składanych do krajowego rejestru urzędowego REGON. W sprawach prowadzenia działalności rolniczej – składanie przez rolników wniosków o dopłaty. W sprawach rozliczania należności podatkowych – m.in. składanie elektronicznych deklaracji podatkowych przez osoby fizyczne i osoby prawne, a także dotyczących podatku od towarów i usług, podatku od spadków i darowizn oraz podatku od czynności cywilnoprawnych. W sprawach obsługi celnej – dokonywanie i rozliczanie drogą elektroniczną większości operacji związanych z obrotem towarowym z zagranicą, w tranzycie i obrocie towarami akcyzowymi. Możliwy był elektroniczny dostęp do danych: przestrzennych, statystycznych, rejestru urzędowego REGON, syste-

[31] Załącznik do uchwały Rady Ministrów nr 1 z dnia 8 stycznia 2014 r. w sprawie przyjęcia programu rozwoju „Program Zintegrowanej Informatyzacji Państwa", www.mac.gov.pl, s. 20–21.

mu TERYT (tj. katalogu jednostek terytorialnych kraju, miejscowości i ulic), zasobów dziedzictwa kulturowego.

W kolejnych latach katalog usług e-administracji był – i jest nadal – sukcesywnie poszerzany. Według stanu z 2019 r., przy realizacji programu „Od papierowej do cyfrowej Polski", którego celem jest poprawa funkcjonowania i lepsze wykorzystanie infrastruktury publicznej, bardziej efektywne wypełnianie swoich funkcji przez państwo oraz zapewnienie warunków do rozwoju innowacyjnej i konkurencyjnej gospodarki, wydzielono dziewięć strumieni roboczych obejmujących działania związane z informatyzacją przestrzeni publicznej[32]. Były to szczegółowe programy strategiczne dotyczące: optymalizacji systemu cyfrowych usług publicznych, e-sprawozdawczości, integracji rejestrów rozproszonych (w ramach technologii blockchain), e-transportu i e-przepływów (m.in. koordynacji zarządzania ruchem i pobierania opłat oraz udrożnienia łańcucha dostaw i standaryzacji wymiany danych transportowych i celnych), zwiększenia obrotu bezgotówkowego, e-faktur i e-paragonów, e-edukacji (stworzenia i upowszechnienia narzędzi informatycznych poprawiających efektywność procesu kształcenia dzieci i młodzieży, seniorów, osób niepełnosprawnych), sztucznej inteligencji oraz internetu rzeczy (IoT). Strumień sztuczna inteligencja obejmuje zintegrowane działania z zakresu gospodarki opartej na danych, finansowania badań i rynku, edukacji oraz etyki i praw człowieka, w tym związane z budową w Ministerstwie Cyfryzacji roboczej platformy wspomagającej w tej dziedzinie synergię międzysektorową. Strumień internet rzeczy ma na celu wypracowywanie regulacji usuwających bariery prawne blokujące rozwój gospodarki w obszarze technologii IoT i wzmacniających współpracę przedsiębiorstw.

W różnej fazie realizacji znajdowały się też programy mieszczące się w wyodrębnionych strumieniach przedmiotowych. Podstawowe znaczenie miały działania dotyczące tożsamości cyfrowej (związane z identyfikacją i uwierzytelnieniem obywateli w administracji publicznej i usługach), architektury IT, e-zdrowia i cyberbezpieczeństwa. Jednym z liderów cyfryzacji usług i rejestrów oraz procedur stał się Zakład Ubezpieczeń Społecznych.

W 2019 r. dowód osobisty z warstwą elektroniczną w postaci bezstykowego chipa, czyli e-dowód, miało już ponad milion obywateli. E-dowód otwiera drogę do komunikowania się elektronicznie z administracją publiczną (w tym zalogowania się do ePUAP), elektronicznego podpisywania dokumentów oraz umożliwia korzystanie z wielu innych elektronicznych procedur w przestrzeni publicznej[33]. Niestety, szybko okazało się, że polskie rozwiązanie nie spełnia standardów Unii Europejskiej, co spowodowało, iż niedługo po jego wprowa-

[32] https://www.gov.pl/web/cyfryzacja/od-papierowej-do-cyfrowej-polski.

[33] http://centrumprasowe.pap.pl/cp/pl/news/info/144866,36,mc-ponad-milion-polakow-ma-e-dowod-co-zrobic-aby-go-zdobyc-(komunikat).

dzeniu trzeba było podjąć prace nad wdrożeniem rozporządzenia Parlamentu Europejskiego i Rady UE ustalającego zasadę pobierania od wnioskodawcy odcisków palców w celu zapisania ich w warstwie elektronicznej dokumentu. Ten przykład dowodzi, jak ważne jest koordynowanie projektów w obszarze e-administracji.

Dane statystyczne pokazują, że e-administracja znajduje w Polsce coraz szersze zastosowanie w praktyce. Według informacji Ministerstwa Cyfryzacji, w 2019 r. w Polsce nastąpiło znaczne przyspieszenie zakładania profilu zaufania (PZ), który stanowi „bramę wejściową" do korzystania z licznych e-usług publicznych. Profil ten został udostępniony w 2011 r. Do 2016 r. korzystało z niego około 400 tysięcy osób, w końcu 2019 r. miało go już ponad 4,7 miliona obywateli, z których ponad 2,1 miliona założyło sobie PZ w tymże roku. Ponadto, w 2019 r.: ponad 160 tysięcy osób złożyło przez internet wniosek o nowy dokument tożsamości, ponad 45 tysięcy osób zgłosiło narodziny dziecka, ponad 63 tysiące skorzystało z e-usługi umożliwiającej zameldowanie lub wymeldowanie się, ponad 533 tysiące skierowało w trybie elektronicznym pismo do urzędu administracji publicznej, a ponad 129 tysięcy skorzystało z cyfrowej usługi umożliwiającej sprawdzenie historii pojazdu[34].

Przydatność e-administracji potwierdziła się w pierwszej połowie 2020 r., w okresie wprowadzania ograniczeń bezpośrednich kontaktów w związku z pandemią koronawirusa. Internet, jak obrazowo to ujął komentator politico.eu, stał się w tych warunkach tak samo ważny jak woda i energia elektryczna. Także w Polsce nastąpiło wówczas przyspieszone testowanie rozwiązań e-administracji. Wypracowywane były zasady i procedury przenoszenia niektórych działań do świata wirtualnego, przechodzenia z trybu stacjonarnego w tryb zdalny. Rozwój e-learningu i innych form nauczania zdalnego potwierdził możliwości tkwiące w komunikacji elektronicznej, ale równocześnie jeszcze wyraźniej uwypuklił ograniczenia w dostępie do szerokopasmowych łączy internetowych oraz pociągnął za sobą nieuniknione koszty awaryjnego wdrażania rozwiązań bez możliwości ich wcześniejszego praktycznego sprawdzenia. Odbywała się też przyspieszona nauka interaktywnego komunikowania za pomocą łączy elektronicznych. Nieoczekiwanie pojawiła się więc szansa podniesienia kompetencji społecznych w zakresie komunikacji elektronicznej. W tym sensie pandemia przyniosła także pozytywne skutki. Dla dużej grupy osób takie rozwiązania, jak elektroniczna recepta, elektroniczny kontakt z administracją skarbową czy ZUS-em stały się oczywiste i naturalne. Można zasadnie przewidywać, że nowe formy elektronicznych kontaktów w wielu sprawach wejdą na trwałe do komunikacji między obywatelami i podmiotami

[34] http://centrumprasowe.pap.pl/cp/pl/news/info/152473,36,mc-ach-co-to-byl-za-rok%E2%80%A6-e-uslugowe-podsumowanie-2019!

administracji publicznej. Z informacji podanych przez Ministerstwo Cyfryzacji wynika, że sfera e-usług publicznych dynamicznie się rozwija; tylko w maju 2020 r. założono niemal 360 tysięcy nowych profili zaufanych (to jest pięć razy więcej niż w maju poprzedniego roku), w trybie elektronicznym skierowano prawie 130 tysięcy pism o charakterze ogólnym do instytucji publicznych, ponad 51 tysięcy osób zgłosiło przez internet zbycie lub nabycie pojazdu, ponad 31 tysięcy – złożyło drogą internetową wniosek o nowy dowód osobisty, ponad 20 tysięcy – wystąpiło o wystawienie odpisu aktu stanu cywilnego, ponad 18 tysięcy – skorzystało z e-usług meldunkowych[35]. Masowe sięganie po narzędzia e-administracji znajduje też potwierdzenie w informacji Ministerstwa Finansów, zgodnie z którą do 30 kwietnia 2020 r. w ramach rozliczenia PIT za rok poprzedni złożono elektronicznie ponad 18,3 miliona deklaracji (na około 20,9 miliona PIT-ów złożonych w tym czasie). Na uwagę zasługuje fakt, że około 8,7 miliona deklaracji złożono poprzez usługę Twój e-PIT, w tym 3,8 miliona razy skorzystano z automatycznego rozliczenia dostępnego w tej usłudze[36].

Dla zapewnienia dostępu do zintegrowanej informacji publicznej – kwestii kluczowej w cywilizacji cyfrowej – istotne znaczenie miało stworzenie mechanizmów Biuletynu Informacji Publicznej, Centralnego Repozytorium Informacji Publicznej i rejestrów publicznych. W ustawach określono różne tryby dostępu. Jako podstawową zasadę przyjęto uzyskiwanie dostępu do informacji publicznej bez składania wniosku. Udostępnianie większości tych informacji odbywa się poprzez: ogłaszanie w Biuletynie Informacji Publicznej (urzędowym publikatorze teleinformatycznym, mającym postać ujednoliconego systemu stron w sieci informatycznej); wyłożenie lub wywieszenie w miejscach ogólnie dostępnych i przez zainstalowane w tych miejscach urządzenia; wstęp obywateli na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów i udostępnianie materiałów, w tym audiowizualnych i teleinformatycznych, dokumentujących te posiedzenia; zamieszczanie w centralnym repozytorium. W przypadku pozostałych informacji udostępnianie następuje na wniosek osoby zainteresowanej (na zasadach określonych oddzielnie w ustawie, pod warunkiem że informacja nie została już wcześniej udostępniona w Biuletynie Informacji Publicznej lub centralnym repozytorium, a także nie podlega wyłączeniu z udostępniania na podstawie przepisów ustawy). Z myślą o dostępie do informacji tworzone są liczne rejestry publiczne. Centralne repozytorium jest prowadzone przez ministra właściwego do spraw informatyzacji. Repozytorium jest powszechnie dostępne w sieci teleinformatycznej i zapewnia przeszukiwanie zasobów infor-

[35] https://www.gov.pl/web/cyfryzacja/e-uslugowe-podsumowanie-maja.

[36] https://www.polsatnews.pl/wiadomosc/2020-06-03/nowy-rekord-183-mln-deklaracji-pit-zlozono-elektronicznie/?ref=kafle.

macyjnych według kryterium przedmiotowego i podmiotowego oraz według wybranych elementów metadanych (repozytorium nie obejmuje informacji zawartych w centralnej bazie danych ksiąg wieczystych, Krajowym Rejestrze Karnym, Krajowym Rejestrze Sądowym, elektronicznym katalogu dokumentów spółek, rejestrze zastawów). Istotne jest, że odmowa udostępnienia informacji publicznej i inne rozstrzygnięcia w tych sprawach następują w drodze decyzji administracyjnej i mają do nich zastosowanie przepisy Kodeksu postępowania administracyjnego, zaś do skarg rozpatrywanych w postępowaniach o udostępnienie informacji publicznej stosuje się przepisy ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi[37]. Ustawa stanowi też, że kto, wbrew ciążącemu na nim obowiązkowi, nie udostępnia informacji publicznej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. W sposób odrębny uregulowano w ustawie sprawy ponownego wykorzystywania informacji publicznej.

Nowe technologie cyfrowe decydują o innowacyjności i konkurencyjności gospodarki. Stopień i sposób ich wykorzystania w sektorze publicznym i obrocie gospodarczym jest probierzem rozwoju społeczno-gospodarczego państwa. Program „Od papierowej do cyfrowej Polski", prowadzony przez Ministerstwa: Rozwoju, Cyfryzacji, Finansów, Infrastruktury oraz Edukacji Narodowej, zmierza do rozwoju e-państwa i cyfryzacji gospodarki. Wpisuje się on w Plan na rzecz Odpowiedzialnego Rozwoju, który zakłada, że nowoczesna e-administracja jest koniecznym elementem sprawnego państwa i zrównoważonego rozwoju.

Powodzenie we wdrażaniu systemu e-administracji jest równoznaczne z ułatwieniem dostępu do cyfrowych informacji i usług państwa. W Polsce, mimo pozytywnych zmian zachodzących w tej dziedzinie w ostatnim czasie, nadal istnieją przeszkody w korzystaniu z zasobów i usług elektronicznych państwa. Przyczynia się do tego m.in.: brak spójności prezentowanych treści, ich zróżnicowana jakość i dostępność cyfrowa, duża czasochłonność i trudność odnajdywania informacji, trudny język używany w wielu informacjach lub opisach usług, niedostateczne dostosowanie rozproszonych systemów do potrzeb osób z niepełnosprawnościami. W tej sytuacji istotne znaczenie ma projekt utworzenia jednego adresu internetowego (www.gov.pl), z którego mogą być uruchamiane kontakty elektroniczne obywatela i przedsiębiorcy z państwem. Realizacja tego projektu jest obecnie znacznie zaawansowana. Docelowo portal www.gov.pl będzie też pełnił funkcję katalogu wszystkich usług, informacji i podmiotów administracji publicznej. Na ten portal zostały już przeniesione strony ministerstw oraz Kancelarii Prezesa Rady Ministrów. Połączono w nim serwisy Biuletynu Informacji Publicznej i strony www. W następnych

[37] Dz.U. z 2012 r., poz. 270 z późn. zm.

latach mają go zasilić strony urzędów centralnych i wojewódzkich. Wartością tworzonego portalu jest jednoznaczna i spójna identyfikacja treści publikowanych przez administrację rządową oraz łatwość dostępu do tych treści[38]. W marcu i kwietniu 2020 r. portal www.gov.pl odwiedziło niemal 46 milionów osób. Kolejne 12,5 miliona (unikalnych użytkowników) odwiedziło go w maju 2020 r.[39].

W innych fragmentach książki zwracam uwagę na problemy, jakie powstają w związku z uruchamianiem elektronicznych procedur administracyjnych. Przede wszystkim chodzi tu o występowanie klasycznego konfliktu wartości: po jednej stronie stoją takie wymagające ochrony wartości, jak integralność i bezpieczeństwo danych gwarantowane obywatelom, po drugiej – fundamentalne wartości: wolność i prawo do prywatności każdej jednostki. Poważnym problemem – już nie etycznym, jak w przypadku konfliktu wartości, lecz praktycznym – są zagrożenia bezpieczeństwa i integralności danych zgromadzonych w elektronicznych zasobach informacji oraz zakłócenia w funkcjonowaniu systemów informatycznych. Na przykład, z powodu zakłóceń w dostępie do Systemów Rejestrów Państwowych, które wystąpiły 22 stycznia 2020 r., blokując pracę licznych urzędów państwowych, przez kilka godzin nie można było załatwić w urzędach gmin rozmaitych spraw obywatelskich, takich jak wydawanie dowodów osobistych czy odpisów aktów stanu cywilnego; nie działały też niektóre rejestry państwowe, m.in. Centralna Ewidencja Pojazdów i Kierowców[40].

Niebezpieczeństwa pojawiające się w związku z rozwojem różnych nowych programów i narzędzi e-administracji nie omijają także Polski. Ujawniły się one w czasie walki z pandemią w 2020 r., kiedy włączono narzędzia elektroniczne do działań mających ograniczyć liczbę zakażeń, a do sfery online przeniesiono dużą część aktywności zawodowej i życiowej milionów Polaków.

Jako przykład programu cyfrowego nastręczającego poważne wątpliwości co do sposobu jego wykorzystania może posłużyć uruchomiona w czasie epidemii aplikacja ProteGO Safe, która ma wspomagać identyfikację kontaktów ludzi zagrożonych zakażeniem koronawirusem na podstawie analizy ich smartfonów. Rząd namawia do powszechnego wpisywania do swoich urządzeń tego programu. Aplikacja rejestruje kontakty telefoniczne w ciągu ostatnich 14 dni. Na podstawie historii aktywności poszczególnych osób korzystających z telefonów komórkowych aplikacja, za pomocą specjalnie stworzonych algorytmów, jest w stanie wychwycić i ocenić kontakty, które mogą stanowić

---

38 https://www.gov.pl/web/cyfryzacja/portal-gov-pl.

39 Zob.: raport *Cyfryzacja podczas pandemii – innowacje, bezpieczeństwo, e-administracja. Wybrane działania Ministerstwa Cyfryzacji*, marzec–wrzesień 2020, https://www.gov.pl/web/cyfryzacja/cyfryzacja-podczas-pandemii; https://www.gov.pl/web/cyfryzacja/e-uslugowe-podsumowanie-maja.

40 https://businessinsider.com.pl/wiadomosci/awaria-dostepu-do-rejestrow-panstwowych/ehe8dcm.

zagrożenie dla tych osób, i daje im sygnały w tej sprawie w postaci komunikatu przekazywanego w poczcie smartfonu. Aplikacja ta może też być pomocna w przeprowadzaniu wywiadu epidemiologicznego przez służby sanitarne, co – nawiasem mówiąc – wiąże się z podniesieniem poziomu ich ucyfrowienia. Osoby zakażone dostają specjalny kod pozwalający im uruchomić system powiadamiania wszystkich osób, z którymi miały kontakt w okresie podlegającym monitorowaniu. Jak zauważył minister cyfryzacji, ma to znaczenie nie tylko dla zdrowia danej osoby, lecz także dla stanu zdrowia publicznego, gdyż „bardziej efektywnie pomoże identyfikować osoby, które wymagają wsparcia i nadzoru sanitarnego", a „czym bardziej jesteśmy precyzyjni we wskazywaniu osób zakażonych, w typowaniu osób do testów – tym jesteśmy skuteczniejsi w panowaniu nad pandemią"[41].

Społeczna użyteczność tej aplikacji nie podlega dyskusji. Zapewnienia jej autorów, że ochrona prywatności użytkowników jest ich priorytetem, zaś program nie obejmuje utrwalania geolokalizacji, a jedynie rejestruje fakt kontaktu, i że korzystanie z tej aplikacji jest dobrowolne i zdecentralizowane, nie rozwiewają niepokoju i obaw, które utrzymują się zwłaszcza w środowisku obrońców praw człowieka. Daje tu o sobie znać ograniczone zaufanie do władz publicznych (nawiasem mówiąc, Polaków charakteryzuje rekordowo niski poziom zaufania społecznego – przodujemy pod tym względem w europejskich rankingach), co znajduje wyraz w przeświadczeniu, że władze zechcą wykorzystać to rozwiązanie do inwigilacji obywateli także w sprawach niezwiązanych z koronawirusem, i w braku wiary w to, iż są one w stanie zagwarantować bezpieczeństwo danych utrwalonych za pomocą omawianej aplikacji. Trzeba jednak dodać, że wiary w bezpieczeństwo danych z pewnością nie umacniają takie zdarzenia, jak pojawienie się w internecie w kwietniu 2020 r. danych adresowych około 300 osób z powiatu gnieźnieńskiego, które zostały poddane kwarantannie w związku z podejrzeniem zakażenia koronawirusem[42]. Nieufność wzmagają także ujawnione przez fundację Panoptykon (badającą m.in. elektroniczne formy nadzoru nad społeczeństwem) informacje mówiące o tym, że już 24 marca 2020 r., w początkowej fazie epidemii, premier, powołując się na przepisy ustaw związanych z ograniczaniem epidemii, wydał operatorom telefonii komórkowej polecenie przekazywania służbom i wojewodom danych lokalizacyjnych telefonów, które należą do osób znajdujących się w nadzorze epidemiologicznym, kwarantannie, hospitalizacji lub izolacji[43].

---

41 https://biznes.interia.pl/gospodarka/news-minister-cyfryzacji-dla-interii-aplikacja-protego-safeto-ni,nId,4521358.

42 https://www.polsatnews.pl/wiadomosc/2020-04-19/adresy-przebywajacych-na-kwarantannie-trafily-do-sieci-sprawe-bada-prokuratura/?ref=slider.

43 https://www.rp.pl/Koronawirus-SARS-CoV-2/200419545-Do-rzadu-poplynal-strumien-danych-o-lokalizacji-osob-poddanych-kwarantannie.html.

Społeczeństwo odniosło się do aplikacji ProteGO Safe z dużą rezerwą, o czym świadczy fakt, że w połowie października 2020 r., a więc już po kilku miesiącach od jej udostępnienia, tylko 2,6% mieszkańców Polski zainstalowało ją w swoich telefonach. Tym samym ProteGO Safe jest praktycznie bezużyteczna dla identyfikacji kontaktów osób zakażonych, gdyż – jak oceniają specjaliści – przydatność takiego narzędzia jest uzależniona od minimum kilkunastoprocentowego udziału wszystkich abonentów w systemie monitorowania kontaktów za jego pomocą. Na marginesie trzeba zauważyć, że podobna aplikacja (Corona-Warn-App) została zainstalowana w Niemczech przez około 22% abonentów telefonów komórkowych[44].

10.4. E-governance: mechanizm wykorzystania możliwości technologii cyfrowej w sferze politycznej

Przydatność narzędzi cyfrowych w kluczowych sferach aktywności podmiotów funkcjonujących w sferze publicznej • Możliwości optymalizacji działań i niebezpieczeństwa związane z wykorzystywaniem narzędzi cyfrowych w przestrzeni publicznej • Brak oznak szybkiego wprowadzenia w Polsce mechanizmów cyfrowych do procesów legitymizacji politycznej

Cyfrowe technologie komputerowe i komunikacyjne stają się w państwach rozwiniętych narzędziami wspomagającymi nie tylko administrację publiczną, lecz także procesy rządzenia i decydowania publicznego. Rozwiązania inteligentnej technologii cyfrowej znajdują zastosowanie we wszystkich obszarach aktywności podmiotów funkcjonujących w sferze publicznej, w tym aktywności politycznej. Tworzą nowe możliwości zdobywania informacji i zarządzania zbiorami danych, programowania działań, zarządzania sprzecznościami (np. sprzecznościami wartości, interesów), uzyskiwania synergii wewnątrzsystemowej, udoskonalania implementacji, komunikacji społecznej i ewaluacji.

Wiele przykładów pokazuje, że zastosowanie narzędzi cyfrowych zwiększa efektywność działania organów publicznych, przyczynia się do rozwoju demokracji partycypacyjnej, obniża koszty funkcjonowania państwa i jego struktur. Obecnie kładzie się więc duży nacisk na kształtowanie infrastruktury systemowej państwa cyfrowego (Digital State). W literaturze podejmuje się próby opisu kolejnych, coraz bardziej zaawansowanych wersji e-państwa (od modelu Government 1, w którym nowe rozwiązania wiążą się głównie z funkcjonowaniem administracji, po model Government 3, w którym cyfry-

[44] P. Szostak, *ProteGo Safe wciąż w niszy*, „Gazeta Wyborcza" z 22 października 2020, s. 16.

zacji, w układzie partycypacyjnym, podlegają już liczne relacje społeczne)[45]. Ograniczenia bezpośrednich kontaktów spowodowane pandemią koronawirusa wymusiły szybkie – niejednokrotnie dokonywane w sytuacjach alarmowych – przenoszenie się aktywności organów publicznych do internetu. Na tryb zdalny w działaniu, w tym także w podejmowaniu decyzji, przechodziły w pierwszej połowie 2020 r. organy instytucji międzynarodowych, parlamenty, gabinety ministrów oraz organy władzy regionalnej i lokalnej. Należy przypuszczać, że w wielu przypadkach z tych rozwiązań, jako procedur nadzwyczajnych, władze publiczne zrezygnują z chwilą ustania zagrożeń, które wymusiły ich zastosowanie. Być może jednak w jakiejś części będą one – w uzupełnionej i poprawionej wersji – utrzymane w przyszłości.

Osiągnięcie pozytywnych rezultatów w budowaniu systemu e-governance wymaga spełnienia pewnych warunków. Z doświadczeń zebranych w różnych państwach jasno wynika, że projekty cyfrowej transformacji (*digital transformation*) muszą uwzględniać całościowo ujęte funkcje i struktury państwa. Nowe rozwiązania cyfrowe muszą się też wpisywać w mechanizmy rozwoju partycypacji obywatelskiej w przestrzeni publicznej. Trzeba zdecydowanie odejść od traktowania obywatela przede wszystkim jako „klienta administracji"[46].

Trzeba też dostrzegać, że z wykorzystywaniem narzędzi cyfrowych w przestrzeni publicznej i politycznej państwa wiążą się nie tylko dodatkowe możliwości optymalizacji działań, lecz także pewne niebezpieczeństwa. Jeśli projekt elektronicznej demokracji ma nieść pozytywne skutki, niezbędne jest stworzenie skutecznych i efektywnych mechanizmów wzmacniających odpowiedzialność w sferze e-polityki, bowiem przenoszeniu do internetu różnych form aktywności politycznej towarzyszą patologiczne zjawiska i procesy, o których wspominałem w poprzednich fragmentach książki. Nasila się walka polityczna w cyberprzestrzeni, przybierająca nieraz formę kampanii nienawiści, co wzmacnia podziały w społeczeństwie i utrudnia realizację dobra wspólnego. Zaostrza się, czy wręcz brutalizuje, język polityczny. Aktorzy sceny politycznej działają niejednokrotnie anonimowo, pod osłoną fałszywej tożsamości. Robią to w poczuciu bezkarności, nie zważając na poprawność polityczną, a fake newsy, memy, posty i komentarze internetowe (często obraźliwe, nasycone niewybrednym słownictwem, zawierające treści zabronione prawem) są tego widomym świadectwem; w wielu wypadkach wygląda to tak, jak gdyby nie działały tu żadne wewnętrzne hamulce. Obrazu sytuacji dopełnia fakt, że przybiera na sile lobbing polityczny w przestrzeni internetowej, w dużej mierze nadal nieuporządkowany. Podsumowując powyższy opis, wypada powtórzyć

[45] Zob. M. Kowalczyk, *Cyfrowe Państwo…*, s. 242 i nast.

[46] Zob.: A. Sobczak, *Wizja Cyfrowego Państwa*; M. Kowalczyk, *Cyfrowe Państwo…*, s. 10 i nast.

znaną tezę, że w świecie polityki (zwłaszcza świecie internetowym) wizerunki medialne i emocje stają się ważniejsze niż twarde fakty i racje rozumowe.

Zawsze należy się liczyć z niebezpieczeństwem nagannego wykorzystywania cyfrowych zbiorów danych do celów politycznych. Z drugiej jednak strony trzeba mieć świadomość, że – pod pewnymi warunkami – te zbiory danych mogą być wielką wartością w polityce. Przy okazji konferencji zorganizowanej w 2017 r. przez ONZ i Międzynarodowe Stowarzyszenie Profesjonalistów ds. Prywatności podkreślono, że „Duże zbiory danych, nowe technologie i nowe podejścia analityczne, jeśli są stosowane w sposób odpowiedzialny, mają ogromny potencjał do wykorzystania dla dobra publicznego. Największa wartość dużych zbiorów danych dla globalnego rozwoju polega na wykorzystaniu siły analityki predykcyjnej w czasie rzeczywistym do mądrzejszego podejmowania decyzji, wyprzedzającego podejścia do zarządzania ryzykiem oraz nowych sposobów pomiaru wpływu społecznego”[47]. Jak czytamy w zaleceniach OECD w sprawie strategii administracji cyfrowej, wartość technologii cyfrowych w rządzeniu polega na tym, że można dzięki nim pójść w kierunku rządów bardziej otwartych, partycypacyjnych, innowacyjnych i prowadzących spójne działania[48]. W enuncjacjach OECD dotyczących tych kwestii wskazuje się na możliwość i potrzebę używania narzędzi cyfrowych do poprawy rozliczalności rządu, wzmocnienia partnerstwa społecznego, tworzenia w sektorze publicznym kultury opartej na danych, poprawy jakości działań we wszystkich obszarach polityki i na różnych szczeblach administracji, wzmocnienia więzi między administracją i programami zarządzania publicznego, kształtowania zdolności instytucjonalnych do zarządzania i monitorowania realizacji projektów oraz zarządzania ryzykiem, w tym ryzykiem sytuacji krytycznych[49].

Warunkiem właściwego spożytkowania zdolności cyfrowych w rządzeniu jest jasne określenie celów i monitorowanie wyników oraz stworzenie ram regulacyjnych i prawnych pozwalających nie tylko wykorzystać nowe możliwości, lecz także ograniczyć związane z nimi ryzyko (takie jak naruszenie bezpieczeństwa i prywatności). Zdaniem OECD, rządzenie cyfrowe tworzy warunki sprzyjające wartościom publicznym i trwałemu rozwojowi. Kluczowe znaczenie przypisuje się w tym przypadku zapewnieniu otwartości rządu, gdyż jest to niezbędny warunek zaufania publicznego potrzebnego do zaangażowania społeczeństwa we współtworzenie wartości publicznych.

Przykłady zaczerpnięte z praktyki politycznej innych państw, które przywołałem we wcześniejszych fragmentach książki, pokazują, że niebezpieczeństwa

---

47 https://iapp.org/resources/article/building-ethics-into-privacy-frameworks-for-big-data-and-ai.

48 http://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm.

49 *Recommendation of the Council on Digital Government Strategies*, OECD 2014, www.oecd.org/governance.

związane z posługiwaniem się narzędziami cyfrowymi w przestrzeni publicznej można odnieść także do aktywności organów władzy państwowej i sił politycznych uczestniczących w wykonywaniu władzy politycznej. I bynajmniej nie chodzi tu tylko o działania władz w państwach niedemokratycznych. Niebezpieczeństwa te występują także w państwach demokratycznych, często stojących przed koniecznością wyboru między ochroną wolności i wymogami bezpieczeństwa, a sprowadzają się one głównie do nadużywania nowych możliwości nadzoru państwa nad obywatelami. Dotyczy to także prób stosowania rozwiązań cyfrowych do celów ściśle politycznych związanych z kształtowaniem stosunków władczych w przestrzeni publicznej. W tej dziedzinie władza uzyskuje zdolność inwigilacji na niespotykanym poprzednio poziomie – za sprawą stale doskonalonych narzędzi niejawnego przechwytywania informacji pojawiających się w przestrzeni cyfrowej, ustalania lokalizacji, niejawnej obserwacji i analizy zdjęć i rozmów, m.in. za pomocą narzędzi rozpoznawania wizerunków i głosu. W tej sytuacji, przedmiotem sporów – i to dość gorących – stała się kwestia celów, granic i zasad wykorzystywania tych nowych możliwości nadzoru. Operowanie na dużych zbiorach danych, jeśli nie będzie oparte na jasnych regułach i wysokich standardach etycznych, niesie ze sobą ryzyko naruszenia prywatności, uczciwości i równości, a w efekcie może prowadzić do stronniczego podejmowania decyzji i pozbawiania ludzi oraz podmiotów pozarządowych praw procesowych. Z tych powodów czynnik etyczny musi być uwzględniony we wszystkich projektach przewidujących włączenie narzędzi cyfrowych do procesów decyzyjnych w przestrzeni publicznej[50].

Cyfryzacja procedur politycznych lub też mających znaczenie polityczne, które można zaliczyć do sfery rządzenia (governance), odbywa się oczywiście także w Polsce. Objęto nią przede wszystkim programowanie i ewaluację polityk publicznych, w mniejszym stopniu zaś procesy decyzyjne w przestrzeni publicznej. W ograniczonym zakresie sięga się w Polsce po narzędzia komunikacji cyfrowej w kształtowaniu decyzji wewnątrz poszczególnych podmiotów politycznych. Warto też zaznaczyć, że temat zastosowania narzędzi internetowych bezpośrednio w etapie podejmowania decyzji w instytucjach publicznych nie mieści się obecnie w Polsce w głównym nurcie debaty politycznej. Pojawiające się w tej sprawie opinie nie wykraczają poza odniesienia do bieżącej gry politycznej.

Obserwując działania na dzisiejszej scenie politycznej, można dojść do wniosku, że partie polityczne i sami politycy często wykorzystują cyfrowe narzędzia zindywidualizowanej komunikacji masowej do wzmacniania i orga-

[50] https://iapp.org/resources/article/building-ethics-into-privacy-frameworks-for-big-data-and-ai/. Tam zob. m.in. przegląd najlepszych praktyk w zakresie bezpieczeństwa i prywatności dużych zbiorów danych.

nizowania zwolenników oraz atakowania swoich adwersarzy[51]. Narzędzi elektronicznych używa się do prognozowania preferencji i zachowań politycznych społeczeństwa. Trudno natomiast znaleźć w Polsce przykłady sięgania do rozwiązań cyfrowych na użytek politycznej legitymizacji. Zamieszczone latem 2019 r. na stronie Platformy Obywatelskiej wezwanie, aby Polska wprowadziła – idąc śladem zachodnich demokracji – formę elektronicznego głosowania, nie miało znamion przemyślanego projektu (nawiasem mówiąc, zawierało nieprawdziwą informację, jakoby ta forma była powszechnie stosowana w tych państwach).

Sprawy możliwości i granic wykorzystywania narzędzi elektronicznych w dziedzinach tak ważnych dla polityki, jak legitymizacja władz publicznych, w tym kwestie dotyczące elektronicznego głosowania w wyborach organów władzy publicznej oraz elektronicznych form demokracji bezpośredniej, podejmuję szerzej w następnym rozdziale. W tym miejscu jednak warto już zauważyć, że w Polsce obecnie można dostrzegać raczej przeszkody w sięganiu do rozwiązań cyfrowych w procesach politycznej legitymizacji niż próby wpisywania tych rozwiązań w projekty regulacji odnoszących się do wyborów, referendów, a nawet do zasad funkcjonowania organów kolegialnych władzy publicznej. Blokady istnieją nie tylko w obszarze regulacji normatywnych, lecz także – co wydaje się ważniejsze – w sferze świadomości społecznej. Znajduje to odbicie w programach polskich partii politycznych, a właściwie w braku w owych programach postulatu wprowadzenia mechanizmów demokracji elektronicznej.

W Polsce w wyborach organów władzy publicznej korzysta się z technik i narzędzi elektronicznych w ograniczonym zakresie, zwykle pełnią one rolę pomocniczą. Co więcej, wydaje się, że w najbliższych latach niewiele się w tej sprawie zmieni i model głosowania przez internet nie znajdzie zastosowania. Decyduje o tym przede wszystkim siła oporu społecznego wynikającego z przekonania, że nie jest możliwe wyeliminowanie niebezpieczeństwa ingerencji w elektroniczny system wyborczy lub awarii tego systemu. Była już o tym mowa – Polak jest z natury nieufny i skłonny do snucia scenariuszy spiskowych… Ale abstrahując od naszego charakteru narodowego, trzeba podkreślić, że negatywne opinie o głosowaniu elektronicznym dochodzą z różnych stron. Na przykład Wojciech Orliński w swoim komentarzu do kłopotów z systemem głosowania za pomocą aplikacji wyborczej na smartfony, które ujawniły się w USA w lutym 2020 r. w czasie wyłaniania przez Demokratów swojego kandydata na prezydenta, stwierdził: „Jest chyba tylko jedna rzecz, która w polskiej polityce przeraża mnie bardziej od PiS – to wracające co chwilę

[51] Zob. A. Stoppel, *Nowe media w polityce na przykładzie kampanii prezydenckich w Polsce w latach 1995–2015*, Poznań 2019.

propozycje wprowadzenia głosowania przez internet", i dodał: „Wszystkie problemy, które miałoby rozwiązać głosowanie przez internet, da się lepiej i taniej rozwiązać metodami nietechnologicznymi"[52].

W polskim prawie wyborczym brakuje niezbędnego odniesienia do aktywności politycznej w cybersferze. Potwierdził to wyraźnie sędzia Wojciech Hermeliński, były przewodniczący Państwowej Komisji Wyborczej, który przyznał, że prawo to „nie reguluje kampanii wyborczej w internecie, zatrzymało się na epoce papieru". Jednocześnie wyraził pogląd, że „manipulacja wyborami za pomocą internetowych narzędzi jest wielkim współczesnym zagrożeniem" i że jest to „bezpośrednie zagrożenie wolności wyborów", gdyż wyborca „zmanipulowany nie dokonuje świadomego wyboru, na którym polega istota demokracji przedstawicielskiej"[53].

Zgodnie z uchwałą Państwowej Komisji Wyborczej ogłoszoną przed wyborami do Sejmu i Senatu w 2019 r., pomocnicze wykorzystanie techniki elektronicznej nie zastępuje ręcznego liczenia głosów przez obwodowe komisje wyborcze oraz konieczności porównania przez okręgowe komisje wyborcze danych zawartych w systemie informatycznym z dostarczonymi protokołami głosowania w obwodzie. Informatyczne wspomaganie organów wyborczych obejmuje wprowadzenie, przechowywanie i weryfikowanie danych, przygotowanie formularzy i dokumentów do drukowania oraz drukowanie tych formularzy i dokumentów[54]. Wszystko to jednak są działania uzupełniające, a nie zastępujące poszczególne działania związane z procesem wyborczym. Podobne zasady zostały przyjęte w wyborach Prezydenta RP w 2020 r.[55]. W wywiadzie prasowym udzielonym w czerwcu 2020 r. Marek Zagórski, ówczesny minister cyfryzacji, poinformował, że w Polsce nie są prowadzone prace nad ewentualnym głosowaniem przez internet[56]. Stwierdził, że wybory prezydenckie lub parlamentarne dopuszczające oddawanie głosu przez internet, przy wykorzystaniu środków zdalnej identyfikacji, wymagałyby specjalnego, całkiem nowego systemu znajdującego się pod pełną kontrolą państwa, na które-

---

52 W. Orliński, *Trump wygrał wśród Demokratów*, „Gazeta Wyborcza" z 8–9 lutego 2020, s. 23.

53 *Może jestem naiwny*, rozmowa E. Siedleckiej z W. Hermelińskim, „Polityka" 2019, nr 21 (3211), s. 31. Zob. też J. Zbieranek, *Alternatywne procedury głosowania w polskim prawie wyborczym – gwarancja zasady powszechności wyborów czy mechanizm zwiększania frekwencji wyborczej?*, Warszawa 2013.

54 Uchwała nr 87/2019 Państwowej Komisji Wyborczej z dnia 12 sierpnia 2019 r. w sprawie warunków oraz sposobu pomocniczego wykorzystania techniki elektronicznej w wyborach do Sejmu Rzeczypospolitej Polskiej i do Senatu Rzeczypospolitej Polskiej zarządzonych na dzień 13 października 2019 r., M.P. z 2019 r., poz. 785.

55 Uchwała nr 162/2020 Państwowej Komisji Wyborczej z dnia 8 czerwca 2020 r. w sprawie warunków oraz sposobu pomocniczego wykorzystania techniki elektronicznej w wyborach Prezydenta Rzeczypospolitej Polskiej zarządzonych na dzień 28 czerwca 2020 r., M.P. z 2020 r., poz. 522.

56 https://biznes.interia.pl/gospodarka/news-minister-cyfryzacji-dla-interii-aplikacja-protego-safeto-ni,nId,4521358.

go przygotowanie potrzeba co najmniej kilkunastu miesięcy, oraz niosłyby ze sobą gigantyczne koszty. Wyraził też opinię, że takie wybory to „bardzo skomplikowane rozwiązanie, nigdy niedające pełnej gwarancji bezpieczeństwa. Poza bezpieczeństwem trzeba zapewnić anonimowość oraz niezaprzeczalność wyniku wyborczego". Zaznaczył, że w tej sprawie byłaby potrzebna zgoda społeczna i polityczna. Nie wykluczył jednak w przyszłości głosowania elektronicznego w lokalach, które przyspieszyłoby liczenie głosów.

W trakcie kampanii wyborczych w Polsce obywatele nie korzystają masowo z internetu w związku z wyborami. Narzędzia internetowe są używane w procesach artykulacji, agregacji i legitymizacji politycznej w ograniczonym zakresie. W istocie dotyczy to obecnie tylko informacji i promocji wyborczej. Wyjątkiem są mechanizmy uruchamiane na poziomie samorządu terytorialnego, m.in. w ramach kształtowania tzw. budżetów obywatelskich. Równocześnie z badań CBOS wynika, że nieznacznie wzrasta znaczenie internetowej formy aktywności o charakterze politycznym.

W badaniach CBOS przeprowadzonych po wyborach do Parlamentu Europejskiego w 2019 r., 26% badanych zadeklarowało, że w trakcie kampanii wyborczej informacje o komitetach i kandydatach startujących w tych wyborach czerpało z internetu[57]. (Widać tu tendencję wzrostową – po wyborach do Parlamentu Europejskiego w 2014 r. na internet jako źródło informacji wskazało zaledwie 16% badanych). Dla porównania: 63% respondentów wskazało jako źródło informacji programy informacyjne i publicystyczne w telewizji; 52% – spoty, reklamy wyborcze (np. w radiu i telewizji); 39% – znajomych i członków rodziny; 35% – billboardy oraz plakaty wyborcze i ulotki; 34% – audycje informacyjne i publicystyczne w radiu. Z kolei z internetem przegrywały następujące źródła informacji: gazety i czasopisma (22% wskazań), indywidualne rozmowy z kandydatami (5%), uczestnictwo w wiecach i spotkaniach wyborczych (3%).

Michał Feliksiak w komunikacie z przywołanych wyżej badań CBOS podał, że w grupie badanych korzystających z internetu przynajmniej raz w tygodniu (a takich było 68% wszystkich badanych): w ciągu miesiąca poprzedzającego wybory do PE 42% (tj. 28% ogółu badanych) czytało w sieci artykuły o tematyce politycznej, 31% (tj. 21% ogółu) oglądało materiały wideo, takie jak spoty wyborcze lub wywiady z politykami, 25% (tj. 17% ogółu) czytało blogi i wpisy związane z polityką, 23% (tj. 16% ogółu) przeglądało strony partii politycznych, komitetów wyborczych lub startujących w wyborach kandydatów. W komunikacie zostały też odnotowane, stosunkowo rzadziej deklarowane,

[57] Badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 6–13 czerwca 2019 r. na liczącej 1073 osoby reprezentatywnej próbie losowej dorosłych mieszkańców Polski. Zob. *Odbiór kampanii wyborczej i aktywność polityczna w internecie przed wyborami do Parlamentu Europejskiego*, CBOS, komunikat z badań nr 86 z lipca 2019 r.

inne formy podejmowania w tym okresie aktywności politycznej w internecie: prowadzenie rozmów w sieci na tematy polityczne na forach, blogach lub w serwisach społecznościowych (5% wskazań); zachęcanie w sieci innych do poparcia jakiegoś komitetu lub kandydata (4%); zapisanie się w miesiącu poprzedzającym wybory do założonej w sieci grupy poparcia jakiegoś komitetu, partii lub kandydata (2%); wysłanie przez internet listu do jakiegoś polityka lub podpisanie w sieci petycji (1%); przekazywanie przez internet pieniędzy na cele polityczne (mniej niż 0,5%). Jest rzeczą charakterystyczną, że co najmniej jedną z wymienionych wyżej aktywności wskazuje ponad połowa użytkowników internetu (53%), czyli więcej niż jedna trzecia ogółu ankietowanych (36%).

W tym samym komunikacie autor zauważa, że: „Udziałem w e-demokracji nieograniczającym się jedynie do aspektu informacyjnego wyróżniają się najmłodsi użytkownicy internetu, mieszkańcy dużych i największych miast, osoby o poglądach lewicowych, badani w dużym stopniu zainteresowani polityką, a także deklarujący głosowanie w wyborach do PE na Konfederację. Z kolei głównie aktywnością informacyjną wyróżniali się najstarsi internauci oraz osoby przeciętnie zainteresowane wydarzeniami politycznymi, deklarujące udział w głosowaniu do PE i popierające w tych wyborach Wiosnę lub Koalicję Europejską. Uczestnictwo w e-demokracji w większym stopniu dotyczy ponadto mężczyzn niż kobiet". W komunikacie czytamy też, że „najmniejszy kontakt z polityką w internecie przed wyborami do PE" miały osoby niezainteresowane polityką, o niesprecyzowanych poglądach politycznych, niebiorące udziału w wyborach lub głosujące na PiS, mieszkające na wsi, posiadające tylko wykształcenie zasadnicze zawodowe lub podstawowe czy gimnazjalne.

Warto przypomnieć, że przed wyborami do Parlamentu Europejskiego w 2019 r. na jednym z portali informacyjnych w Polsce można było skorzystać z aplikacji pod nazwą Latarnik Wyborczy, w ramach której użytkownik mógł się ustosunkować do 24 stwierdzeń odnoszących się do kwestii politycznych, społecznych i ekonomicznych i uzyskać informację na temat procentowej zgodności swojej deklaracji z programami poszczególnych partii i komitetów wyborczych. Niestety, sztab Koalicji Europejskiej – zawiązanej na eurowybory 2019 (zdobyła w nich drugie miejsce, za Prawem i Sprawiedliwością) – nie włączył się do tego projektu i nie nadesłał odpowiedzi na pytania ujęte w badaniu; internauta nie mógł więc ocenić wszystkich opcji czy ofert politycznych i musiał wybierać spośród propozycji zgłoszonych przez pozostałe komitety wyborcze[58].

Nieco wyższe niż w przypadku wyborów w 2019 r. do Parlamentu Europejskiego wartości wskaźników aktywności w internecie związanej z wyborami

[58] Por. aplikacja ze strony wp.pl.

zarejestrowano w badaniach CBOS przeprowadzonych po wyborach krajowych, zwłaszcza w 2015 r. Przed wyborami parlamentarnymi, które odbyły się w tymże roku, korzystało z internetu w celu uzyskania informacji 32% badanych (dla porównania: w 2011 r. – 24%). Najwyższe wskaźniki odnotowano w badaniach po wyborach prezydenckich w 2015 r. – korzystanie z internetu jako źródła informacji zadeklarowało aż 37% badanych. Z kolei w wyborach samorządowych w 2018 r. odsetek osób czerpiących informacje z internetu wyniósł 34% (dla porównania: w 2014 r. – 23%).

W badaniach CBOS dotyczących aktywności politycznej Polaków w internecie przed wyborami parlamentarnymi na jesieni 2019 r.[59] uzyskano wyniki zbliżone do rejestrowanych przy okazji wyborów do Sejmu i Senatu z 2015 r. Tym razem 31% ankietowanych zadeklarowało, że w trakcie kampanii wyborczej informacje o komitetach i kandydatach startujących w wyborach czerpało z internetu. Dla porównania: 70% wskazało jako źródło informacji programy informacyjne i publicystyczne w telewizji; 55% – spoty, reklamy wyborcze (np. w radiu i telewizji); 41% – znajomych, członków rodziny; 41% – billboardy oraz plakaty wyborcze i ulotki; 30% – gazety i czasopisma; 7% – indywidualne rozmowy z kandydatami; 4% – uczestnictwo w wiecach i spotkaniach wyborczych.

M. Feliksiak w komunikacie z badań przeprowadzonych na jesieni 2019 r. podaje następujące dane: w ciągu miesiąca poprzedzającego wybory do Sejmu i Senatu 48% internautów (czyli 34% ogółu badanych) czytało w sieci artykuły o tematyce politycznej; 36% (czyli 26% ogółu) oglądało materiały wideo, takie jak reklamy wyborcze lub wywiady z politykami; 31% (czyli 22% ogółu) przeglądało strony partii politycznych, komitetów wyborczych lub osób startujących w wyborach; 27% (czyli 20% ogółu) czytało blogi i wpisy innych użytkowników związane z polityką. Jak podano w komunikacie, „Znacznie rzadziej miały miejsce kontakty bezpośrednie w formie rozmowy online na tematy polityczne. W ciągu miesiąca poprzedzającego wybory na forach, blogach lub w serwisach społecznościowych pisało o polityce 6% użytkowników internetu, a niemal tyle samo (5%) prowadziło agitację, zachęcając w sieci innych do poparcia jakiegoś komitetu lub kandydata. Czterech na stu internautów (4%) zapisało się w miesiącu poprzedzającym wybory parlamentarne do założonej w sieci grupy poparcia jakiegoś komitetu lub kandydata, a jeden na stu (1%) wysłał w tym czasie e-maila do polityka lub podpisał w sieci petycję. Bardzo rzadko (0,3%) przekazywano przez internet pieniądze na cele polityczne". Wśród

[59] Badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 7–17 listopada 2019 r. na liczącej 944 osoby reprezentatywnej próbie losowej dorosłych mieszkańców Polski. Zob. *Odbiór kampanii wyborczej i aktywność polityczna w internecie przed wyborami parlamentarnymi*, CBOS, komunikat z badań nr 152 z grudnia 2019 r.

respondentów korzystających z sieci aktywność o charakterze deliberatywnym zadeklarowało 8% osób, zaś o charakterze partycypacyjnym – 9%.

Najważniejszym czynnikiem różnicującym stopień korzystania z internetu w celu uzyskania informacji na temat komitetów i kandydatów startujących w wyborach do Sejmu i Senatu był wiek respondentów. Pozyskiwanie informacji wyborczych z internetu zadeklarowało aż 59% respondentów w wieku 18–24 lat. Podobne deklaracje przedstawiło: 39% respondentów w wieku 25–44 lat, 27% – w wieku 45–64 lat, a tylko 16% w wieku od 65 lat.

Autor cytowanego wyżej komunikatu odnotował także, że „Udziałem w e-demokracji głównie w wymiarze informacyjnym wyróżniają się najstarsi internauci, mieszkańcy największych miast, umiarkowanie zainteresowani polityką, deklarujący udział w ostatnich wyborach parlamentarnych i głosowanie w nich na KW Polskie Stronnictwo Ludowe lub KKW Koalicja Obywatelska PO.N IPL Zieloni". W komunikacie wskazano, że zaangażowaniem politycznym online wykraczającym poza wymiar informacyjny wyróżniają się osoby zainteresowane polityką, wyborcy KW Konfederacja Wolność i Niepodległość oraz KW Sojusz Lewicy Demokratycznej, wyborcy identyfikujący się z lewicą lub prawicą, a także osoby młode (mające od 18 do 34 lat), mieszkańcy średniej wielkości miast oraz ludzie najlepiej wykształceni. Najmniejszą styczność z polityką w sieci przed wyborami do Sejmu i Senatu deklarowali w omawianych badaniach: internauci mało zainteresowani polityką lub niezainteresowani nią wcale, osoby niemające sprecyzowanych poglądów politycznych, niegłosujące w tych wyborach lub też głosujące na kandydatów PiS, mające wykształcenie zasadnicze zawodowe, będące w wieku od 45 do 54 lat i mieszkające na wsi.

Wzrost aktywności politycznej społeczeństwa w internecie mającej związek z wyborami odnotowano w badaniach CBOS dotyczących wyborów prezydenckich w 2020 r.[60]. Niemal połowa (45%) wszystkich ankietowanych zadeklarowała, że w trakcie kampanii wyborczej czerpała z internetu informacje o kandydatach startujących w wyborach prezydenckich (najwięcej, bo aż 79% badanych czerpało je z programów informacyjnych i publicystycznych w telewizji). Sposób korzystania z internetu był zróżnicowany. W ciągu miesiąca poprzedzającego wybory prezydenckie (I lub II turę) 57% internautów (tj. 40% wszystkich badanych) oglądało w internecie materiały o tematyce politycznej, np. wywiady z politykami, spoty, reklamy wyborcze; 54% (38% wszystkich badanych) czytało w internecie artykuły o tematyce politycznej; 41% (29% wszystkich badanych) przeglądało strony internetowe partii politycznych lub

[60] Badanie przeprowadzono w dniach 18–27 sierpnia 2020 r. w ramach procedury mixed-mode na reprezentatywnej imiennej próbie pełnoletnich mieszkańców Polski, wylosowanej z rejestru PESEL. Zob. *Odbiór kampanii wyborczej i aktywność polityczna w internecie przed wyborami prezydenckimi*, CBOS, komunikat z badań nr 108 z września 2020 r.

kandydatów startujących w wyborach; tyle samo, czyli 41%, czytało blogi o tematyce politycznej; 13% (9% wszystkich badanych) pisało w internecie o polityce (np. na forach, blogach, portalach społecznościowych); 7% (5% wszystkich badanych) zachęcało w internecie innych użytkowników do głosowania w wyborach na dany komitet lub któregoś z kandydatów; tyle samo, czyli 7%, zapisało się w internecie do grupy popierającej jakiegoś kandydata lub organizację polityczną czy komitet wyborczy; 4% (3% wszystkich badanych) wysłało przez internet list do polityka lub podpisało internetową petycję; 1% (0,4% wszystkich badanych) przekazało przez internet pieniądze dla organizacji politycznej, komitetu wyborczego.

Z omówionych wyżej badań CBOS wynika, że w ostatnich dziesięciu latach nastąpiło wyraźne zwiększenie internetowej aktywności politycznej, o charakterze zarówno deliberatywnym: z 4% internautów (2% wszystkich badanych) w 2010 r., do – odpowiednio – 16% (11% wszystkich badanych) w 2020 r., jak i partycypacyjnym: z 5% (3% wszystkich badanych) do 15% (10% wszystkich badanych). Istotnymi uwarunkowaniami zróżnicowania poziomu aktywności politycznej internautów w czasie kampanii wyborczej w 2020 r. okazały się: wiek badanych (taką aktywność zadeklarowało 85% respondentów w wieku od lat 18 do 24, a 76% w wieku 65 lat i więcej), miejsce zamieszkania (wieś – 63%, miasta od 500 tys. mieszkańców – 87%), wykształcenie (wykształcenie podstawowe lub gimnazjalne – 65%, zaś wyższe – 85%), zainteresowanie polityką (wśród osób deklarujących duże zainteresowanie – 93%, wśród osób całkowicie niezainteresowanych – 47%). Poziom aktywności politycznej różnicowały też poglądy polityczne. W przypadku internautów deklarujących się jako zwolennicy PiS była to aktywność na poziomie 67%, KO – 90%, lewicy – 85%, Konfederacji WiN – 94%, PSL i KP – 70%. Tylko w niewielkim stopniu internetową aktywność polityczną różnicowała płeć osób badanych (mężczyźni – 75%, kobiety – 70%).

Rozdział jedenasty

Co dalej? Strategiczne dylematy przyszłości rządzenia i polityki w warunkach ekspansji cywilizacji cyfrowej

11.1. Świadomość nieuchronności dalszych jakościowych zmian w świecie stosunków społecznych pod wpływem nowych technologii

Postępy w uczeniu maszynowym, doskonalenie technik komputerowych i powstawanie nowych generacji robotów jako procesy o istotnym znaczeniu społecznym • Zacieranie się granic między sferą fizyczną, cyfrową i biologiczną w ramach czwartej rewolucji przemysłowej • Przyspieszenie cyfryzacji w związku z wybuchem pandemii koronawirusa w 2020 r.

Można wskazywać coraz więcej przykładów oddziaływania nowych technologii cyfrowych na aktywność ludzi oraz struktur politycznych i gospodarczych. Równocześnie trwają intensywne prace zmierzające do zwiększania zdolności narzędzi cyfrowych. W tej dziedzinie ilość nieuchronnie przechodzi w jakość, zaś dokonujące się zmiany mają charakter strategiczny. Nie dziwi więc fakt, że wielu analityków wskazuje na nieuniknione, jakościowe zmiany w sferze stosunków społecznych pod wpływem szybkiego postępu uczenia maszynowego, doskonalenia technik komputerowych i powstawania nowych generacji robotów.

W prognozach podkreśla się szczególnie, że zdolności urządzeń świata cyfrowego wykraczają poza proste uczenie maszynowe (zwane nieraz uczeniem nadzorowanym). Doskonalenie narzędzi cyfrowych nie odbywa się już obecnie tylko dzięki spożytkowaniu wcześniejszych doświadczeń „na zasadzie dedukcji, z wykorzystaniem wcześniej zdobytej bazy wiedzy”[1]. Pojawiają się nowe mechanizmy uzyskiwania przez maszyny zdolności autonomicznego dzia-

[1] M. Kowalczyk, *Cyfrowe Państwo…*, s. 172–173.

łania. Marcin Kowalczyk, odwołując się do literatury światowej na ten temat, wymienia w tym kontekście: uczenie ze wzmocnieniem – w którym obok wcześniejszych doświadczeń jest wykorzystywana wiedza o wyniku podjętych działań i na tej podstawie są podejmowane kolejne próby tworzenia rozwiązań wolnych od wcześniejszych błędów; uczenie nienadzorowane – w którym ma miejsce „poszukiwanie lub odkrywanie całkowicie nowych wzorców"; uczenie przez transfer – w którym wiedza dotycząca określonego przypadku jest używana do rozwiązywania nowych problemów[2]. To właśnie te zdolności są najczęściej wskazywane jako najważniejszy czynnik sprawczy przyszłych zmian we wszystkich dziedzinach.

Należy się spodziewać znacznych i głębokich przeobrażeń rzeczywistości w wyniku doskonalenia technologii cyfrowych. Tak mówi o tym autor cytowanej tu już pracy: „Postępy w intelektualnych i fizycznych możliwościach maszyn zmienią sposób, w jakim żyjemy, pracujemy, bawimy się, szukamy partnerów seksualnych, wychowujemy dzieci i dbamy o naszych seniorów. Przewrócą do góry nogami rynki pracy, przetasują nasz porządek społeczny i wystawią na próbę instytucje prywatne i publiczne"[3]. Oczywiście, zawsze warto zachować ostrożność w kreśleniu scenariuszy przyszłości, jednak przedstawiona powyżej prognoza – może dlatego, że jest niezwykle ogólna – wydaje się bardzo prawdopodobna. Co więcej, zapowiedź głębokich zmian z pewnością ziści się również w sferze rządzenia. Biorąc pod uwagę silne powiązania polityki z jej otoczeniem, musimy przyjąć, że wszystkie zasygnalizowane dotychczas w tej książce przejawy rewolucji cyfrowej, m.in. dynamiczny rozwój sztucznej inteligencji, wpłyną na decydowanie polityczne i rządzenie, a mówiąc wprost – wymuszą zmiany w rządzeniu. Kwestią otwartą pozostaje kalendarz i charakter zmian. Natomiast jest rzeczą bezsporną, że nie da się budować cyfrowej przyszłości polityki i decydowania politycznego za pomocą narzędzi pochodzących z niecyfrowej przeszłości. Ci, którzy tego faktu nie uwzględnią w swoim myśleniu, mają małą szansę na zaproponowanie rozwiązań przydatnych już w najbliższej przyszłości.

Ryan Avent – dziennikarz tygodnika „The Economist", autor książki poświęconej modyfikacjom relacji społeczno-ekonomicznych i stosunków pracy zachodzącym pod wpływem rewolucji informatycznej XXI wieku – porównuje cyfryzację z ukształtowaniem w XIX wieku świata przemysłowego. Zwraca przy tym uwagę, że w związku z cyfryzacją pojawią się poważne problemy

---

[2] Tamże, s. 173 i nast. Zob. też: G. Hulten, *Budowanie systemów inteligentnych. Przewodnik po inżynierii uczenia się maszyn*, Warszawa 2020; M. Szeliga, *Data Science i uczenie maszynowe*, Warszawa 2017; A. Wodecki, *Sztuczna inteligencja w kreowaniu wartości organizacji. Analiza generowania wartości przez firmy wykorzystujące sztuczną inteligencję w prowadzeniu biznesu*, Kraków 2018, s. 81 i nast.

[3] J. Kaplan, *Sztuczna inteligencja…*, s. 11.

i przeciwności: „Może kiedyś będziemy musieli się zmagać ze sztuczną inteligencją o złych intencjach albo z problemem genetycznie modyfikowanych superludzi – jednak znacznie szybciej, w ciągu 10 do 20 lat, będziemy musieli stawić czoło zagrożeniom, jakie technologia stwarza dla naszego porządku społecznego i naszej polityki”[4].

Przywołana wyżej prognoza współbrzmi z problematyką podejmowaną w ramach Światowego Forum Ekonomicznego (World Economic Forum, WEF) w 2016 r. W materiałach WEF czytamy: „Pierwsza rewolucja przemysłowa wykorzystała moc wody i pary do zmechanizowania produkcji. Druga wykorzystała energię elektryczną do stworzenia masowej produkcji. Trzecia wykorzystała elektronikę i technologię informacyjną do automatyzacji produkcji. Teraz czwarta rewolucja przemysłowa opiera się na trzeciej, cyfrowej rewolucji, która ma miejsce od połowy ubiegłego wieku. Charakteryzuje się połączeniem technologii, w którym zacierają się linie między sferą fizyczną, cyfrową i biologiczną”[5]. Według analityków WEF: „Szybkość obecnych przełomów nie ma precedensu historycznego. W porównaniu z poprzednimi rewolucjami przemysłowymi czwarta ewoluuje raczej w tempie wykładniczym niż liniowym. Co więcej, zakłóca to niemal każdą dziedzinę w każdym kraju. A szerokość i głębokość tych zmian zapowiada transformację całych systemów produkcji, zarządzania i rządzenia”[6].

Wprowadzanie rozwiązań cyfrowych do polityki, rządzenia i administrowania publicznego wyraźnie przyspieszyło w następstwie pandemii koronawirusa w 2020 r. Życie polityczne w szybkim tempie przeniosło się do sfery online. Zagrożenie infekcją w istotnej mierze zablokowało na całym świecie tradycyjne formy funkcjonowania organów publicznych. W sposób zdalny, z wykorzystaniem łączy i innych narzędzi internetowych, działały parlamenty i organy władzy wykonawczej w państwach i organizacjach międzynarodowych. Wiele milionów ludzi na całym świecie musiało przestawić się na pracę i naukę zdalną. W normalnych warunkach taka zmiana wymagałaby długotrwałych przygotowań i stanowiłaby przedmiot zażartych sporów. W obliczu zagrożenia epidemicznego sięgnięcie po narzędzia elektroniczne okazało się rozwiązaniem najlepszym, a w wielu wypadkach bezalternatywnym. Źle by się jednak stało, gdyby miano je potraktować jako rozwiązanie doraźne, przejściowe – rodzaj narzędzia na potrzeby stanu wyjątkowego. Nadzwyczajna sytuacja obnażyła braki w infrastrukturze cyfrowej, którym trzeba zdecydowanie zaradzić, myśląc już także o okresie po ustaniu pandemii. Należy oczekiwać przyspieszenia

---

4 R. Avent, *The Wealth of Humans: Work, Power, and Status in the Twenty-first Century*, New York 2016.

5 https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond.

6 Tamże.

prac zmierzających do informatyzacji procedur publicznych oraz wzmożenia wysiłków na rzecz podniesienia kompetencji cyfrowych społeczeństwa. Nie ulega wątpliwości, że powstały okoliczności przemawiające za szybkim rozwojem technologii 5G i tworzeniem za pomocą tej technologii narzędzi decydowania w sprawach publicznych.

11.2. Brak jednego scenariusza rozwoju demokracji elektronicznej

Możliwości techniczne przenoszenia procesów artykulacji i agregacji oraz legitymizacji politycznej i rządzenia do internetu • Społeczne i polityczne bariery wykorzystania internetu w wyborach powszechnych • Intensyfikacja wysiłków na rzecz bezpieczeństwa informacyjnego i informatycznego przed wyborami prezydenckimi w USA w 2020 r. • Ograniczony zakres testowania możliwości włączenia narzędzi i mechanizmów elektronicznych do procedur wyborów powszechnych • Odległa perspektywa upowszechnienia technik elektronicznych w ramach wykonywania praw i obowiązków obywatelskich oraz rządzenia

Jak sygnalizowałem w poprzednich rozdziałach, cyfryzacja jest dotychczas wykorzystywana w polityce w większym stopniu do tworzenia przez podmioty władzy niedemokratycznej systemu permanentnej inwigilacji – czegoś na kształt Benthamowskiego panoptykonu – na skalę ogólnopaństwową, niż do wspomagania procesów demokratycznych. Po technologie internetowe, uznane początkowo nie bez racji za dobro wspólne[7] i narzędzia wolności, sięgnęli dość szybko politycy o zapędach dyktatorskich, dostrzegając możliwości ich użycia do elektronicznej inwigilacji oraz blokowania aktywności swych oponentów – ludzi, organizacji społecznych i instytucji. Na tle prób zawładnięcia internetem przez zwolenników silnej władzy – określanych nieraz jako przejawy imperializmu technologicznego – działania na rzecz elektronicznej partycypacji politycznej o charakterze prodemokratycznym wyglądają niezbyt imponująco. Kierunek zachodzących w świecie zmian czyni jednak aktualnym pytanie o możliwość kształtowania się w praktyce systemu ustrojowego zwanego nieraz demokracją elektroniczną[8].

Samo pojęcie demokracji elektronicznej (e-demokracji) jest rozumiane w różny sposób, w każdym jednak przypadku wskazuje się na jego aspekty społeczne, komunikacyjne i technologiczne. W wymiarze społecznym demokra-

[7] Zob.: M. Castells, *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, Poznań 2003; J. Hofmokl, *Internet jako nowe dobro wspólne*, Warszawa 2009.

[8] Zob.: G. Browning, *Elektroniczna demokracja…*; L.K. Grossman, *Republika elektroniczna*; M. Marczewska-Rytko (red.), *Demokracja elektroniczna…*; M. Musiał-Karg (red.), *Demokracja w obliczu nowych mediów…*; R. Olszowski, *Elektroniczna Republika…*

cję elektroniczną wiąże się przede wszystkim z ukształtowaniem się sieciowego społeczeństwa informacyjnego oraz z tym, że o zachowaniach politycznych ludzi zasadniczo decydują uzyskane i przyjęte przez nich za własne informacje o faktach i wizerunki tych faktów zaczerpnięte z mediów społecznościowych, elektronicznych wyszukiwarek i kontaktów internetowych. W wymiarze komunikacji społecznej na gruncie demokracji elektronicznej jako standard przyjęto wykorzystywanie narzędzi zindywidualizowanych i interaktywnych kontaktów masowych w internecie do działalności politycznej. Chodzi tu o działania mające na celu zdobycie, utrzymywanie i wykonywanie władzy politycznej w państwie. W tym modelu demokracji elektroniczna komunikacja społeczna jest głównym narzędziem kreowania i wzmacniania określonych poglądów, żądań, ocen i programów politycznych, płaszczyzną do prowadzenia debaty publicznej, sposobem budowania i wzmacniania siły oraz organizowania działalności ruchów i ugrupowań politycznych, a także osłabiania pozycji konkurentów politycznych i znaczenia głoszonych przez nich programów. W wymiarze technologicznym za miarę rozwoju demokracji elektronicznej należy uznać w pierwszej kolejności zakres korzystania z internetu i z narzędzi cyfrowych w procesach legitymizacji wyborczej związanej z ustalaniem składu politycznego i personalnego organów publicznych w trybie wyborów powszechnych oraz w rozstrzyganiu kwestii oddanych do decydowania bezpośredniego w trybie referendalnym.

Jak dotąd, model elektronicznej demokracji nie został w pełni urzeczywistniony w żadnym państwie. Zakres i tempo wprowadzania w życie tego modelu są w poszczególnych jego aspektach zróżnicowane. Relatywnie najwolniej zmienia się stopień wykorzystania możliwości technologicznych do legitymizacji wyborczej i do rozszerzania procedur decydowania z użyciem narzędzi elektronicznych w ramach demokracji bezpośredniej. W tej dziedzinie zmiany mają charakter pomocniczy, w wielu przypadkach eksperymentalny, i nie łamią dotychczasowych rozwiązań systemowych. W świecie współczesnym dominuje nadal model przedstawicielski władz publicznych i są stosowane tradycyjne metody kształtowania składu organów władzy publicznej i decydowania publicznego. Pomijając państwa autorytarne i totalitarne, artykulacja i agregacja interesów politycznych odbywa się przy udziale podmiotów instytucjonalnych, zwłaszcza partii politycznych, zaś legitymacja władzy pochodzi z cyklicznych, powszechnych i – zwykle – bezpośrednich wyborów. W większości państw reprezentujących różne warianty demokracji parlamentarnej wyborcy decydują co kilka lat, komu chcą powierzyć rządzenie. Obowiązuje najczęściej zasada mandatu wolnego. Przeważają ordynacje proporcjonalne, które premiują na listach wyborczych polityków wskazanych przez partie polityczne. Zmiany preferencji wyborczych w okresie trwania kadencji władz nie powodują automatycznego cofnięcia legitymacji do rzą-

dzenia. Korekta jest dokonywana dopiero po zakończeniu kadencji lub po rozpadzie zaplecza politycznego rządu w parlamencie. Decydowanie w trakcie kadencji w formie referendum o wcześniejszym odwołaniu organów władz publicznych pochodzących z wyborów powszechnych jest możliwe zwykle tylko na szczeblu lokalnym i regionalnym. Wymaga to jednak dochowania skomplikowanych procedur i wyzwolenia potencjału aktywności obywatelskiej. Podejmowanie decyzji w trybie referendum podlega znacznym ograniczeniom i stanowi z zasady tylko uzupełnienie dominującego trybu rozstrzygania przez organy publiczne[9].

W świetle przewidywanych na wstępie tego rozdziału jakościowych zmian w decydowaniu politycznym pod wpływem postępującego procesu cyfryzacji, praktycznego znaczenia nabierają pytania o przyszłość demokracji elektronicznej i perspektywy modelu nazywanego – za Lawrence'em K. Grossmanem – republiką elektroniczną. Odpowiedzi na te pytania nie są łatwe i jednoznaczne. Pewne argumenty przemawiają za tym, że w modelu demokracji elektronicznej nastąpią szybkie i daleko idące zmiany, inne zaś skłaniają do dużej ostrożności w prognozowaniu takich zmian.

Rozwój technologii cyfrowych sprzyja przenoszeniu do internetu istotnych elementów procesu artykulacji i agregacji interesów politycznych oraz legitymizacji rozstrzygnięć personalnych i programowych w ramach decydowania politycznego i rządzenia. Możliwości technologii cyfrowych oraz zmiany sposobu funkcjonowania ludzi związane z ukształtowaniem się społeczeństwa sieciowego tworzą realną perspektywę optymalizowania polityki. Odnosi się to także do instrumentów demokracji bezpośredniej. Zwolennicy demokracji elektronicznej uważają, że w przyszłości – mimo widocznych teraz przeszkód – inteligentne technologie cyfrowe mogą z powodzeniem służyć optymalizowaniu decydowania politycznego. Ich zdaniem coraz bardziej realne z punktu widzenia technologicznego staje się powszechne wykorzystywanie komunikacji internetowej w wyborach organów publicznych, powstają też lepsze warunki do decydowania w wybranych sprawach w trybie referendalnym bez ponoszenia dużych kosztów. Ponadto, z upływem czasu coraz mniej zrozumiałe będzie wyłączenie z procesów informatyzacji praktyk obywatelskich, w tym związanych z legitymizacją i partycypacją polityczną. Już dzisiaj ludzie załatwiają za pomocą łączy internetowych wiele swoich spraw – nie tylko osobistych, lecz także pozostających w sferze relacji publicznych.

Szukając odpowiedzi na pytanie o przyszłość demokracji elektronicznej, trzeba brać pod uwagę dość skromne i niejednoznaczne doświadczenia zebrane dotychczas przy wprowadzaniu narzędzi cyfrowych do procesów wyborczych[10].

[9] Zob. M. Musiał-Karg, *Referendum w państwach europejskich*, Toruń 2008.

[10] Zob.: M. Musiał-Karg, *Elektroniczne głosowanie. Wybrane dylematy dotyczące e-votingu*, w: M. Marczewska-Rytko (red.), *Demokracja elektroniczna…*; tejże, *Elektroniczne referendum*

Procedury i narzędzia elektroniczne są już obecnie (obok głosowania korespondencyjnego lub przez przedstawiciela) testowane w niektórych krajach jako rozwiązania alternatywne wobec tradycyjnego sposobu głosowania. Mają one jednak przeważnie charakter pomocniczy i nie obejmują głosowania przez internet. Jarosław Zbieranek wskazuje w tym kontekście, odwołując się do systematyki wypracowanej przez Międzynarodowy Instytut Demokracji i Pomocy Wyborczej (International IDEA – Institute for Democracy and Electoral Assistance)[11], przykłady rozwiązań opartych na: maszynach do głosowania (DRE – *direct recording electronic voting machines*), skanerach umożliwiających odczytanie karty ze wskazaną przez wyborców preferencją (OMR – *optical mark recognition*), drukarkach głosów elektronicznych (EBPs – *electronic ballot printers*) umożliwiających wydruk kart lub oznaczeń wskazujących preferencje wyborcy, a także na wykorzystaniu internetu (*i-voting*)[12].

W praktyce narzędzia elektroniczne są stosowane dotychczas najczęściej do rejestrowania wyborców oraz liczenia głosów oddanych w lokalach wyborczych za pomocą elektronicznej wersji kartki do głosowania, skanerów optycznych i terminali internetowych. Różne możliwości wykorzystania takich narzędzi testuje się m.in. w Niemczech, we Francji i w Wielkiej Brytanii. Maszyny do oddawania głosu w lokalu wyborczym wprowadzono już w 1996 r. w Brazylii. Przykładowo, w wyborach prezydenckich w tym kraju w 2018 r. wyborca mógł się zalogować w lokalu wyborczym do maszyny i zagłosować poprzez wpisanie i zaakceptowanie numeru popieranego kandydata. W artykule opublikowanym na stronie IDEA w 2017 r. Peter Wolf zauważył, że wzrasta liczba krajów, w których na kolejnych etapach procesów wyborczych stosuje się różne narzędzia technologii elektronicznej. Zaznaczył jednak równocześnie, że nieraz kończy się to niepowodzeniem, podając przykład wyborów prezydenckich w Kenii w 2017 r., które zostały unieważnione z powodu nieprawidłowości w elektronicznym przekazywaniu wyników głosowania. Według informacji zawartych w tymże artykule, opartych na danych znajdujących się w zasobach IDEA, tylko w około 11% państw na świecie przeprowadza się wybory bez używania jakiegoś narzędzia technologii elektronicznej. Rodzaje i liczba stosowanych technologii są jednak w poszczególnych państwach bardzo zróżnicowane. Około 71% organów zarządzających wyborami odpowiedzialnych za rejestrację wyborców korzysta w tym celu z narzędzi elektronicznych,

w Szwajcarii. Wybrane kierunki zmian helweckiej demokracji bezpośredniej, Poznań 2012; tejże, *E-voting jako nowa forma uczestnictwa obywateli w procesach wyborczych. Doświadczenia wybranych państw europejskich*, w: A. Stelmach (red.), *Prawo wyborcze i wybory. Doświadczenia dwudziestu lat procesów demokratyzacyjnych w Polsce*, Poznań 2010; J. Zbieranek, *Głosowanie przez internet (i-voting) w wybranych państwach*, Biuro Analiz Sejmowych, „Zeszyty Prawnicze BAS" 2018, nr 1 (57).

11 *Introducing Electronic Voting: Essential Considerations*, IDEA, Stockholm 2011, s. 9–11.

12 J. Zbieranek, *Głosowanie przez internet…*, s. 10 i nast.

tylko 21% państw sięga do technologii identyfikacji wyborców w lokalach wyborczych, a jeszcze mniej (15%) stosuje narzędzia elektroniczne do liczenia głosów w lokalach wyborczych, w około 15% państw przesyła się wyniki drogą elektroniczną z podłączonych lokali wyborczych, zaś 57% państw używa elektronicznych systemów tabelarycznych do zestawiania oficjalnych wyników. Z kolei sam fakt wykorzystywania narzędzi elektronicznych jest uzależniony od rodzaju wyborów – wyraźnie widać, że częściej ma to miejsce w przypadku wyborów lokalnych[13]. W materiale przygotowanym w 2019 r. dla jednego z kanałów telewizyjnych wskazano, powołując się na zebrane przez IDEA dane z 175 państw, że jakakolwiek forma głosowania elektronicznego jest stosowana w 35 spośród nich[14].

Podejmuje się próby wykorzystania narzędzi komunikacji elektronicznej do zwiększenia frekwencji wyborczej. Przykładowo w USA, gdzie elementem procesu wyborczego jest zarejestrowanie się obywateli jako wyborców, w 2019 r. jedno ze środowisk politycznych zaczęło w internecie agitować na rzecz rejestracji. Grupa popierająca środowisko Demokratów przygotowała program internetowy, który za pomocą Snapchata, Instagrama i innych platform cyfrowych miał mobilizować do rejestracji wyborczej w południowych stanach młode osoby pochodzące z mniejszości. Organizatorzy tej akcji stawiali sobie za cel zmobilizowanie w trybie online przed wyborami prezydenckimi w 2020 r. ponad 100 tysięcy osób[15].

Próbując prognozować rozwój demokracji elektronicznej, trzeba uwzględnić fakt, że współcześnie tylko w bardzo nielicznych przypadkach można oddać głos w wyborach lub referendum za pośrednictwem łączy internetowych. Na poziomie ogólnokrajowym jest to możliwe jedynie w Estonii. Poza tym jednostkowym przypadkiem, głosowanie przez internet ma miejsce w wyborach na niższych poziomach podziału administracyjnego: w kilku kantonach Szwajcarii i prowincjach Kanady oraz – z uwzględnieniem pewnych grup wyborców (np. ludzi starszych, niepełnosprawnych, mieszkających na oddalonych terenach) – w niektórych stanach w USA, a także – jako możliwość na szczeblu lokalnym – we Francji.

Warto poświęcić kilka słów więcej Estonii. Po raz pierwszy dopuszczono tam do oddania głosu przez internet w wyborach samorządowych w 2005 r.[16]. W wyborach parlamentarnych w 2019 r. w tym trybie oddało głos już prawie

[13] https://www.idea.int/news-media/news/election-technology-precondition-transparent-elections-or-pretext-questioning.

[14] https://konkret24.tvn24.pl/polityka,112/glosowanie-elektroniczne-to-standard-w-zachodnich-demokracjach-sprawdzamy-wpis-po,961141.html.

[15] https://www.politico.com/story/2019/08/14/progressive-online-voter-registration-drive-1461912.

[16] Zob. M. Musiał-Karg, *Internetowe głosowanie w E-stonii na przykładzie wyborów w latach 2005–2009*, „Przegląd Politologiczny" 2011, nr 3, s. 99 i nast.; J. Rzucidło, *Referendum w obliczu głosowania za pośrednictwem Internetu – doświadczenia Estonii, Norwegii i Szwajcarii*, w:

350 tysięcy Estończyków, co stanowiło ponad 40% uprawnionych do głosowania. A obecnie, jak już wspomniałem, taką możliwość mają wszyscy wyborcy na szczeblu ogólnokrajowym. Wyborca może w tym kraju unieważnić swój głos oddany przez internet w dniach poprzedzających dzień wyborów i zagłosować ponownie w tradycyjny sposób w lokalu wyborczym. Doświadczenia zebrane w Estonii pokazały, że głosowanie przez internet to szansa na zwiększenie frekwencji w wyborach oraz rozwiązanie szczególnie przydatne dla osób niepełnosprawnych i mających z różnych innych powodów trudności z dotarciem do lokalu wyborczego. Trzeba jednak pamiętać, że w tej dziedzinie Estonia stanowi wyjątek, zaś różne formy głosowania elektronicznego nie wychodzą jak dotychczas poza ramy rozwiązań pomocniczych i polegają raczej na wykorzystywaniu środków elektronicznych do oddawania głosu w lokalu wyborczym niż na głosowaniu na odległość poprzez łącza internetowe.

Oceniając szanse wprowadzenia głosowania na odległość za pomocą łączy internetowych, należy wziąć pod uwagę fakt, że manipulowanie w internecie na wielką skalę opiniami wyborców oraz częste naruszanie bezpieczeństwa informacyjnego i informatycznego systemu wyborczego budzą silne obawy – nie tylko decydentów publicznych, lecz także opinii publicznej – i przyczyniają się do wyraźnego obniżenia zaufania do internetu (pomijam tu, oczywiście, inne czynniki, które na to rzutują, niezwiązane z procesem wyborczym)[17]. Jeśli nie będzie się eliminować patologii, perspektywa upowszechnienia wyborów elektronicznych wydaje się niepewna. A więc, rozpatrując zalety demokracji elektronicznej i opowiadając się za jej rozwojem, nie wolno zapominać o istniejących zagrożeniach bezpieczeństwa wyborów elektronicznych.

Wiele wskazuje na to, że na kształt demokracji elektronicznej w najbliższych latach w istotny sposób wpłyną wnioski wynikające z wyborów prezydenckich w USA. Próby włamywania się do elektronicznych baz danych i systemów komunikacji internetowej komitetów wyborczych Obamy i McCaina odnotowano już w 2008 r. Działania te przypisuje się powszechnie hakerom powiązanym z władzami chińskimi. W 2016 r. zewnętrzne ingerencje w sprawy dotyczące wyboru prezydenta USA nabrały jednak nowego charakteru. Doszło wówczas, jak się powszechnie uważa, do czegoś więcej niż włamania i kradzież lub zniekształcanie treści zasobów elektronicznych danych podmiotów politycznych uczestniczących w wyborach. Miała miejsce złożona operacja oddziaływania na opinię publiczną i na świadomość ludzi. Objęła ona: włamania do sieci, kradzieże dokumentów i korespondencji oraz informacji elektronicznych; udostępnianie wykradzionych dokumentów w sieci za pomocą fałszywych toż-

O. Hałub, M. Jabłoński, M. Radajewski (red.), *Instytucje demokracji bezpośredniej w praktyce*, Wrocław 2016.

17 https://www.idea.int/publications/catalogue/introducing-electronic-voting-essential-considerations?lang=en.

samości (takich jak Guccifer 2.0 i DCLeaks); posługiwanie się wykradzionymi materiałami jako bronią propagandową w komunikacji internetowej (m.in. za pośrednictwem WikiLeaks); organizowanie dyskusji w sieci elektronicznej przy wykorzystaniu armii internetowych trolli. Przedmiotem ataku stały się internetowe zasoby danych i narzędzia komunikacji elektronicznej Krajowego Komitetu Partii Demokratycznej (Democratic National Committee – DNC) oraz sieci komputerów i łączności kierownictwa kampanii Hillary Clinton. Celem cyberagresji stał się także Komitet Partii Demokratycznej do spraw Kampanii do Kongresu (Democratic Congressional Campaign Committee – DCCC). Ujawniono wewnętrzne dokumenty, oceny, korespondencję, charakterystyki personalne, plany terenowe, strategie DCCC. Na te działania nałożyły się próby ingerencji w systemy informatyczne służące do obsługi głosowania, w tym stanowe systemy komputerowe (szczególnie bazy wyborców). Mechanizmy tych manipulacji, mimo toczących się śledztw i sporządzanych raportów, nie są do końca rozpoznane. Amerykańskie służby specjalne całą tę operację przypisały Rosji. Taką samą konkluzję zawiera raport senackiej komisji wywiadu, która badała kwestię zewnętrznych ingerencji w wybory w 2016 r. W dokumencie stwierdzono, że istnieją przesłanki, aby uznać, iż polecenie włamania się do sieci komputerowych i kont powiązanych z Partią Demokratyczną wyszło bezpośrednio od prezydenta Rosji Władimira Putina, zaś rosyjska ingerencja internetowa w politykę USA trwała co najmniej do stycznia 2020 r.[18].

Warto zauważyć, że do świadomości polityków w USA w okresie przed wyborami w 2016 r. dość długo docierała prawda, że współcześnie ingerencja w zasoby informacyjne oraz narzędzia komunikacyjne systemów i struktur wyborczych nie musi przypominać afery Watergate ani żadnej akcji w jej stylu. Nie trzeba się już uciekać do włamania czy innej formy fizycznej przemocy… Jak się okazało, FBI pierwsze sygnały dotyczące cyberataku przekazało przedstawicielom DNC już we wrześniu 2015 r. Atak powiązano z aktywnością grupy hakerów APT 29 – traktowanej jako ekspedytura wywiadu cywilnego Rosji. Kolejne ostrzeżenia, tym razem przed wyraźnie zidentyfikowaną grupą APT 28 – stanowiącą narzędzie rosyjskiego wywiadu wojskowego GRU – amerykańskie służby specjalne przekazały decydentom politycznym na początku 2016 r. Również i te sygnały zostały w gruncie rzeczy zlekceważone.

Jak zwykle bywa w takich sytuacjach, politycy musieli sobie odpowiedzieć na pytanie, w jakim zakresie mogą się na forum publicznym posługiwać informacjami, których źródeł i sposobów pozyskania nie wolno im ujawnić. Tę bardzo delikatną kwestię komplikował fakt, że w grę wchodziły sprzeczne

[18] https://www.politico.com/news/2020/08/18/manafort-worked-with-russian-intel-officer-who-may-have-been-involved-in-dnc-hack-senate-panel-says-397597.

interesy z obszaru stosunków z Rosją. Kłopotliwe stały się także wewnątrzkrajowe uwarunkowania polityczne wynikające z podejrzeń Demokratów o to, że środowisko Donalda Trumpa z zadowoleniem odnosi się internetowej nagonki na Hillary Clinton[19]. W połowie 2020 r. podejrzenia te urealniły się dzięki ustaleniom senackiej komisji do spraw wywiadu, zgodnie z którymi czołowi sztabowcy Trumpa mieli w okresie kampanii wyborczej w 2016 r. bezpośrednie kontakty z przedstawicielami Rosji zaangażowanymi w operację osłabiania pozycji kandydatki Partii Demokratycznej na prezydenta USA[20].

Doświadczenia wyniesione z agresji internetowej z 2016 r. zostały uzupełnione wiedzą o próbach ingerencji w wybory do Kongresu w 2018 r. Nikt nie mógł już mieć wątpliwości co do tego, że tego rodzaju ataki mogą się powtarzać. Problem ten zaczął dostrzegać także prezydent Trump, który w kolejnych latach swojego urzędowania miał coraz bardziej napięte stosunki z mediami społecznościowymi oraz z Chinami, Iranem i Rosją – państwami tradycyjnie kojarzonymi z wykorzystywaniem internetu do walki politycznej. W tych warunkach bezpieczeństwo wyborów stało się w USA najwyższym priorytetem. Już w styczniu 2017 r. infrastruktura wyborcza (obejmująca bazy rejestracji wyborców oraz lokalizacji wyborczych i powiązane systemy informatyczne przeznaczone do zarządzania wyborami, w tym głosowania oraz liczenia głosów, audytu i wyświetlania wyników wyborów, raportowania i potwierdzania wyników) została uznana za część krajowej infrastruktury krytycznej i podsektor w sektorze obiektów rządowych[21].

Przed wyborami prezydenckimi w 2020 r. przyjęto w USA strategię maksymalnego eliminowania zagrożeń internetowych i w efekcie ogłoszono wyborczy alert antyelektroniczny. Zaczęto dublować wyborcze procedury elektroniczne poprzez sporządzanie dokumentacji papierowej. Pojawiły się próby całkowitego odejścia od elektronicznego wspomagania głosowania. Jednak wprowadzanie zmian w procedurach wyborczych nie jest w USA łatwe, m.in. dlatego, że rozwiązania te podlegają jurysdykcji poszczególnych stanów. Jak stwierdzono w badaniach prowadzonych w Stanach Zjednoczonych od 2017 r. przez Politico, niemal każdy stan stosuje elektroniczne urządzenia do głosowania – najczęściej są to skanery optyczne. W raporcie z tych badań podano, że prawie 90% systemów wyborczych korzysta z maszyn do głosowania wyposażonych w jakąś formę kopii papierowych, tylko mniej niż 2% systemów opiera się wyłącznie na maszynach do głosowania bez zapasowej kopii papierowej, 30% stanów używa nadal elektronicznych maszyn do głosowania, które nie generują kopii papierowych. Prawie 8 na 10 stanów posługuje się urządzeniami

[19] Zob. M. Isikoff, D. Corn, *Rosyjska ruletka. Jak Putin zaatakował Amerykę…*

[20] https://www.reuters.com/article/us-usa-trump-russia-senate-findings-fact/factbox-key-findings-from-senate-inquiry-into-russian-interference-in-2016-u-s-election-idUSKCN25E2OY.

[21] https://www.dhs.gov/topic/election-security.

do znakowania głosów i komputerów, które drukują zapisy papierowe, ale są narażone na włamania. W blisko 40% stanów dokumentację elektroniczną uzupełniono w ostatnich latach kopiami papierowymi[22].

W wyborach parlamentarnych w USA w 2018 r. rozwiązanie w postaci podwojonej rejestracji oddanych głosów – za pomocą maszyn elektronicznych i wydruków papierowych – przyjęto w 14 stanach[23]. Wszelkie systemowe zmiany rozwiązań stosowanych przy wyborach bardzo trudno wprowadzić także z tego powodu, że pociągają one za sobą wielomilionowe wydatki. Już w 2018 r. Kongres przekazał stanom 380 milionów dolarów na poprawę bezpieczeństwa wyborów, co nie rozwiązało jednak problemów finansowych w tej dziedzinie. Mimo wytaczania licznych argumentów przeciwko używaniu w wyborach urządzeń elektronicznych, władze kilku stanów zadecydowały, że pozostają przy rozwiązaniu, które nie wymaga papierowego potwierdzenia zapisu każdego oddanego głosu. Eksperci dopatrują się tutaj realnego niebezpieczeństwa w postaci niewykrywalnego ataku hakerów i wskazują na brak możliwości alternatywnego sprawdzenia wyników głosowania. Urzędnicy wyborczy w tych stanach widzą jednak przede wszystkim korzyści: narzędzia elektroniczne automatycznie sumują wyniki, eliminują potrzebę ochrony i przechowywania kart do głosowania i zdecydowanie ułatwiają oddanie głosu. Ekrany dotykowe w smartfonach, tabletach i maszynach wyborczych – dzięki temu, że można się nimi łatwo (intuicyjnie) posługiwać – są dogodne nawet dla osób debiutujących w roli wyborców, a także dla wyborców starszych, którzy mają problemy z wypełnianiem formularzy. W niektórych stanach (np. w Oklahomie), gdzie obowiązują głównie systemy z papierową kartą wyborczą, utrzymuje się maszyny elektroniczne jako narzędzia do głosowania dla osób niepełnosprawnych, co eksperci do spraw bezpieczeństwa traktują jako lukę systemową pozwalającą ingerować w cały system wyborczy. Ponadto stawiany jest zarzut naruszenia zasady równouprawnienia poprzez przyjęcie odmiennego sposobu głosowania dla osób niepełnosprawnych. Z kolei za korzystaniem z narzędzi elektronicznych w rejestrowaniu głosów oddanych na poszczególnych kandydatów przemawiają m.in. negatywne doświadczenia z wyborów prezydenckich w 2000 r., kiedy to liczenie głosów oddanych w tradycyjny sposób przeciągnęło się na Florydzie do sześciu tygodni[24].

Ostatnie miesiące przed wyborami prezydenckimi w USA w 2020 r. przyniosły nieco inne rozstawienie akcentów w debacie na temat bezpieczeństwa wyborów. Donald Trump zaczął bowiem eksponować zagrożenia związane

[22] https://www.politico.com/story/2019/06/27/paperless-voting-machines-eac-survey-1385307.

[23] https://www.politico.com/interactives/2019/election-security-americas-voting-machines/; https://www.politico.com/story/2019/08/05/election-security-cybersecurity-1445539; https://www.politico.com/story/2019/08/05/election-security-texas-1445537.

[24] Tamże.

z popieraną przez Demokratów korespondencyjną formą głosowania. Doszło do bezprecedensowego starcia, w którym prezydent USA wyraźnie się nie krył z zamiarem zmniejszenia – przez zmiany kadrowe, organizacyjne i finansowe – zdolności poczty do skutecznej obsługi głosowania korespondencyjnego. Sprawy zagrożeń internetowych, jakie niosą ze sobą kampanie wpływu prowadzone przez media społecznościowe i tradycyjne, nie zniknęły jednak z agendy publicznej. O ich aktualności przypominały kolejne oświadczenia przedstawicieli kierownictwa Wspólnoty Wywiadów (Intelligence Community) i innych służb bezpieczeństwa. W swoim oświadczeniu z dnia 7 sierpnia 2020 r. dyrektor Narodowego Centrum Kontrwywiadu i Bezpieczeństwa (National Counterintelligence and Security Center, NCSC) przyznał, że należy się spodziewać, iż przed wyborami w USA w 2020 r. „obce państwa będą nadal stosować tajne i jawne środki wywierania wpływu, próbując wpływać na preferencje i perspektywy amerykańskich wyborców, zmieniać politykę USA, zwiększać podziały w Stanach Zjednoczonych i podważać zaufanie Amerykanów do (…) demokratycznych procesów. Mogą również próbować naruszyć (…) infrastrukturę wyborczą", posługując się takimi metodami, jak ingerowanie w proces głosowania, kradzież wrażliwych danych lub kwestionowanie ważności wyników wyborów[25]. Jako potencjalnych agresorów dyrektor NCSC William Evanina wskazał Chiny – zainteresowane porażką Trumpa, Rosję – znajdującą się na kursie kolizyjnym przede wszystkim z kandydatem Demokratów, i Iran – dążący do podważenia zaufania do amerykańskich wyborów i destabilizacji sytuacji w USA. Pojawiały się ostrzeżenia przed kolejną ingerencją zewnętrzną w wybory, powrócił też temat niedoskonałości urządzeń elektronicznych wykorzystywanych w wyborach, zwłaszcza urządzeń stosowanych do rejestracji wyborców (które nie podlegają certyfikacji na szczeblu federalnym) oraz elektronicznych maszyn do głosowania używanych w lokalach wyborczych[26]. Jak dotychczas, nie ma informacji wskazujących na to, że w czasie wyborów prezydenckich w 2020 r. doszło do ingerencji w elektroniczne systemy wyborcze. Nie ma też sygnałów mówiących o tym, że na zachowania wyborców wpłynął zmasowany atak propagandowy prowadzony spoza USA za pomocą komunikatorów internetowych. W chwili oddawania tej książki do druku jest za wcześnie, aby oceniać, czy państwa, które są znane z tego, że wykorzystują internet do osiągania swoich celów politycznych, w tym przypadku ograniczyły swoje działania czy też tylko zmodyfikowały aktywność w sposób utrudniający jej wykrycie. Zgodnie z obowiązującymi przepisami, stanowisko służb specjalnych dotyczące ingerencji w wybory powinno zostać opracowane w ciągu 45 dni od dnia głosowania, a następnie przedstawione

[25] https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

[26] https://www.politico.com/news/2020/08/31/election-security-hole-406471.

opinii publicznej w formie raportu. Zmiana na stanowisku prezydenta USA może spowodować opóźnienie w opublikowaniu tych informacji.

Należy dodać, że powszechne użycie technologii elektronicznych w procedurach związanych z wyborami, w tym przyjęcie trybu głosowania przez internet, nie może się obyć bez spełnienia wielu warunków wstępnych, wymaga czasu, kompetencji i znacznych nakładów finansowych. Chodzi tu w szczególności o: pełny i równy dostęp do internetu, w tym zagwarantowanie drożnych, szerokopasmowych kanałów komunikacji elektronicznej; stworzenie narzędzi powszechnej identyfikacji elektronicznej poszczególnych obywateli przy równoczesnym zapewnieniu tajności zachowań wyborczych; zagwarantowanie bezpieczeństwa procesu wyborczego oraz skonstruowanie osłony całego systemu przed niebezpieczeństwem manipulacji i fałszerstw na wszystkich jego etapach.

Trzeba pamiętać, że proces przenoszenia wyborów do internetu ma istotne uwarunkowania i implikacje prawne, co raczej nie pozwala na podejmowanie pospiesznych decyzji o wykorzystaniu w nim najnowszych narzędzi i rozwiązań IT. Obowiązujące współcześnie prawo wyborcze było tworzone w poprzedniej (przedcyfrowej) epoce komunikacji społecznej, kiedy w kampaniach wyborczych kładziono nacisk na kontakty bezpośrednie z elektoratem i posługiwano się tradycyjnymi środkami wizualnymi (np. plakatami) i mediami, w tym przede wszystkim przekazem telewizyjnym[27]. Na ogół nie ma w tym prawie odniesień do aktywności trolli i botów, handlu metadanymi oraz do konsekwencji działania platform i programów internetowych, takich jak Google, YouTube, Twitter czy Facebook. W kontekście zmian w mechanizmach masowej, zindywidualizowanej komunikacji społecznej liczne przepisy obecnie wymagają już rewizji. Zawarte w nich rozwiązania mające gwarantować ograniczenie możliwości manipulowania zachowaniami wyborców nie przystają do realiów interaktywnej komunikacji społecznej. Wyrazistym przykładem rozwiązania przestarzałego, coraz bardziej fikcyjnego, jest cisza wyborcza. To samo można powiedzieć o skrupulatnym wyliczeniu wydatków na kampanię wyborczą, bo przecież nie da się ustalić dokładnych kosztów kampanii internetowej. Trzeba zaznaczyć, że w większości państw podstawowe zasady wyborcze stanowią materię konstytucyjną. Wszelkie zmiany w tym obszarze wymagają więc przeprowadzenia – zazwyczaj trudnych politycznie i skomplikowanych proceduralnie – nowelizacji konstytucji[28].

---

[27] Zob. A. Jaskiernia, *Media masowe w demokratycznych procesach wyborczych. Standardy europejskie i uwarunkowania ich realizacji*, Warszawa 2008.

[28] Zob.: M. Rulka, *E-voting a zasady prawa wyborczego*, „Przegląd Sejmowy" 2017, nr 3; tegoż, *Orzecznictwo dotyczące konstytucyjności regulacji umożliwiających głosowanie elektroniczne (Niemcy, Austria, Estonia, Indie)*, „Przegląd Sejmowy" 2015, nr 6; D. Mider, *Głosowanie przez Internet a demokracja*, „Studia Politologiczne" 2011, t. 20.

Na świecie są już podejmowane próby normatywnej standaryzacji procedur głosowania elektronicznego, traktowanego jako alternatywa wobec podstawowej formy, tj. oddania głosu w lokalu wyborczym. W ramach prac instytucji wchodzących w skład systemu Rady Europy można tu wskazać: kodeks dobrych praktyk wyborczych przygotowany przez Komisję Wenecką, dokument Komitetu Ministrów Rady Europy z 2004 r. zawierający stanowisko w sprawie prawnych, praktycznych i technicznych standardów głosowania elektronicznego, kolejny dokument Komitetu Ministrów, z 2017 r., mówiący bardziej szczegółowo o głosowaniu za pomocą internetu[29].

Regulacji prawnej wymaga także posługiwanie się w wyborach elektronicznych – kontrowersyjną, jak już wcześniej sygnalizowałem – metodą rejestracji i identyfikacji wyborców na podstawie danych biometrycznych. Ta technologia (Biometric Voter Registration), rozpoznająca unikalne cechy fizyczne wyborcy, takie jak rysy twarzy lub odciski palców, jest już obecnie stosowana w celu wyeliminowania kradzieży tożsamości i przypadków wielokrotnego głosowania. Według danych IDEA, które przedstawiły Dana Iverson i Andrea Garland, ta technologia jest wykorzystywana w procesie rejestracji wyborców w około 25% państw, a w 35% państw stosuje się ją w lokalach wyborczych. W 9% państw stanowi ona podstawowe narzędzie weryfikacji tożsamości wyborcy. Są to głównie państwa położone w Afryce, Azji Zachodniej i Ameryce Łacińskiej. Identyfikacja odbywa się za pomocą zdjęć (m.in. w Indiach, Pakistanie i Afganistanie), skanowania odcisków palców (m.in. w Maroku, Kolumbii i Peru) lub przy użyciu obu tych identyfikatorów (m.in. w Meksyku, Nigerii i Mozambiku). W Brazylii oprócz zdjęć i odcisków palców są także weryfikowane wzory podpisów[30].

Nasuwają się tu – rzecz jasna – pytania o bezpieczeństwo danych zarejestrowanych przez kamerę lub czujnik i o zasady ich przechowywania. Odrębnym problemem w niektórych państwach są obowiązujące w nich kody kulturowe. We wspomnianej wyżej analizie wspomina się w tym kontekście o Papui Nowej Gwinei i wiejskich obszarach Nigerii, gdzie zdjęcia są traktowane jako

[29] *Code of good practice in electoral matters. Guidelines and explanatory report. Adopted by the Venice Commission at its 52nd session (Venice, 18–19 October 2002)*, opinion no 190/2002; *Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting. (Adopted by the Committee of Ministers on 30 September 2004…); Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. (Adopted by the Committee of Ministers on 14 June 2017…)*. Zob. też J. Jaskiernia, *Alternatywne sposoby głosowania w świetle prac instytucji systemu Rady Europy*, w: S. Grabowska, R. Grabowski (red.), *Międzynarodowa Konferencja Naukowa nt. Alternatywne sposoby głosowania a aktywizacja elektoratu*, Rzeszów 2007.

[30] https://www.idea.int/news-media/news/five-things-know-about-biometric-voter-registration. Zob. też raport na temat problemów i implikacji związanych z zastosowaniem biometrii w wyborach: https://www.idea.int/publications/catalogue/introducing-biometric-technology-elections?lang=en.

zagrożenie – coś, co może „wyrządzić duchowe szkody". Problemy mogą też wynikać z obowiązku noszenia w krajach islamskich przez kobiety nakrycia głowy, bo uniemożliwia to dokładne ustalenie rysów ich twarzy.

Uwzględniając wszystkie zasygnalizowane wyżej uwarunkowania i przesłanki rozwoju republiki elektronicznej, w której podstawowe znaczenie będą miały mechanizmy demokracji elektronicznej, warto – jak już zaznaczałem – zachować dużą wstrzemięźliwość w prognozowaniu bardzo szybkiego upowszechnienia się w praktyce tego modelu demokracji. Do blokad rozwoju zaliczyłbym m.in. trudności w szybkim przeniesieniu wyborów władz publicznych do internetu oraz w zwiększeniu liczby decyzji podejmowanych bezpośrednio przez ludzi w trybie referendów. Niemniej jednak, projekty włączenia narzędzi elektronicznych, w tym internetu, do procesów wyborczych z pewnością – w niedalekim horyzoncie czasowym – doczekają się realizacji. Również na zagrożenia bezpieczeństwa wyborów elektronicznych znajdzie się jakieś antidotum – można mieć nadzieję, że lepsza będzie ochrona cyberprzestrzeni, w tym także przy użyciu narzędzi sztucznej inteligencji. Zwolennicy wyborów elektronicznych zwracają uwagę na to, że już obecnie, mimo wszystkich (sygnalizowanych wcześniej w tej książce) trudności, narzędzia elektroniczne są wykorzystywane coraz powszechniej w bankowości oraz w sprawach podatkowych i w innych obszarach e-administracji. Jak się okazuje, w przestrzeni internetowej da się już zagwarantować w kontaktach elektronicznych niezbędny poziom bezpieczeństwa oraz udokumentowania poszczególnych operacji systemowych. Oczywiście, trzeba sobie zdawać sprawę z tego, że odpowiedzią na doskonalenie kluczy kryptograficznych i zabezpieczeń cyberprzestrzeni będzie doskonalenie narzędzi używanych przez internetowych przestępców i manipulantów (czy na odwrót – bo nieraz przestępcy są o krok do przodu w tym wyścigu)… Zaś co do procesów wyborczych, dużo będzie zależało od umiejętności współpracy między państwami w identyfikowaniu i ograniczaniu ryzyka związanego ze stosowaniem w nich narzędzi elektronicznych[31]. Należy oczekiwać, że postęp w dziedzinie technologii elektronicznych pozwoli podnieść poziom niezawodności sprzętu i sieci oraz przejrzystości procesów wyborczych. Można się też spodziewać, że zostanie rozwiązany problem uzależnienia działania organów wyborczych od programów i sprzętu produkowanego przez biznesowych partnerów zewnętrznych. Wreszcie, zapewne uda się także pokonać techniczne ograniczenia dostępności internetu i wypracować niezbędne prawne uregulowania demokracji elektronicznej.

Nie tracąc z oczu wymienionych wyżej kwestii i uwarunkowań – technicznych, ekonomicznych, prawnych – trzeba mieć na uwadze fakt, że o przyszłości

[31] Zob. interesujące studium na temat cyberbezpieczeństwa wyborczego, w którym S. van der Staak i P. Wolf omawiają dobre praktyki w tej dziedzinie na 20 przykładach z różnych państw, https://www.idea.int/publications/catalogue/cybersecurity-in-elections.

demokracji elektronicznej zadecydują przede wszystkim uwarunkowania społeczne. Jak zwykle najważniejsze i najtrudniejsze są bowiem wyzwania dotyczące kształtowania postaw i zachowań ludzi. Niezwykłej ostrożności wymaga ingerowanie w sferę społecznych nawyków i praktyk opartych na tradycji; projekty upowszechnienia demokracji elektronicznej zawsze należy rozpatrywać w kontekście przyjętego w danym kraju modelu kultury politycznej i prawnej. Podstawowe znaczenie będzie miał poziom gotowości i przyzwolenia społecznego na korzystanie z nowych rozwiązań, a zwłaszcza poziom zainteresowania obywateli bezpośrednim udziałem w decydowaniu o sprawach publicznych w ramach referendów[32]. Toomas Hendrik Ilves, były prezydent Estonii, jako kwestię kluczową dla procesu cyfryzacji wyborów wskazał poziom zaufania do nowych rozwiązań. Jego zdaniem, „przyszłość rządzenia będzie cyfrowa", ale nie wolno zapominać, że system głosowania internetowego jest problemem politycznym, zaś przy jego wprowadzaniu „najważniejsze jest, żeby ludzie mu ufali"[33]. W krajach, w których występuje deficyt zaufania do władz publicznych i utrzymuje się atmosfera podejrzliwości wobec wszystkich i wszystkiego (a więc także urządzeń komunikacji cyfrowej), może to przemawiać za trzymaniem się tradycyjnych technik głosowania i metod decydowania w sprawach publicznych. W takich krajach (a Polska do nich niewątpliwie się zalicza) społeczeństwa nie od razu oswoją się z myślą, że narzędzia cyfrowe mają odgrywać coraz większą rolę w organizowaniu i przeprowadzaniu wyborów powszechnych.

Wdrażanie rozwiązań informatycznych do praktyki wywiązywania się z praw i obowiązków obywatelskich poprzez udział w wyborach rodzi istotne pytania dotykające samej istoty demokracji. Tutaj nie chodzi już o trudności z zagwarantowaniem w takim głosowaniu bezpieczeństwa oraz pewności identyfikacji wyborców i tajności ich zachowań, lecz o to, że tryb aktywności obywatelskiej online niezbyt pasuje do współczesnego modelu wspólnotowości politycznej i pozbawia wybory cech zbiorowej obywatelskiej mobilizacji. Głosowanie nie w lokalu wyborczym, lecz we własnym lokum, w domowym zaciszu, w jakimś sensie „prywatyzuje" akt wyborczy, mający przecież publiczny charakter. Można też mieć poważne wątpliwości, czy w sprawach wdrażania elektronicznych wyborów i ograniczania decydowania przez organy przedstawicielskie na rzecz referendów uda się uzyskać niezbędne poparcie ze strony partii politycznych, których reprezentanci w organach władzy publicznej muszą zaakceptować takie projekty.

Z dotychczasowych spostrzeżeń dotyczących uwarunkowań rozwoju demokracji elektronicznej wynika, że nie można postawić znaku równości między

---

[32] Zob. M. Musiał-Karg, *Głosowanie elektroniczne jako alternatywna metoda uczestnictwa w wyborach – opinie Polaków*, „Political Preferences" 2015, nr 10, s. 87 i nast.

[33] https://tvn24.pl/magazyn-tvn24/zadnych-rewolucji-w-glosowaniu-to-jest-proces-ktory-zajmuje-lata,267,4674.

osiągnięciem technicznej zdolności do wprowadzania przyjętych rozwiązań a praktycznym ich wykorzystywaniem. Mimo dostępności nowych rozwiązań technologicznych nie należy się spodziewać szybkiego tempa przenoszenia procedur wyborczych i decydowania politycznego do cyberprzestrzeni. Prawdopodobnie jeszcze dość długo w tej sferze narzędzia internetowe będą używane tylko pomocniczo i w ograniczonym zakresie. Mogą się jednak pojawić czynniki przyspieszające wdrażanie technik elektronicznych do zadań związanych z wykonywaniem praw i obowiązków obywatelskich oraz kształtowaniem nowego modelu rządzenia. Mam tu na myśli m.in. upowszechnienie rozwiązań internetu ciała. Wraz z rozwojem sztucznej inteligencji wyłaniają się nowe możliwości – właśnie w ramach internetu ciała bardziej realne staje się tworzenie mechanizmów bezpośredniej, permanentnej komunikacji między ludźmi i platformami internetowymi zbierającymi sygnały rejestrowane u tych ludzi mówiące o ich stanowisku w danych sprawach, w tym w sprawie legitymizacji władzy. Kwestią techniczną będzie oczywiście zachowanie w wybranych procedurach standardów bezpieczeństwa i prywatności poszczególnych osób. W najdalej idącej wersji tych innowacyjnych rozwiązań, pewnego dnia elektroniczne centra wyborcze pobiorą od wyborców w sposób automatyczny, przy użyciu łączy i mechanizmów internetu ciała, dane na temat ich preferencji wyborczych i za pomocą bezpiecznych aplikacji przetworzą te dane na głosy poparcia dla określonych podmiotów politycznych. Podobny mechanizm mógłby zostać użyty do ustalenia stanowiska wyborców w konkretnych sprawach skierowanych do rozstrzygnięcia w trybie elektronicznego referendum. Oczywiście, są to plany na dość odległą przyszłość, trudno się dziś wypowiadać o szansach i horyzoncie czasowym ich realizacji. W jeszcze większej mierze odnosi się to do rozwiązania polegającego na tym, że wyborca, wyrażając swoje różnorakie preferencje (np. polityczne, ideologiczne, osobowościowe, a nawet… estetyczne), będzie tym samym dokonywał wyboru personalnego – za pomocą algorytmów stanowiących podstawę elektronicznych programów komputerowych identyfikujących profile poszczególnych polityków i ugrupowań politycznych. Dziś wygląda to jeszcze na pomysł zaczerpnięty ze świata fantastyki naukowej, ale obserwując tempo i kierunki rozwoju narzędzi sztucznej inteligencji, można być niemal pewnym, że kiedyś takie rozwiązanie doczeka się realizacji. Całkiem realny jest natomiast wariant polegający na wspomaganiu się w dokonywanym wyborze politycznym aplikacjami i programami komputerowymi. Wyborca nie oddawałby więc swojego głosu w zarząd aplikacji, lecz posługiwałby się aplikacją przy dokonywaniu wyboru. Trzeba zresztą zaznaczyć, że to rozwiązanie jest już praktycznie stosowane. Jak zauważa Jamie Bartlett: „Już teraz istnieje zatrzęsienie aplikacji, które zaprojektowano w dobrej wierze, by pomóc nam w decyzji, na kogo głosować. Wpisujemy swoje poglądy i preferencje, a maszyna wyrzuca nazwę par-

tii. Prawie pięć milionów Brytyjczyków skorzystało już z aplikacji iSideWith (JestemZa) w kilku różnych wyborach”[34].

Nie musimy więc używać czasu przyszłego i odwoływać się do wyobraźni, gdy mówimy o roli cyfryzacji w procesie wyborczym, bo narzędzia elektroniczne już w tej chwili są wykorzystywane do tworzenia sieci politycznych alternatywnych wobec partii politycznych i innych podmiotów politycznych. Służą pozyskiwaniu i organizowaniu zwolenników poszczególnych programów i struktur instytucjonalnych w polityce, używa się ich do promocji i walki politycznej. Narzędzia komunikacji elektronicznej są też już uwzględniane w procedurach decydowania w partiach politycznych. Przykładem może być mechanizm decyzyjny we włoskim Ruchu Pięciu Gwiazd (Movimento 5 Stelle, M5S). Około stu tysięcy osób, które są zarejestrowane na internetowym forum Rousseau M5S, ma możliwość wypowiadania się w trybie elektronicznym w ogłaszanych sukcesywnie wewnątrzpartyjnych referendach dotyczących strategicznych decyzji partii. W tym trybie rozstrzygnięto m.in. kwestię wejścia tego ugrupowania w 2019 r. do rządu. Demokracja internetowa jest w tej partii praktykowana i traktowana jako jedna z głównych zasad jej funkcjonowania, mimo napięć wynikających z ataków hakerów i oskarżeń o brak wystarczającej ochrony danych osobowych użytkowników[35].

Pojawianie się tych czy innych zagrożeń wymaga oczywiście podejmowania działań naprawczych w celu ich eliminowania bądź ograniczania, natomiast w żadnym razie nie jest argumentem przemawiającym za niestosowaniem nowych technologii w decydowaniu politycznym.

Obecnie mechanizmy cyfrowe są wykorzystywane w procesie decyzyjnym przez niewiele partii i ruchów politycznych. Należy się spodziewać, że w wyniku postępującej cyfryzacji elektroniczny tryb decydowania będzie stopniowo wprowadzany w coraz większej liczbie podmiotów politycznych.

11.3. Nieuchronność dalszej cyfryzacji administracji i polityk publicznych oraz realna możliwość wykorzystywania w sferze publicznej elektronicznych procedur decyzyjnych

Zmiany w sferze polityk publicznych jako efekt ekspansji technologii cyfrowych i budowania systemu państwa cyfrowego • Nieuniknione zmiany na płaszczyźnie stosunków społecznych i w obszarze rynku pracy • Postępujące zmiany modelu i obszaru konkurencji między państwami • Prawdopodobieństwo upowszechnienia się w przestrzeni publicznej elektronicznych mechanizmów i procedur decyzyjnych

[34] J. Bartlett, *Ludzie przeciw technologii…*, s. 40–41.

[35] https://www.theguardian.com/world/2019/sep/02/m5s-online-vote-whether-form-italy-coalition.

Nadal nie wiadomo, jak – w bliższej lub dalszej przyszłości – będą wyglądały elektroniczne wybory powszechne, natomiast możemy z dużą dozą pewności powiedzieć, w jaki sposób cyfryzacja wpłynie na działanie administracji publicznej i prowadzenie polityk publicznych już w nieodległym czasie. Pojawianie się kolejnych narzędzi cywilizacji cyfrowej, w tym szczególnie sztucznej inteligencji, doprowadzi w tym obszarze do gruntownych zmian. Po pierwsze – przekształceniu ulegnie katalog polityk publicznych, zostaną do niego wpisane polityki odnoszące się wprost do cyfryzacji. Po wtóre – zmieni się zbiór środków działania dostępnych w prowadzeniu poszczególnych polityk; w wielu sprawach będzie można sięgać po narzędzia cyfrowe. Po trzecie – zajdą zmiany w kryteriach, które muszą być brane pod uwagę w działaniach podejmowanych w przestrzeni publicznej; na jedną z czołowych pozycji wysunie się cyberbezpieczeństwo oraz wymiar etyczny prac wdrożeniowych w dziedzinie cyfryzacji. Po czwarte – powstaną możliwości znacznego ograniczenia bezpośredniego zaangażowania ludzi w działania obarczone dużym ryzykiem utraty życia lub zdrowia oraz wiążące się z największym wysiłkiem fizycznym, wiele prac będzie wykonywanych za pomocą urządzeń cyfrowych.

Jak wcześniej wskazywałem, rozwiązania e-administracji stanowią już obecnie element kształtowania państwa cyfrowego. Narzędzia sztucznej inteligencji są coraz częściej używane do racjonalizowania i optymalizowania działań w ramach polityk publicznych. Pozwala to przyspieszać procesy decyzyjne, obiektywizować i standaryzować kryteria wyboru kierunku i sposobu działania oraz umożliwia realizację scenariuszy, które dotychczas ze względów technicznych były niewykonalne.

Dalsza ekspansja technologii elektronicznej będzie nieść za sobą poważne konsekwencje natury społecznej oraz głębokie przeobrażenia rynku pracy[36]. Rządzenie i decydowanie polityczne stanie wkrótce w obliczu nowej odmiany uwarstwienia społecznego; sytuacji, w której na to, jak przebiega linia podziału w społeczeństwie, będzie w większym stopniu wpływał dostęp do narzędzi cyfrowych, do nowych technologii informatycznych, do sieci internetowej. W następstwie doskonalenia konstrukcji różnorodnych robotów może – czy raczej musi – dojść do podziału ludzi na potrzebnych w świecie cyfrowym, którzy będą stanowić mniejszość, oraz na zawodowo nieprzydatnych, zbędnych w tym świecie. Ci ostatni zajmą miejsce przypisane historycznie klasom lub warstwom wyzyskiwanym. Od połowy XIX wieku ludzie uczą się zastępować lub przynajmniej wspomagać swoje działania za pomocą automatów i różnego rodzaju produktów postępu naukowo-technicznego. Kilka razy wieszczono już, że postęp techniczny zdecydowanie ograniczy zapotrzebowanie na aktywność

[36] J. Stawnicka, D. Morańska, W. Kubies (red.), *Świat nowych technologii. Czy sztuczna inteligencja zdominuje życie człowieka?*, Sosnowiec 2020.

zawodową ludzi i przełoży się na lawinowy wzrost bezrobocia, gdyż maszyny – działające bardziej perfekcyjnie i niemające „złych dni" – zastąpią ludzi, zabiorą im pracę. Ta prognoza dotychczas się (w pełnym wymiarze) nie sprawdziła. Człowiek nadal panuje nad światem robotów i algorytmów, bowiem to on, na swoich zasadach i warunkach, uruchamia ich potencjał. Trzeba jednak zauważyć, że w zastosowaniach nowych technologii dochodzi do istotnych zmian. Początkowo możliwości tych technologii były wykorzystywane głównie w procesie produkcyjnym, w pracach odtwórczych, wymagających jedynie wysiłku fizycznego, z czasem jednak potencjał cyfrowy zaczęto także angażować do opracowywania analiz, ocen i prognoz. Oznaczało to jakościowy postęp, ale też zapowiadało poważny problem. Chodzi o to, że decyzje podejmowane przez ludzi (także wydawane przez nich dyrektywy, rekomendacje, wytyczne itp.), będące rezultatem ich procesów myślowych, mogą stać w sprzeczności z dyspozycjami wypracowanymi przez urządzenia cyfrowe. Taka sytuacja to nic innego, jak spór decyzyjny – tyle że w niekonwencjonalnej obsadzie… Prawdziwym zaś przełomem byłoby wejście do gry robotów mających zdolności kognitywne (poznawcze), prościej zaś mówiąc – robotów myślących, a nie tylko działających na podstawie algorytmów. (Powrócę jeszcze do tego wątku).

Tak więc, groźba wypierania ludzi przez narzędzia cyfrowe z rynku pracy urealnia się, zgodnie z sygnalizowanymi wyżej przepowiedniami. W tym kontekście na uwagę zasługują wyniki badań przeprowadzonych w University of Oxford, które opublikowano w 2013 r. Opierając się na analizie 702 zawodów, stwierdzono, że w zderzeniu z uczącymi się urządzeniami sztucznej inteligencji mocno zagrożone automatyzacją jest w USA w perspektywie kilkudziesięciu lat aż 47% miejsc pracy, dalsze 19% miejsc pracy uznano za średnio zagrożone[37]. W czarnym scenariuszu, opartym na różnych badaniach (przeprowadzonych m.in. przez firmę Pearson oraz omawianych w raporcie World Economic Forum), który przedstawia Michał Duszczyk, 20% zawodów zniknie całkowicie w związku z ich mechanizacją, a 70% ulegnie zmianom koniecznym do przystosowania ich do nowych realiów. Już w 2022 r. aż 42% przepracowanych godzin przypadnie w udziale maszynom.

W 2017 r. wartość rynku robotów na świecie wyniosła około 80 miliardów dolarów. Globalny rynek robotów rośnie w tempie od 10 do 15% rocznie. Automatyzacja, która skutkuje spadkiem zapotrzebowania na pracę ludzi w branżach o wysokim udziale pracy fizycznej oraz na stanowiskach pracy opartych na powtarzalnych i standardowych procedurach, stwarza oczywiście zapotrzebowanie na nowe miejsca pracy w zawodach związanych z informatyką. Nie da się jednak „zagospodarować" zbytecznej, nisko wykwalifikowanej siły roboczej poprzez przesunięcie jej do sektora informatycznego, gdyż

[37] J. Kaplan, *Sztuczna inteligencja*…, s. 147 i nast.

tam niezbędne są specjalistyczne kwalifikacje zawodowe. Już obecnie stawia to przed polityką państwa konkretne wyzwania w sferze edukacji. Tendencje, które są obserwowane współcześnie na rynkach pracy w wielu krajach, występują także w Polsce, chociaż robotyzacja przebiega u nas stosunkowo wolno. Z raportu OECD wynika, że do 2030 r. w Polsce praca wykonywana aktualnie przez ludzi zostanie w 49% zautomatyzowana. Może to oczywiście ograniczyć negatywne skutki zmniejszenia się liczby osób w wieku produkcyjnym, ale stanie się tak tylko wówczas, gdy państwo ukierunkuje edukację, a zwłaszcza kształcenie zawodowe, na zdobywanie kompetencji przydatnych w epoce cyfrowej[38].

Pod wpływem rozwoju inteligentnych technologii cyfrowych zapewne zajdą zasadnicze zmiany w sferze stosunków międzynarodowych. Jak już wcześniej sygnalizowałem, gwałtowne przyspieszenie postępu naukowo-technicznego będzie prowadzić do zmian modelu oraz obszaru konkurencji i walki między państwami, a w konsekwencji – do istotnych przekształceń geopolitycznych w świecie. Państwom narodowym wyrasta poważny i zyskujący na znaczeniu konkurent – podmioty ponadnarodowe, które w licznych sprawach już osiągają nad nimi przewagę. Zmieniać się też będą formy kontaktów między podmiotami prawa międzynarodowego. Tradycyjne kontakty i negocjacje polityków i dyplomatów ustępują często miejsca procedurom określanym jako „elektroniczna dyplomacja".

Wspólna przestrzeń informacyjna będzie wzmacniać tendencje globalizacyjne i wpływać na przyspieszenie przekształceń cywilizacyjnych i kulturowych. Powszechny dostęp do tłumaczenia w czasie rzeczywistym sprawi, że będzie się zmieniać znaczenie tożsamości językowej poszczególnych grup narodowych i zmaleje znaczenie zróżnicowania językowego ludzkości.

Nowe możliwości pozyskiwania informacji i zarządzania ich zasobami, a także rozbudowywane i doskonalone komputerowe systemy wspomagania procesów decyzyjnych z pewnością przyczynią się do rozwoju mechanizmów online w decydowaniu publicznym. Elektroniczne procedury decyzyjne będą w coraz większym stopniu uzupełniać, a w dalszej kolejności wypierać tradycyjne – pozostające w gestii polityków i technokratów władzy – decydowanie w sprawach publicznych. Tempo podejmowania decyzji przez polityków, nawet tych, którzy mają cechy niezbędne do sprawnego wykonywania władzy, może się okazać zbyt wolne w sytuacji zdominowanej przez konieczność szybkiego przetwarzania danych w obszarach istotnych dla rządzenia. Jak słusznie zauważa Harari, instytucje i rozwiązania polityczne dominujące współcześnie w decydowaniu publicznym, tzn. wybory, partie polityczne i parlamenty, „powstały

[38] Zob. M. Duszczyk, *Robotyzacja może być szokiem. Bezrobocie i nowe podatki?*, https://cyfrowa.rp.pl/technologie/36713-robotyzacja-przyniesie-bezrobocie-i-nowe-podatki?utm_source=rp&utm_medium=teaser_redirect.

w epoce, w której polityka była szybsza od techniki", a tymczasem „Rewolucje technologiczne pozostawiają teraz w tyle procesy dokonujące się w polityce, sprawiając, że zarówno parlamentarzyści, jak i wyborcy tracą kontrolę"[39].

W następstwie zmian w świecie technologii, w dalszej przyszłości realne jest pojawienie się w obszarze publicznym nowego autonomizującego się podmiotu: decyzyjnych maszyn elektronicznych. Już nie wydaje się to scenariuszem rodem z literatury czy filmów *science fiction*. Wyżej poruszyłem już tę kwestię, mówiąc o możliwości kolizji decyzyjnych na linii człowiek – maszyna cyfrowa. Nie inaczej może być w przypadku decydowania politycznego. Decyzje poszczególnych polityków i sił politycznych, wynikające z ich rozumienia sytuacji, na których ma się opierać rządzenie, będą się zderzać z wyborami wypracowywanymi przez urządzenia cyfrowe na podstawie algorytmów. Będzie to rodzić nowe, w dużej mierze jeszcze nierozpoznane wyzwania, niebezpieczeństwa i konflikty. Algorytmy są bowiem tworzone przez ludzi i odzwierciedlają ich preferencje i ograniczenia. Dotychczasowa praktyka, przede wszystkim w sferze działania mediów społecznych i elektronicznych wyszukiwarek, pokazuje znaczną nieprzejrzystość świata algorytmów. Dziś jest za wcześnie, aby wyrokować, czy udział decyzyjnych maszyn elektronicznych w kreowaniu polityki będzie oznaczał prymat technologii w rządzeniu. Bardziej prawdopodobne jest, że politycy uzyskają dzięki temu nowy, mniej przejrzysty mechanizm rządzenia.

11.4. Strategiczna aktualność pytań o przyszłość demokracji – wobec rosnącego znaczenia informacji w obszarze władzy, cywilizacji cyfrowej i sztucznej inteligencji

Znaki zapytania wokół przyszłości dzisiejszego modelu polityki, decydowania politycznego i rządzenia • Poważne wyzwanie naszych czasów: utrzymanie władzy człowieka nad jego tworami – technologią i maszyną

Na tle zjawisk i procesów ukazanych w tej książce nasuwają się zasadnicze pytania: o miejsce człowieka i obywatela w cyfrowym świecie wypełnionym przez coraz bardziej perfekcyjne twory sztucznej inteligencji (ale także przez elektroniczne gadżety – zwykle produkty chwilowej mody), o strategiczne usytuowanie oraz funkcje i struktury państwa w tej nowej rzeczywistości, a wreszcie – o możliwości przetrwania modelu klasycznej demokracji przedstawicielskiej. Te pytania oraz wiążące się z nimi kwestie i zjawiska nie powinny

[39] Y.N. Harari, *Homo deus…*, s. 475.

umykać uwadze nawet tych osób, które są zaledwie przeciętnie zainteresowane procesami informatyzacji i automatyzacji.

Upowszechnienie internetu, umocnienie się struktury sieciowej społeczeństwa oraz powstawanie globalnej sieci urządzeń sztucznej inteligencji zdolnej do autonomicznego komunikowania się z pewnością nie pozostaną bez wpływu na współczesny model polityki, decydowania politycznego i rządzenia. Oczywiście, trzeba zachować dużą ostrożność w prognozowaniu tempa zmian w tej dziedzinie, jednak bez większego ryzyka popełnienia błędu można założyć, że w perspektywie długoterminowej w sferze rządzenia będzie mniej miejsca dla mechanizmów klasycznej demokracji parlamentarnej i dla demokracji przedstawicielskiej. Wyraźniej niż w sprawach elektronicznych wyborów powszechnych rysuje się w tej chwili możliwość zwiększenia roli decydowania w trybie referendalnym. Mechanizmy demokracji przedstawicielskiej mają teraz zastosowanie głównie w decydowaniu w sprawach dotyczących kształtu konstytucji oraz w ramach prowadzenia polityk lokalnych. Ich zastosowanie na szerszą skalę, z wykorzystaniem nowoczesnych narzędzi komunikacji internetowej, stworzy podstawy do silniejszego powiązania obywateli – wyborców z reprezentującymi ich politykami. Na znaczeniu będą zyskiwać bieżące rekomendacje w szczegółowych sprawach, co może prowadzić do podważania zasadności mandatu wolnego i przemawiać na korzyść mandatu związanego (zwanego również imperatywnym).

Jak wcześniej sygnalizowałem, prognozy rozwoju demokracji elektronicznej i partycypacji politycznej w internecie nie są już tylko wizją entuzjastów cyfrowych rozwiązań – okazują się całkiem realną perspektywą zmian w domenie publicznej. Oczywiście, wdrożenie e-demokracji napotka bariery. Zastępowaniu niektórych mechanizmów demokracji przedstawicielskiej procedurami demokracji elektronicznej stoi obecnie na przeszkodzie przede wszystkim ograniczony poziom zaufania społecznego do tych procedur oraz brak bieżącej i powszechnej aktywności politycznej społeczeństwa. W mniejszym stopniu przeszkodą są niedoskonałości dzisiejszych rozwiązań technologicznych. Mimo istnienia tych czynników spowalniających rozwój e-demokracji, zmiany są nieuniknione, można być pewnym, że model demokracji nie przetrwa w swej dotychczasowej formie. Trudno bowiem przyjąć, że decydowanie w sprawach publicznych będzie wyjątkiem w toczącym się procesie przemian. Dziś nie można jeszcze orzec, jak długo zmiany będą się sprowadzały jedynie do rewizji narzędzi rządzenia, kiedy zaś zmiany będą już oznaczały rewizję samego modelu demokracji przedstawicielskiej. Można jednak zakładać, że już w perspektywie średniookresowej pojawią się różne mutacje demokracji elektronicznej wykorzystującej narzędzia komunikacji na odległość. W tym kontekście warto przywołać znamienne zdania Harariego: „Niebawem staniemy w obliczu zalewu niezwykle pożytecznych urządzeń, narzędzi i struktur,

które nie będą brały poprawki na wolną wolę poszczególnych ludzi. Czy demokracja, wolny rynek i prawa człowieka przetrwają ten potop?”[40]. Autor w lapidarnej formie zawarł tu zarówno zapowiedź tego, co nas – ludzi – czeka i co zapewne bardzo ułatwi nam życie, jak i ostrzeżenie przed tym, co nas czeka i czego skutków żadną miarą przewidzieć nie umiemy…

W refleksji na temat rządzenia w wymiarze podmiotowym podejmowano zwykle problemy aktywności osób lub grup ludzi ujętej w ramy struktur instytucjonalnych. Analiza zjawiska władzy koncentrowała się dotąd wokół relacji między ludźmi. Maszyny i algorytmy były uwzględniane w rozważaniach dotyczących władzy co najwyżej jako narzędzia, pełniące rolę pomocniczą i w pełni poddane woli ludzi. Trzeba jednak spojrzeć na nie w inny sposób, zdając sobie sprawę z możliwości – w istocie zaś niebezpieczeństwa – autonomizowania się urządzeń cyfrowych. Według czarnego scenariusza – z gatunku horroru technologicznego – maszyny wypowiedzą kiedyś ludziom posłuszeństwo, zaczną „żyć własnym życiem”. Nasuwają się tu oczywiście skojarzenia z wszelkimi wersjami opowieści o złu, które wymknęło się spod kontroli. Musimy się nastawić – choć dzisiaj taka wizja przyszłości wydaje się większości z nas wytworem bujnej wyobraźni – na to, że w dłuższej perspektywie czasowej urządzenia cyfrowe będą się stawać autonomicznymi podmiotami, np. dokonującymi wyboru ścieżek działania w przestrzeni publicznej, przestaną być tylko narzędziami polityki i zaczną pełnić samodzielną rolę jako aktorzy polityczni. Ale to wciąż jest – jak to się mówi – pieśń przyszłości; mamy więc trochę czasu na oswojenie się z tą perspektywą. A kiedy teraz myślimy o samowoli produktów elektronicznych, mamy na uwadze w pierwszej kolejności agresję różnego rodzaju wirusów internetowych, które najczęściej są świadomie tworzone przez ludzi. Wirusy te wykradają, zmieniają, likwidują zasoby naszych komputerów, łącza i identyfikatory – zgodnie z projektem swoich twórców. Ale niektóre z nich wymykają się im spod kontroli i autonomizują. To pierwsze oznaki buntu w świecie pozornie martwych tworów człowieka…

Produkty technologiczne okazują się w coraz większym stopniu zdolne do klonowania swoich zdolności już bez udziału człowieka, a nawet w opozycji do niego. Na pytanie, czy i jak długo człowiek będzie w stanie utrzymać swoje panowanie w świecie cyfrowym, nie ma obecnie jednoznacznej odpowiedzi. Z jednej strony nie udało się – jak dotychczas – obdarzyć urządzeń technologicznych niezwykłymi zdolnościami ludzkiego umysłu, nie ma też pewności, że stanie się to możliwe w przyszłości. Z drugiej zaś strony, tempo i zakres zmian w cyberprzestrzeni, postęp badań naukowych, a także zacieśniające się związki między światem rzeczywistym i wirtualnym nie pozwalają już być całkowicie pewnym, że człowiek utrzyma pełnię władzy, tzn. zachowa kontrolę nad

[40] Y.N. Harari, *Homo deus...*, s. 385. Zob. tegoż, *21 lekcji na XXI wiek*, Kraków 2018.

swoimi wytworami – produktami wysokiej technologii. Spektakularny postęp w tej dziedzinie budzi u ludzi ambiwalentne odczucia. Z kilku zdań, których autorem jest jeden z najbardziej wpływowych intelektualistów na świecie, wielokrotnie tu cytowany, można wyczytać zarówno podziw dla kreatywności, zdolności poznawczych człowieka, jak i ostrzeżenie przed uroszczeniami współczesnej nauki: „Programowanie genetyczne należy dziś do najbardziej obiecujących dziedzin informatyki. Usiłuje ono naśladować metody ewolucji genetycznej. Wielu programistów marzy o napisaniu programu potrafiącego uczyć się i ewoluować zupełnie niezależnie od swojego stwórcy. W tym wypadku programista byłby *primum mobile*, pierwszym poruszycielem, lecz jego dzieło mogłoby samoistnie ewaluować w kierunkach, których ani jego twórca, ani inni ludzie nie byliby w stanie przewidywać. Prototyp takiego programu już istnieje – to wirus komputerowy”[41].

[41] Tegoż, *Sapiens. Od zwierząt…*, s. 500.

Tytułem zakończenia

Rozważając, jaki kształt w przyszłości przybiorą – czy też w jakim kierunku będą ewoluować – polityka, decydowanie polityczne i rządzenie, warto odwoływać się nie tylko do wiedzy i doświadczenia, lecz także do intuicji. Może ona podpowiedzieć, który z rozpatrywanych scenariuszy ma największe szanse realizacji. Ale wobec istnienia wielu niewiadomych, czasem trzeba poprzestać na wskazaniu alternatywy czy wariantów scenariuszy – bez typowania zwycięzcy. Z pewnością nie zadowoli to tych, którzy oczekują jednoznacznych ustaleń, niepozostawiających marginesu wątpliwości. Podejmuję pewne ryzyko, decydując się podzielić swoimi przewidywaniami co do przyszłości polityki i rządzenia. Traktuję je jako możliwy punkt odniesienia w dyskusji o perspektywach zmian, jakie będą zachodzić w rzeczywistości wokół nas. Dyskusji, która jest konieczna, byśmy zaczęli pisać – posłużę się tu określeniem użytym przez Harariego – „krótką historię jutra".

Tak więc, poniżej przedstawiam dziesięć punktów zawierających moje oceny, opinie i prognozy, a także rekomendacje.

I. Świat staje się coraz bardziej cyfrowy. Decydują o tym następujące czynniki: rozwój internetowych narzędzi komunikacji społecznej łączących masowość i zindywidualizowanie, kształtowanie się społeczeństwa sieciowego, intensywność prac nad kolejnymi rozwiązaniami inteligentnych technologii cyfrowych i ogromne środki finansowe, które są angażowane w tej dziedzinie. Jakościowe zmiany spowodowane cyfryzacją obejmą wszystkie dziedziny życia ludzi i funkcjonowania struktur instytucjonalnych, w tym także w sferze władzy publicznej. Jak wiadomo, rządzenie jest silnie uzależnione od zdarzeń zachodzących w jego otoczeniu, w związku z czym cyfryzacja jest już obecnie obszarem współpracy, konkurencji i konfrontacji między państwami. Równocześnie w sytuacji, gdy komunikatory internetowe stały się nowym narzędziem uprawiania polityki, widać wyraźnie, że państwa podejmują działania zmierzające do utrzymania dominującej pozycji w zakresie ładu informacyjnego i komunikacyjnego na swoim terytorium. Wszystko to nakazuje sądzić, że cyfryzacja będzie w szybkim tempie zyskiwać większe znaczenie w strategiach, regulacjach i praktyce działania podmiotów międzynarodowych oraz poszczególnych państw.

II. Umacnia się władza informacji, komunikacji i technologii. Ekspansja informacji, internetowej komunikacji społecznej i cyfryzacji już teraz silnie oddziałuje na model i praktykę władzy w przestrzeni politycznej. Cyfryzacja stała się równocześnie obszarem realizacji, zadaniem i narzędziem polityki oraz rządzenia. W mediach społecznościowych ujawniają się trudności w godzeniu wolnościowej istoty komunikacji internetowej z wymogami zachowania prywatności i ochrony danych. Właściciele mediów społecznościowych oraz producenci i administratorzy programów komputerowych, głównie za sprawą swoich decyzji co do stosowania algorytmów oraz zasad monitorowania aktywności internetowej i blokowania kont użytkowników, zaczynają odgrywać samodzielną rolę w grze politycznej. Jednak biznesowy charakter tych podmiotów sprawia, że ich ważne decyzje o znaczeniu politycznym (dotyczące m.in. reklam politycznych i ograniczania języka nienawiści) są podporządkowane celom finansowym, zwłaszcza maksymalizacji zysku. Niezbędne staje się poddanie tych podmiotów kontroli zewnętrznej.

Badania i wdrożenia w dziedzinie sztucznej inteligencji przesuwają granice technologicznych możliwości. W zasięgu tych możliwości leży projektowanie autonomicznych tworów sztucznej inteligencji. Aby na bieg zdarzeń w tej dziedzinie wpływały uniwersalne wartości i wspólne interesy ludzi, musi być ona objęta ciągłym monitoringiem oraz zbiorowo wypracowanymi i skutecznie egzekwowanymi regulacjami prawnymi.

III. Intensywność i powszechność jakościowych zmian w otoczeniu polityki wymusi systemowe przewartościowania w mechanizmach rządzenia. Obecny model uzyskiwania i wykonywania władzy w przestrzeni publicznej stanie wobec zasadniczego wyzwania: radykalnej zmiany swego technicznego instrumentarium. Należy przy tym zaznaczyć, że pojawienie się możliwości sięgnięcia po nowe rozwiązania systemowe nie jest równoznaczne z ich faktycznym wykorzystaniem. Możliwości pojawiające się w związku z rozwojem technologii cyfrowych to tylko jedno z uwarunkowań zmian w mechanizmach rządzenia. Kluczowe znaczenie będą miały w tej sferze uwarunkowania społeczne: zmiany świadomościowe, w tym stopniowe wygasanie obaw związanych z cyfryzacją polityki, oraz tempo rozwoju społeczeństwa cyfrowego. Najszybciej rozwiązania elektroniczne staną się standardem w przestrzeni administracyjnej oraz w procesach decyzyjnych w strukturach instytucjonalnych państwa. Istotnych zmian należy się spodziewać w sposobach prowadzenia polityk publicznych. W tych obszarach zmiany są już w dużej mierze wprowadzane. Do ich przyspieszenia przyczyniła się pandemia 2020 r., która spowodowała gwałtowne upowszechnienie procedur elektronicznych we wszystkich dziedzinach życia i pracy ludzi.

IV. Aktualność zachowują pytania o przyszłość demokracji w warunkach szybkiego rozwoju uczenia maszynowego. Mimo iż powstały ku temu możliwości techniczne, raczej nie dojdzie do bardzo szybkiego wdrażania mechanizmów legitymizacji elektronicznej w polityce. Dotyczy to zwłaszcza wyborów powszechnych, gdyż gruntowne zmiany w tej dziedzinie wymagałyby przełamania bariery świadomości społecznej (m.in. obawy przed fałszowaniem wyborów), a rządzący nie są chyba gotowi do podjęcia wiążącego się z tym ryzyka. Koncepcja demokracji cyfrowej i projekt elektronicznych wyborów organów władzy publicznej zapewne doczekają się realizacji dopiero w dalszej przyszłości. Tempo i zakres ich urzeczywistniania będą zapewne przedmiotem zasadniczych kontrowersji. Być może długo jeszcze będą się pojawiać jedynie kolejne rozwiązania cząstkowe, polegające na pomocniczym wykorzystaniu techniki elektronicznej w wyborach powszechnych. W dyskusji na temat wprowadzenia elektronicznej formy głosowania często akcentuje się związane z tym przeszkody i niebezpieczeństwa. Siłą rzeczy więc, w centrum uwagi pozostają także działania mające na celu ograniczanie zagrożenia dezinformacją w internecie oraz zagrożenia bezpieczeństwa systemu informatycznego. Oskarżenia o dezinformację cyfrową, prowadzoną w sieci, bywają niejednokrotnie narzędziem politycznej manipulacji. Nowe możliwości, jakie dają narzędzia technologii informacyjno-komunikacyjnych, będą wykorzystywane do tworzenia wirtualnych środowisk politycznych, kształtowania wizerunków i budowania poparcia oraz walki z konkurentami politycznymi. W tym sensie można już mówić o nowym modelu uprawiania polityki, należy też oczekiwać dalszej profesjonalizacji działań. Co ważniejsze, tworzenie rozwiązań sieciowej demokracji obywatelskiej, powstającej w ramach społeczeństwa informacyjnego, będzie wzmacniać różne formy partycypacji politycznej. Wraz z rosnącą gotowością społeczeństwa do włączenia się w bieżące decydowanie publiczne za pomocą elektronicznych mechanizmów demokracji bezpośredniej, zacznie tracić na znaczeniu obecny model demokracji przedstawicielskiej.

V. Cyfryzacja ma w sobie wielki pozytywny potencjał: jest dźwignią postępu i przyczynia się do poprawy jakości działań. Ale ma też drugie oblicze: niesie ze sobą poważne zagrożenia, wywołuje liczne negatywne skutki, wywiera zgubny wpływ na pewne zjawiska i zachowania społeczne, np. coraz dotkliwszym problemem staje się uzależnienie ludzi od urządzeń i procedur elektronicznych. Nowe technologie przeniknęły już do świata polityki, gdzie bywają wykorzystywane do nieczystej gry. Ujawniają się różne patologie związane z komunikacją społeczną i cyfryzacją, w tym cyberprzestępczość oraz dezinformacja i manipulacja. Na władzy publicznej ciąży obowiązek uświadamiania społeczeństwu zagrożeń związanych z korzystaniem z narzędzi komunikacji

cyfrowej oraz budowania jego odporności na dezinformację i manipulację w internecie. W rządzeniu trzeba mieć na względzie fakt, że trwałym i ważnym komponentem bezpieczeństwa staje się bezpieczeństwo informatyczne i informacyjne. Umacnianie się władzy komunikacji oraz zwiększanie mocy dostępnych narzędzi cyfrowych, algorytmów i tworów sztucznej inteligencji rodzi potrzebę ich wnikliwej obserwacji i analizy. Należy doskonalić metody przeciwdziałania negatywnym następstwom wykorzystania narzędzi cyfrowych wynikającym ze złych intencji ludzi lub z awarii technicznych. Zagrożenia, jakie niesie ze sobą cyfryzacja, biorą się także z faktu wykorzystania jej do celów militarnych. Konflikty zbrojne mogą się przenosić – i w pewnych przypadkach przenoszą się już – do cybersfery. Co gorsza, z postępem cyfryzacji wiąże się niebezpieczeństwo obniżenia progu konfliktu przy użyciu zabójczych autonomicznych systemów broni.

Potrzebne jest globalne współdziałanie w ukierunkowywaniu i standaryzacji prac nad nowymi rozwiązaniami i urządzeniami w sferze sztucznej inteligencji. Osiągnięcie sukcesu społecznego, ekonomicznego i politycznego będzie w coraz większym stopniu uzależnione od współpracy ludzi z tworami sztucznej inteligencji. Aktualną sytuację trafnie ujął słynny rosyjski szachista Garri Kasparow, mówiąc, że wszyscy już gramy partię z maszynami[1]…

VI. Zasoby danych cyfrowych stają się czynnikiem strategicznym w rządzeniu. Już obecnie są dobrem tak samo ważnym dla egzystencji ludzi i funkcjonowania struktur instytucjonalnych, jak surowce naturalne, źródła energii i kapitał finansowy. Uzyskanie i utrzymanie dostępu do nich będzie więc w dalszym ciągu celem jawnych i niejawnych zabiegów prowadzonych przez organy władzy publicznej i podmioty pozarządowe, w tym gospodarcze. W tych działaniach należy się spodziewać występowania różnych dysfunkcji: nadużyć, zagrożenia praw i wolności oraz konfliktu interesu. W globalnych systemach magazynowania, przetwarzania i dystrybucji danych cyfrowych ubywa szans na ochronę prywatności. Walka o zapewnienie prywatności stanie się jedną z ważniejszych kwestii poruszanych w związku z cyfryzacją. Poważnym wyzwaniem politycznym będzie znajdowanie równowagi między potrzebami wolności a wymaganiami bezpieczeństwa w wykorzystywaniu danych osobowych, w tym zwłaszcza danych biometrycznych. Realnym zagrożeniem wynikającym z jednej strony z rozwoju nowoczesnych technik nadzoru, z drugiej – z braku niezbędnych regulacji prawnych, jest nieustanna inwigilacja ludzi i całych społeczeństw; koresponduje to z Benthamowskim projektem panoptykonu, w którym myśl współczesna dostrzegła alegorię społeczeństwa i świata jako

[1] Zob. P. Szostak, *Algorytmy, które przepowiadają przyszłość*, „Gazeta Wyborcza" z 12 października 2019, dodatek „Nasza Europa", s. 9.

globalnego więzienia. Błędna okazała się teza, że cyfryzacja służyć będzie wyłącznie wzmocnieniu rozwiązań demokratycznych. Rządy autokratyczne szybko nauczyły się korzystać z narzędzi cyfrowych, aby kontrolować życie społeczne i umacniać swoją władzę.

Dane zgromadzone w cyberprzestrzeni, precyzyjnie zaś: zawarty w nich zasób wiedzy, mają – przynajmniej potencjalnie – znaczenie polityczne (zgodnie z hasłem „Kto ma wiedzę, ten ma władzę"), a równocześnie stanowią wartość rynkową. Dlatego tak ważny jest dostęp do tych danych. Nierówny dostęp do danych elektronicznych, objawiający się tzw. asymetrią informacji, wynika z nowego układu sił w świecie, a zarazem układ ten współkształtuje i utrwala.

VII. Cyfryzacja i sztuczna inteligencja kształtują nowe relacje władcze w świecie i stają się przedmiotem rywalizacji politycznej i biznesowej na skalę globalną. W dziedzinie cyfryzacji należy wykorzystać doświadczenia zebrane w ramach programowania, kontrolowania oraz modyfikowania procesów zachodzących w podmiotach gospodarczych, a także zarządzania tymi procesami. Powszechną praktyką w gospodarce jest strategiczny i operacyjny *controlling*. Systematycznie analizuje się zachodzące zmiany oraz pojawiające się zagrożenia i odchylenia od założonych celów. Dzięki temu, w razie potrzeby wprowadza się niezbędne korekty i stymulanty rozwoju. Przedmiotem wnikliwej obserwacji, analizy i – jeśli jest to konieczne – modyfikacji czyni się niejednokrotnie same cele działania, a nie tylko rozwiązania wykonawcze. W kontekście decydowania politycznego i rządzenia podobnym strategicznym i operacyjnym *controllingiem* powinny zostać objęte także zjawiska ekspansji technologii informacyjno-komunikacyjnych i postępy cyfryzacji.

VIII. Rozwój zindywidualizowanej, elektronicznej komunikacji masowej oraz ekspansja cyfryzacji i sztucznej inteligencji mają znaczenie geopolityczne. Zmieniają się w ich następstwie kryteria oceny suwerenności poszczególnych państw i pozycji struktur międzynarodowych oraz międzypaństwowych. Należy przypuszczać, że będzie wzrastać znaczenie technologicznego kontekstu suwerenności. Kształtowanie się w świecie nowego, cybernetycznego porządku niesie ze sobą niebezpieczeństwo nasilenia się nierówności społecznych i ekonomicznych oraz konfliktów politycznych. Cyberprzestrzeń staje się ważnym obszarem konkurencji i konfrontacji między państwami. Geopolityka nabiera wymiaru cyfrowego. Zdolność wykorzystania danych cyfrowych i nowych technik będzie coraz istotniejszym uwarunkowaniem siły politycznej i będzie się przekładać na nową konfigurację wpływów gospodarczych w świecie. Kluczowe znaczenie już obecnie ma udział w kontroli globalnych sieci i węzłów komunikacji elektronicznej. Rośnie świadomość faktu, że sztuczna inteligencja to „przemysł przyszłości", który będzie decydować o pozycji w świecie jutra.

Państwa mocniej angażują się w działania na rzecz rozwoju inteligentnych technologii. W USA nadano im status zadania strategicznego o zasadniczym znaczeniu dla pozycji i bezpieczeństwa państwa. W Chinach stanowią one część całościowego programu narodowego. W Unii Europejskiej, która stara się odrabiać swoje zapóźnienie w tej dziedzinie, udział państw członkowskich w pracach nad rozwojem sztucznej inteligencji uznano za nadrzędne zadanie. Nasila się rywalizacja o prymat w projektach dotyczących sztucznej inteligencji, która przerodziła się w otwarty konflikt, w wojnę technologiczną między USA i Chinami. W amerykańsko-chiński spór o piątą generację sieci komórkowej (sieć 5G) są wciągane inne państwa, nie można tu więc mówić jedynie o starciu między dwoma mocarstwami.

Do rangi czynnika o znaczeniu politycznym urasta wykluczenie cyfrowe. Strategie rozwojowe, które nie uwzględniają w wystarczający sposób wykorzystania zdolności technologii cyfrowych, nie są w stanie sprostać potrzebom zrównoważonego i odpowiedzialnego rozwoju oraz wyzwaniom bezpieczeństwa.

IX. W relacjach między decydowaniem politycznym i rządzeniem a nowoczesnymi technikami i urządzeniami cyfrowymi podstawowa rola nadal będzie przypadać ludziom i kształtowanym przez nich strukturom publicznym. To od ludzi zależy – i zapewne nie zmieni się to w przyszłości – jak będą wykorzystywane rosnące możliwości nowych technologii cyfrowych i jak będzie ukierunkowywany i monitorowany ich rozwój. Ludzie stanowią najważniejszy, a zarazem najbardziej podatny na zakłócenia w funkcjonowaniu, element systemu rządzenia. Błędy i zaniechania ludzi mogą prowadzić do wzmacniania już widocznych i ujawnienia się nowych następstw „złej strony" cyfryzacji. W dłuższym okresie mogą one prowadzić wręcz do powstawania napięć między ludźmi a tworzonymi przez nich, coraz bardziej autonomizującymi się, produktami technologii cyfrowej.

X. Wzmacnianie pozytywnego oddziaływania i osłabianie negatywnych skutków cyfryzacji i sztucznej inteligencji wymaga globalnego współdziałania. Odpowiedzialność za realizację tych zadań ciąży przede wszystkim na rządzących, ale powodzenie jest uzależnione od współdziałania polityków, naukowców i technologów pracujących nad nowymi rozwiązaniami, podmiotów finansowych i gospodarczych oraz liderów organizacji i ruchów społecznych. Stanowi to wielkie wyzwanie dla prawa międzynarodowego oraz państwowych systemów normatywnych. Zasadnicze znaczenie ma umiejętność wypracowania wspólnych kanonów postępowania, wychodzących poza partykularne sposoby widzenia poszczególnych kwestii i rozbieżne interesy. Potrzebne jest zbudowanie sprawnego, wyposażonego w odpowiednie narzędzia wykonawcze systemu

monitorowania i interwencji stojącego na straży przyjętych standardów. To jedno z najtrudniejszych zadań, jednak już teraz, obserwując próby działań pozytywnych, można być w tych sprawach – używając określenia zaczerpniętego z książki Maxa Tegmarka – „świadomym optymistą”[2].

W przypadku scenariuszy przyszłości – czyli „wizji przyszłych możliwości oraz dróg rozwoju”[3] – skupianie uwagi na konkretach nie jest wskazane. W miarę odpowiedzialnie można tworzyć szczegółową prognozę tylko w krótkiej perspektywie czasowej. Dotyczy to zwłaszcza dziedzin objętych dynamicznie zachodzącymi zmianami, takich jak rządzenie, komunikacja społeczna, cyfryzacja i sztuczna inteligencja. Biorąc to pod uwagę, koncentrowałem się na problemach i tendencjach, które – w świetle dzisiejszej wiedzy – mają charakter strategiczny. Tak jak zapowiadałem we wstępie do tej książki, chciałbym, by była ona nie tylko obrazem czy bilansem aktualnie zachodzących zmian na styku nowych technologii i rządzenia, lecz także zaproszeniem do wspólnego myślenia o wyzwaniach przyszłości.

[2] M. Tegmark, *Życie 3.0...*, s. 427.

[3] Zob. http://infuture.institute/scenariusze-przyszlosci.

Literatura cytowana i przywołana

Publikacje zwarte

Aboujaoude Elias, *Wirtualna osobowość naszych czasów. Mroczna strona e-osobowości*, Kraków 2012.

Adamik-Szysiak Małgorzata (red.), *Media i polityka. Relacje i współzależności*, Lublin 2014.

Adamowski Janusz (red.), *Demokracja a nowe środki komunikacji społecznej*, Warszawa 2004.

Adamski Andrzej, *Media w analogowym i cyfrowym świecie. Wpływ cyfrowej rewolucji na rekonfigurację komunikacji społecznej*, Warszawa 2012.

Adamski Andrzej, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001.

Aleksandrowicz Tomasz R., *Podstawy walki informacyjnej*, Warszawa 2016.

Ancona Matthew d', *Postprawda*, Warszawa 2018.

Angwin Julia, *Społeczeństwo nadzorowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji*, Warszawa 2020.

Bajor Piotr, Gruszczak Artur (red.), *Między wiedzą a władzą. Bezpieczeństwo w erze informacji*, Kraków 2019.

Banasiński Cezary (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.

Barney Darin, *Społeczeństwo sieci*, Warszawa 2008.

Bartlett Jamie, *Ludzie przeciw technologii. Jak Internet zabija demokrację (i jak ją możemy ocalić)*, Katowice 2019.

Baszkiewicz Jan, *Władza*, Wrocław 1999.

Bączek Piotr, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2011.

Beck Ulrich, *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Warszawa 2002.

Bendyk Edwin, *Antymatrix. Człowiek w labiryncie sieci*, Warszawa 2004.

Bendyk Edwin, *Bunt sieci*, Warszawa 2012.

Berlin Isaiah, *Cztery eseje o wolności*, Warszawa 1994.

Bilton Nick, *Król darknetu. Polowanie na genialnego cyberprzestępcę*, Sękowa 2020.

Boden Margaret A., *Sztuczna inteligencja. Jej natura i przyszłość*, Łódź 2020.

Bógdał-Brzezińska Agnieszka, Gawrycki Marcin F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*. Warszawa 2003.

Browning Gary, *Elektroniczna demokracja. Wybory w Internecie*, Warszawa 1997.

Brynjolfsson Erik, McAfee Andrew, *Drugi wiek maszyny. Praca, postęp i dobrobyt w czasach genialnych technologii*, Warszawa 2015.

Brzeski Rafał, *Wojna informacyjna – wojna nowej generacji*, Komorów 2014.

Brzeziński Zbigniew, *Between Two Ages. America's Role in the Technetronic Era*, New York 1970.
Bułat Adam, Jaroszewska-Choraś Dagmara, Kilińska-Pękacz Agnieszka (red.), *Prawne aspekty cyberprzestrzeni*, Bydgoszcz 2020.
Castells Manuel, *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, Poznań 2003.
Castells Manuel, *Siła oburzenia i nadziei. Ruchy społeczne w erze Internetu*, Warszawa 2013.
Castells Manuel, *Społeczeństwo sieci*, Warszawa 2007.
Castells Manuel, *Władza komunikacji*, Warszawa 2013.
Chałubińska-Jentkiewicz Katarzyna, *Cyberodpowiedzialność*, Toruń 2019.
Chałubińska-Jentkiewicz Katarzyna, Karpiuk Mirosław, *Prawo bezpieczeństwa informacyjn*ego, Warszawa 2015.
Chałubińska-Jentkiewicz Katarzyna, Karpiuk Mirosław, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.
Chłopecki Aleksander, *Sztuczna inteligencja. Szkice prawnicze i futurologiczne*, Warszawa 2018.
Comey James, *Wyższa lojalność. Prawda, kłamstwo i przywództwo*, Kraków 2019.
Denning Dorothy E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
Flaga-Gieruszyńska Kinga, Gołaczyński Jacek, Szostek Dariusz (red.), *E-obywatel. E-sprawiedliwość. E-usługi*, Warszawa 2017.
Foucault Michel, *Bezpieczeństwo, terytorium, populacja*, Warszawa 2010.
Foucault Michel, *Filozofia, historia, polityka. Wybór pism*, Warszawa 2004.
Foucault Michel, *Nadzorować i karać. Narodziny więzienia*, Warszawa 1998.
Freedman Lawrence, *Przyszła wojna. Wizja przyszłej wojny. Jak ją sobie wyobrażano dawniej? Jak widzimy ją dzisiaj?*, Warszawa 2019.
Friedman Allan, Singer Peter W., *Cybersecurity and Cyberwar. What everyone needs to know*, New York 2014.
Ganczar Małgorzata, *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009.
Garlicki Jan, Noga-Bogomilski Artur, *Kultura polityczna w społeczeństwie demokratycznym*, Warszawa 2004.
Gawrysiak Piotr, *Cyfrowa rewolucja. Rozwój cywilizacji informacyjnej*, Warszawa 2008.
Gęsicka Daria K., *Wyłączenie odpowiedzialności cywilnoprawnej dostawców usług sieciowych za treści użytkowników*, Warszawa 2014.
Gillespie Tarleton, *The Relevance of Algorithms*, w: Tarleton Gillespie, Pablo Boczkowski, Kristen Foot (eds.), *Media Technologies: Essays on Communication, Materiality and Society*, Cambridge 2014.
Goban-Klas Tomasz, *Komunikowanie i media masowe. Teorie prasy, radia, telewizji i Internetu*, Warszawa 1999.
Goban-Klas Tomasz, Sienkiewicz Piotr, *Społeczeństwo informacyjne. Szanse, wyzwania i zagrożenia*, Kraków 1999.
Goździewicz Sylwia, Tomaszycki Krzysztof (red.), *Prawne i społeczne aspekty cyberbezpieczeństwa*, Warszawa 2017.
Goździewicz Wiesław, *Cyberobrona i nie tylko. Rola wojska w budowaniu ekosystemu cyberbezpieczeństwa w kraju*, w: Wiesław Goździewicz i in., *Bezpieczeństwo poprzez*

innowacje. Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego, Kraków 2017.
Górka Marek, *Cyberbezpieczeństwo jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku*, Warszawa 2014.
Grabowski Radosław (red.), *Wpływ internetu na ewolucję państwa i prawa,* Rzeszów 2008.
Grabowski Tomasz W., Lakomy Mirosław, Oświecimski Konrad (red.), *Postprawda jako zagrożenie dla dyskursu publicznego*, Kraków 2018.
Greenwald Glenn, *Snowden. Nigdzie się nie ukryjesz*, Warszawa 2014.
Grossman L.K., *Republika elektroniczna*, w: Jerzy Szczupaczyński (red.), *Władza i społeczeństwo 2. Antologia tekstów z socjologii polityki*, Warszawa 1998.
Halavais Alexander, *Wyszukiwarki internetowe a społeczeństwo*, Warszawa 2012.
Harari Yuval Noah, *21 lekcji na XXI wiek*, Kraków 2018.
Harari Yuval Noah, *Homo deus. Krótka historia jutra*, Kraków 2018.
Harari Yuval Noah, *Sapiens. Od zwierząt do bogów*, Kraków 2018.
Harrel Yannick, *Rosyjska cyberstrategia*, Warszawa 2015.
Hofmokl Justyna, *Internet jako nowe dobro wspólne*, Warszawa 2009.
Hulten Geoff, *Budowanie systemów inteligentnych. Przewodnik po inżynierii uczenia się maszyn*, Warszawa 2020.
Isikoff Michael, Corn David, *Rosyjska ruletka. Jak Putin zaatakował Amerykę i wygrał wybory dla Donalda Trumpa*, Warszawa 2018.
Jankowski Jacek, *Trendy cywilizacji informacyjnej. Nowy technototalitarny porządek świata*, Warszawa 2019.
Jaskiernia Alicja, *Media masowe w demokratycznych procesach wyborczych. Standardy europejskie i uwarunkowania ich realizacji*, Warszawa 2008.
Jaskiernia Jerzy, *Alternatywne sposoby głosowania w świetle prac instytucji systemu Rady Europy*, w: Sabina Grabowska, Radosław Grabowski (red.), *Międzynarodowa Konferencja Naukowa nt. Alternatywne sposoby głosowania a aktywizacja elektoratu*, Rzeszów 2007.
Jeziński Marek (red.), *Nowe media i polityka. Internet, demokracja, kampanie wyborcze*, Toruń 2008.
Jeziński Marek (red.), *Nowe media w systemie komunikowania: polityka,* Toruń 2011.
Juza Marta, *Między wolnością a nadzorem. Internet w zmieniającym się społeczeństwie*, Warszawa 2019.
Kacała Tomasz, *Działania psychologiczne wybranych państw*, Toruń 2016.
Kai-Fu Lee, *Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata*, Poznań 2018.
Kaiser Brittany, *Dyktatura danych, Kulisy działania Cambridge Analytica. Jak big data, Trump i Facebook zniszczyły demokrację i dlaczego może się to powtórzyć*, Warszawa 2020.
Kalinowska-Żeleźnik Anna, Kuczamer-Kłopotowska Sylwia, Lusińska Anna, *Znaczenie mediów społecznościowych w życiu codziennym młodszych millenialsów*, w: Jan Kreft (red.), *Facebook. Oblicza i dylematy*, Kraków 2017.
Kaplan Jerry, *Sztuczna inteligencja. Co każdy powinien wiedzieć*, Warszawa 2019.
Karpiński Andrzej, *Co trzeba wiedzieć o studiach nad przyszłością?*, Warszawa 2009.

Kelly Kevin, *Nieuniknione. Jak inteligentne technologie zmienią naszą przyszłość*, Warszawa 2017.
Kitler Waldemar, Taczkowska-Olszewska Joanna (red.), *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne*, Warszawa 2017.
Kloch Józef (red.), *Internet i Kościół*, Warszawa 2011.
Kosiński Jerzy, *Paradygmaty cyberprzestępczości*, Warszawa 2015.
Kotowicz Dominika, *Internet – szanse i zagrożenia dla demokracji*, w: Dominik Batorski, Mirosława Marody, Andrzej Nowak (red.), *Społeczna przestrzeń Internetu*, Warszawa 2006.
Kowalczyk Marcin, *Cyfrowe Państwo. Uwarunkowania i perspektywy*, Warszawa 2019.
Kowalewski Jakub, Kowalewski Marian, *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*, Warszawa 2017.
Kożdoń-Dębecka Monika, *Internet w prezydenckich kampaniach wyborczych w USA w latach 2000–2012,* Warszawa 2019.
Krasuski Andrzej, *Status prawny sztucznego agenta. Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2021.
Krawiec Jerzy, *Internet rzeczy (IoT). Problemy cyberbezpieczeństwa*, Warszawa 2020.
Kreft Jan (red.), *Facebook. Oblicza i dylematy*, Kraków 2017.
Kreft Jan, *Władza algorytmów. U źródeł potęgi Google i Facebooka*, Kraków 2019.
Krztoń Waldemar, *Walka o informację w cyberprzestrzeni w XXI wieku*, Warszawa 2017.
Krzysztofek Kazimierz, *Społeczeństwo w dobie internetu: refleksyjne czy algorytmiczne?*, w: Łukasz Jonak (red.) i in., *Re: internet – społeczne aspekty medium. Polskie konteksty i interpretacje*, Warszawa 2006.
Kubiak Mariusz, Topolewski Stanisław (red.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce 2016.
Kuczyńska-Zonik Aleksandra, *Strategia bezpieczeństwa informacyjnego Federacji Rosyjskiej*, w: Justyna Trubalska, Łukasz Wojciechowski (red.), *Bezpieczeństwo państwa w cyberprzestrzeni*, Lublin 2017.
Kurz Constanze, Rieger Frank, *Pożeracz danych. O zawłaszczaniu naszych danych i o tym jak odzyskać nad nimi kontrolę*, Warszawa 2013.
Lakomy Mirosław, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.
Lakomy Mirosław, *Demokracja 2.0. Interakcja polityczna w nowych mediach*, Kraków 2013.
Lakomy Mirosław, Oświecimski Konrad (red.), *Zarządzanie i nowe technologie ICT w sferze publicznej*, Kraków 2017.
Lakomy Mirosław, Porębski Leszek, Natalia Szybut, *Polityka 2.0. Aktorzy polityczni w świecie nowych technologii. Dyskurs politologiczny*, Kraków 2014.
Lebiedź Jacek, Krztoń Waldemar, Stefaniuk Barbara, *Współczesne wyzwania bezpieczeństwa narodowego. Zarządzanie kryzysowe, wojna informacyjna w cyberprzestrzeni, rzeczywistość wirtualna*, Warszawa 2018.
Levinson Paul, *Miękkie ostrze, czyli historia i przyszłość rewolucji informacyjnej*, Warszawa 2006.
Lorenzi Jean-Hervé, Berrebi Mickaël, *Przyszłość naszej wolności. Czy należy rozmontować Google'a... i kilku innych?*, Warszawa 2019.

Lucas Edward, *Oswoić cyberświat. Tożsamość, zaufanie i bezpieczeństwo w internecie*, Warszawa 2017.

McNamee Roger, *Nabici w Facebooka. Przestroga przed katastrofą*, Poznań 2020.

Madej Marek, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007.

Madej Marek, Terlikowski Marcin (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.

Maj Przemysław, *Internet i demokracja. Ewolucja systemu politycznego*, Rzeszów 2009.

Majorek Marta, Olszyk Sabina, Winiarska-Brodowska Małgorzata, *Cyberpolityka. Internet jako przestrzeń aktywności politycznej*, Warszawa 2018.

Marczewska-Rytko Maria (red.), *Demokracja elektroniczna. Kontrowersje i dylematy*, Lublin 2013.

Marczyk Maciej, Janczewski Robert, Terebiński Bartłomiej (red.), *Militarne aspekty cyberbezpieczeństwa państwa w czasie działań hybrydowych przeciwko RP*, Warszawa 2020.

Mazurek Kamil, *Facebook: od portalu społecznościowego do narzędzia polityki*, Lublin 2018.

Maziarz Wiesław M., *Społeczny wymiar społeczeństwa informacyjnego*, Szczecin 2020.

Mider Daniel, *Partycypacja polityczna w Internecie. Studium politologiczne*, Warszawa 2008.

Milczarek Ewa, *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w internecie*, Warszawa 2020.

Mileszyk Natalia, Paszcza Bartosz, Tarkowski Alek, *AlgoPolska. Zautomatyzowane podejmowanie decyzji w służbie społeczeństwu*, Kraków 2019.

Miller Michael, *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016.

Musiał-Karg Magdalena (red.), *Demokracja w obliczu nowych mediów. Elektroniczna demokracja, wybory przez Internet, kampania w sieci*, Toruń 2013.

Musiał-Karg Magdalena, *Elektroniczne głosowanie. Wybrane dylematy dotyczące e-votingu*, w: Maria Marczewska-Rytko (red.), *Demokracja elektroniczna. Kontrowersje i dylematy*, Lublin 2013.

Musiał-Karg Magdalena, *Elektroniczne referendum w Szwajcarii. Wybrane kierunki zmian helweckiej demokracji bezpośredniej*, Poznań 2012.

Musiał-Karg Magdalena, *E-voting jako nowa forma uczestnictwa obywateli w procesach wyborczych. Doświadczenia wybranych państw europejskich*, w: Andrzej Stelmach (red.), *Prawo wyborcze i wybory. Doświadczenia dwudziestu lat procesów demokratyzacyjnych w Polsce*, Poznań 2010.

Musiał-Karg Magdalena, *Referendum w państwach europejskich*, Toruń 2008.

Nowak Jacek J., *Wprowadzenie do matematycznego formułowania problemów decyzyjnych*, Warszawa 1999.

Nowak Jakub, *Aktywność obywateli online. Teorie a praktyka*, Lublin 2011.

Nowina-Konopka Maria, *Rola internetu w rozwoju demokracji w Polsce*, Kraków 2008.

Nowina-Konopka Maria, *Społeczeństwo informacyjne a teorie demokracji*, w: Marta Witkowska, Kamila Cholawo-Sosnowska (red.), *Społeczeństwo informacyjne. Istota – rozwój – wyzwania*, Warszawa 2006.

Oleksiewicz Izabela, *Transformacja polityki cyberbezpieczeństwa RP w XXI wieku*, Warszawa 2020.

Oleksiewicz Izabela, *Zarys polityki cyberbezpieczeństwa Unii Europejskiej. Casus Polski i RFN*, Warszawa 2019.
Olsztyński Andrzej, Sroczyński Tomasz, Frąk Michał, Kozielski Robert, *Internet ludzi. Organizacja jutra*, Warszawa 2018.
O'Neil Cathy, *Broń matematycznej zagłady. Jak algorytmy zwiększają nierówności i zagrażają demokracji*, Warszawa 2017.
Ormsby Eileen, *Darknet*, Kraków 2019.
Osipow Jurij M., Nowak Alojzy Z. (red.), *Rewolucja cyfrowa. Wyzwania, problemy, perspektywy rozwoju*, Warszawa 2019.
Oświecimski Konrad, Lakomy Mirosław, *E-kampanie prezydenckie w USA i w Polsce*, Kraków 2017.
Oświecimski Konrad, Pohl Aleksandra, Lakomy Mirosław (red.), *NetoDEMOkracja: Web 2.0 w sferze publicznej*, Kraków 2016.
Podrecki Paweł (red.), *Prawo Internetu*, Warszawa 2007.
Polański Grzegorz, *Cechy pokolenia sieci w perspektywie pokolenia Y. Raport z badań*, w: Janusz Morbitzer, Emil Musiał (red.), *Człowiek – media – edukacja*, Kraków 2014.
Porębski Leszek, *Elektroniczne oblicze polityki. Demokracja, państwo, instytucje polityczne w okresie rewolucji informacyjnej*, Kraków 2001.
Porębski Leszek, *Lokalny wymiar elektronicznej demokracji*, Kraków 2012.
Poulet Bernard, *Śmierć gazet i przyszłość informacji*, Wołowiec 2011.
Przegalińska Aleksandra, Oskanowicz Paweł, *Sztuczna Inteligencja. Nieludzka, arcyludzka*, Kraków 2020.
Pudełko Marek, *Prawdziwa historia internetu na świecie*, Piekary Śląskie 2020.
Rajczyk Robert, *Nowoczesne wojny informacyjne*, Warszawa 2016.
Rid Thomas, *Active Measures: The Secret History of Disinformation and Political Warfare*, New York 2020.
Rogala-Lewicki Adam, *Informacja jako autonomiczny czynnik wpływu w przestrzeni publicznej. Studium władztwa informacyjnego*, Częstochowa 2015.
Roguski Artur, *Zrozumieć social media*, Gliwice 2020.
Rothert Agnieszka, *Cybernetyczny porządek polityczny*, Warszawa 2005.
Rothert Agnieszka, *Demo-net. Wirtualna projekcja rzeczywistości*, Warszawa 2001.
Rothert Agnieszka, *Technopolis: wirtualne sieci polityczne*, Warszawa 2003.
Rydlewski Grzegorz, *Coś więcej niż spór o model rządzenia. Kilka kwestii do przemyślenia nie tylko przez politologów*, Warszawa 2017.
Rydlewski Grzegorz, *Polska polityczna 2012/2013. Sfera publiczna jako środowisko decydowania politycznego*, Warszawa 2014.
Rydlewski Grzegorz, *Rządy i rządzenie w Polsce 1918–2018. Ciągłość i zmiany*, Warszawa 2018.
Rydlewski Grzegorz, *Rządzenie w świecie megazmian. Studium politologiczne*, Warszawa 2009.
Rzucidło Jakub, *Referendum w obliczu głosowania za pośrednictwem Internetu – doświadczenia Estonii, Norwegii i Szwajcarii*, w: Olga Hałub, Mariusz Jabłoński, Mateusz Radajewski (red.), *Instytucje demokracji bezpośredniej w praktyce*, Wrocław 2016.
Scott John, *Władza*, Warszawa 2006.
Sears David O., Jervis Robert, Huddy Leonie (red.), *Psychologia polityczna*, Kraków 2014.

Semetko Holli A., *Komunikacja polityczna*, w: Russell J. Dalton, Hans-Dieter Klingemann, *Zachowania polityczne*, tom 1, Warszawa 2010.
Sikorski Marcin, Roman Adam (red.), *Internet rzeczy*, Warszawa 2020.
Skibińska Małgorzata, Siemieniecka Dorota, Majewska Kamila, *Cyberagresja. Zjawisko, skutki, zapobieganie*, Toruń 2020.
Singer Peter W., Brooking Emerson T., *Nowy rodzaj wojny. Media społecznościowe jako broń*, Kraków 2019.
Sitek Magdalena, Zientarski Piotr B. (red.), *Wybrane aspekty informatyzacji w samorządach a zasada dobrej administracji*, Warszawa 2019.
Siwicki Maciej, *Cyberprzestępczość,* Warszawa 2013.
Skarżyńska Krystyna, *Człowiek a polityka. Zarys psychologii politycznej*, Warszawa 2005.
Sloterdijk Peter, *Czas i gniew*, Warszawa 2011.
Staniszkis Jadwiga, *O władzy i bezsilności*, Kraków 2006.
Staniszkis Jadwiga, *Zawładnąć! Zarys procesualnej teorii władzy*, Warszawa 2012.
Stawnicka Jadwiga, Morańska Danuta, Kubies Wacław (red.), *Świat nowych technologii. Czy sztuczna inteligencja zdominuje życie człowieka?*, Sosnowiec 2020.
Stoppel Anna, *Nowe media w polityce na przykładzie kampanii prezydenckich w Polsce w latach 1995–2015*, Poznań 2019.
Strittmatter Kai, *Chiny 5.0. Jak powstaje cyfrowa dyktatura*, Warszawa 2020.
Sułek Mirosław, *Prognozowanie i symulacja międzynarodowa*, Warszawa 2010.
Surma Jerzy (red.), *Hakowanie sztucznej inteligencji*, Warszawa 2020.
Szeliga Marcin, *Data Science i uczenie maszynowe*, Warszawa 2017.
Szpor Grażyna (red.), *Internet. Cloud Computing. Przetwarzanie w chmurach*, Warszawa 2013.
Szpor Grażyna (red.), *Internet rzeczy. Bezpieczeństwo w Smart city*, Warszawa 2015.
Szpor Grażyna, Czaplicki Kamil (red.), *Internet. Analityka danych. Data Analytics*, Warszawa 2019.
Szpor Grażyna, Gryszczyńska Agnieszka (red.), *Internet. Strategie bezpieczeństwa*, Warszawa 2017.
Sztompka Piotr, *Kapitał społeczny. Teoria przestrzeni międzyludzkiej*, Kraków 2016.
Szuniewicz Marta, *Ochrona bezpieczeństwa państwa jako przesłanka ograniczenia praw i wolności jednostki w świetle Europejskiej Konwencji Praw Człowieka*, Warszawa 2016.
Świeboda Halina (red.), *Prognozowanie w naukach społecznych. Wymiar narodowy i międzynarodowy*, Warszawa 2018.
Świerczyński Marek, Lai Luigi (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.
Tapscott Don, *Cyfrowa dorosłość. Jak pokolenie sieci zmienia świat*, Warszawa 2007.
Tegmark Max, *Życie 3.0. Człowiek w erze sztucznej inteligencji*, Warszawa 2019.
Thompson John B., *Skandal polityczny. Władza i jawność w epoce medialnej*, Warszawa 2010.
Tocqueville Alexis de, *O demokracji w Ameryce*, Warszawa 1976.
Toffler Alvin, *Trzecia fala*, Poznań 2006.
Trejderowski Tomasz, *Kradzież tożsamości. Terroryzm informatyczny*, Warszawa 2013.
Vaidhyanathan Siva, *Antisocial Media. Jak Facebook oddala nas od siebie i zagraża demokracji*, Warszawa 2018.
Walewski Łukasz, *Władza w sieci. Jak nami rządzą social media*, Kraków 2020.

Wallace Patricia, *Psychologia Internetu*, Poznań 2003.
Wiak Krzysztof, Podraza Andrzej, Potakowski Paweł (red.), *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa 2013.
Witkowska Marta, Cholawo-Sosnowska Kamila (red.), *Społeczeństwo informacyjne. Istota – rozwój – wyzwania*, Warszawa 2006.
Wnuk-Lipiński Edmund, *Świat międzyepoki*, Kraków 2004.
Wodecki Andrzej, *Sztuczna inteligencja w kreowaniu wartości organizacji. Analiza generowania wartości przez firmy wykorzystujące sztuczną inteligencję w prowadzeniu biznesu*, Kraków 2018.
Woolley Samuel, *The Reality Game: How the Next Wave of Technology Will Break the Truth*, New York 2020.
Wrzosek Marek, Markiewicz Szymon, Modrzejewski Zbigniew (red.), *Informacyjny wymiar wojny hybrydowej*, Warszawa 2019.
Wylie Christopher, *Mindf*ck. Cambridge Analytica, czyli jak popsuć demokrację*, Kraków 2020.
Xi Jinping, *Innowacyjne Chiny*, Warszawa 2015.
Zajdowski Karol, *Marketing produktu politycznego. Analiza porównawcza*, Warszawa 2017.
Zalewski Sławomir, *Bezpieczeństwo polityczne państwa. Studium funkcjonalności instytucji*, Siedlce 2010.
Zalewski Tomasz, *Definicja sztucznej inteligencji*, w: Marek Świerczyński, Luigi Lai (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.
Zbieranek Jarosław, *Alternatywne procedury głosowania w polskim prawie wyborczym – gwarancja zasady powszechności wyborów czy mechanizm zwiększania frekwencji wyborczej?*, Warszawa 2013.
Zuboff Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York 2019.
Zwierżdżyński Marcin K., Lakomy Mirosław, Oświecimski Konrad (red.), *E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni*, Kraków 2016.
Zwierżdżyński Marcin K., Lakomy Mirosław, Oświecimski Konrad, *Technopolityka w świecie nowych mediów*, Kraków 2015.
Zych Jan, *Teleinformatyka dla bezpieczeństwa 2.0*, Poznań 2019.
Żurawski Jakub, *Internet jako współczesny środek elektronicznej komunikacji wyborczej i jego zastosowanie w polskich kampaniach parlamentarnych*, Kraków 2010.

Wybrane artykuły, opracowania, akty normatywne, dokumenty, materiały prasowe oraz netografia

Allison Graham, Schmidt Eric, *Is China Beating the U.S. to AI Supremacy?*, https://www.belfercenter.org/publication/china-beating-us-ai-supremacy.
Avent Ryan, *The Wealth of Humans: Work, Power, and Status in the Twenty-first Century*, New York 2016.
Balcewicz Justyna, Babraj Rafał, *Analiza. Akt o cyberbezpieczeństwie – nowy mandat ENISA i certyfikacja cyberbezpieczeństwa*, maj 2019, www.cyberpolicy.nask.pl.
Batorski Dominik, *Wykluczenie cyfrowe w Polsce*, Biuro Analiz Sejmowych, „Studia BAS" 2009, nr 3 (19), pt. *Społeczeństwo informacyjne*, pod redakcją Doroty Grodzkiej.

Benaich Nathan, Hogarth Ian, *State of AI Report 2020*, https://docs.google.com/presentation/d/1ZUimafgXCBSLsgbacd6-a-dqO7yLyzIl1ZJbiCBUUT4/edit#slide=id.g557254d430_0_0.

Bodio Tadeusz, Chodubski Andrzej, *O prognostyce w politologii*, „Studia Politologiczne" 2004, t. 8.

Borkowski Piotr, *Koncepcja cyberbezpieczeństwa w ujęciu Chińskiej Republiki Ludowej – wybrane aspekty*, Agencja Bezpieczeństwa Wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13 (7).

Brent Laura, *Rola NATO w cyberprzestrzeni*, https://www.nato.int/docu/review/pl/articles/2019/02/12/rola-nato-w-cyberprzestrzeni/index.html.

Chodubski Andrzej, *Prognostyka jako wyzwanie metodologiczne w badaniu stosunków międzynarodowych*, Annales Universitatis Mariae Curie-Skłodowska, Lublin 2009, sectio K, vol. XVI, 2.

Code of good practice in electoral matters. Guidelines and explanatory report, Venice Commission, opinion no 190/2002, https://rm.coe.int/090000168092af01.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions: A European strategy for data, Brussels, 19.2.2020, COM(2020) 66 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future, Brussels, 19.2.2020, COM(2020) 67 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:67:FIN.

Cyfryzacja podczas pandemii – innowacje, bezpieczeństwo, e-administracja. Wybrane działania Ministerstwa Cyfryzacji, raport, marzec–wrzesień 2020, https://www.gov.pl/web/cyfryzacja/cyfryzacja-podczas-pandemii.

Darczewska Jolanta, *Rosyjskie siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*, Ośrodek Studiów Wschodnich, Warszawa 2016, Prace OSW nr 57.

Dekret Prezydenta FR z dnia 22 maja 2015 r. *O niektórych problemach bezpieczeństwa informacyjnego FR* oraz *Doktryna bezpieczeństwa informacyjnego* z dnia 5 grudnia 2016 r., w: Marek Berliński, Robert Zulczyk, *Federalna Służba Bezpieczeństwa Federacji Rosyjskiej*, Warszawa 2016.

Digital economy report 2019. Value creation and capture: Implications for developing countries, UNCTAD ONZ, Geneva 2019, https://unctad.org/webflyer/digital-economy-report-2019.

Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej (zatwierdzona przez Prezydenta Federacji Rosyjskiej dekretem nr Pr-1895 z dnia 9 września 2000 r.), w: Marek Berliński, Robert Zulczyk, *Federalna Służba Bezpieczeństwa Federacji Rosyjskiej*, Warszawa 2016.

Doktryna bezpieczeństwa informacyjnego RP. Projekt, Warszawa 2015, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf.

Domańska Maria, *Zakneblować Runet, uciszyć społeczeństwo. Kremlowskie ambicje „suwerenizacji" Internetu*, Ośrodek Studiów Wschodnich, „Komentarze OSW" nr 313, z 4 grudnia 2019 r., www.osw.waw.pl.

Freedom on the Net 2019. The Crisis of Social Media, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.

Gorgosz Adrian, *Perspektywa prognostyczna w polityce publicznej. Metody umożliwiające prognozowanie – ich rola w procesie formułowania polityk publicznych*, „Zarządzanie Publiczne" 2014, nr 1 (25).

Górnisiewicz-Kaczor Ewa, *Zasady odpowiedzialności administratora portalu internetowego za bezprawne treści zamieszczane przez użytkowników*, http://www.codozasady.pl/zasady-odpowiedzialnosci-administratora-portalu-internetowego-za-bezprawne-tresci-zamieszczane-przez-uzytkownikow.

Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI). Sprawozdanie krajowe na 2019 r. Polska, http://eregion.wzp.pl/sites/default/files/desi2019langpoland.pdf.

Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI). Sprawozdanie krajowe na 2020 r. Polska, https://www.cloudforum.pl/wp-content/uploads/2020/06/DESI2020-POLAND-lang.pdf.

Internetowy Frankenstein. Prof. Michał Kosiński o tym, jak nowoczesne metody marketingowe pozwalają wpływać na polityczne decyzje każdego człowieka, rozmowa Jacka Żakowskiego z Michałem Kosińskim, https:www.polityka.pl/tygodnik polityka/społeczeństwo/1690344,4.

Introducing Electronic Voting: Essential Considerations, IDEA, Stockholm 2011.

Januszewska Paulina, *15 sekund do sławy*, „Newsweek" 2019, nr 5, wydanie specjalne pt. *Technoczłowiek. Przewodnik po cyberświecie*.

Jeangène Vilmer Jean-Baptiste, Escorcia Alexandre, Guillaume Marine, Herrera Janaina, *Information Manipulation. A Challenge for Our Democracies*, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

Kaczmarski Marcin, *Chiny przyjmują nowe prawo o bezpieczeństwie narodowym*, Analizy Ośrodka Studiów Wschodnich, 15.07.2015.

Kucharski Kamil, *Narzędzia anonimizujące działania w Internecie jako instrumentarium do prowadzenia operacji informacyjnych w ramach wojny hybrydowej*, Agencja Bezpieczeństwa Wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego", wydanie specjalne, październik 2015.

Legucka Agnieszka, *Walka z rosyjską dezinformacją w Unii Europejskiej*, Polski Instytut Spraw Międzynarodowych, „Biuletyn PISM" 2019, nr 111.

Liedel Krzysztof, Piasecka Paulina, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 17.

Mickiewicz Piotr, *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, nr 1.

Mider Daniel, *Głosowanie przez Internet a demokracja*, „Studia Politologiczne" 2011, t. 20.

Mider Daniel, Garlicki Jan, Mincewicz Wojciech, *Pozyskiwanie informacji z Internetu metodą Google Hacking – biały, szary czy czarny wywiad?*, Agencja Bezpieczeństwa Wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 20.

Musiał-Karg Magdalena, *Głosowanie elektroniczne jako alternatywna metoda uczestnictwa w wyborach – opinie Polaków*, „Political Preferences" 2015, nr 10.

Musiał-Karg Magdalena, *Internetowe głosowanie w E-stonii na przykładzie wyborów w latach 2005–2009*, „Przegląd Politologiczny" 2011, nr 3.

Narodowy Plan Szerokopasmowy, Ministerstwo Administracji i Cyfryzacji, Warszawa, styczeń 2014 r. (aktualizowana wersja dokumentu przyjęta przez Radę Ministrów w dniu 8 stycznia 2014 r.), https://www.gov.pl/web/cyfryzacja/narodowy-plan-szerokopasmowy---zaktualizowany.

Olszowski Rafał, *Elektroniczna Republika: udział obywateli w życiu publicznym za pośrednictwem narzędzi ICT*, Fundacja Instytut Aurea Libertas, 2018, https://aurealibertas.org/elektroniczna-republika.

Open Data Barometer – Leaders Edition, World Wide Web Foundation, Washington 2018, https://opendatabarometer.org/?_year=2017&indicator=ODB.

Operation "Secondary Infektion". A Suspected Russian Intelligence Operation Targeting Europe and the United States, https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf.

Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019–2027. Godna zaufania sztuczna inteligencja, autonomia i konkurencja, +PL, projekt dla konsultacji społecznych, Ministerstwo Cyfryzacji, Warszawa, 20 sierpień 2019.

Polska droga do strategii AI, www.gov.pl/web/cyfryzacja/ai.

Pudzianowski Jarosław, *System Wczesnego Ostrzegania o Zagrożeniach w sieci internet*, Rządowe Centrum Bezpieczeństwa, „Biuletyn Kwartalny" 2019, nr 28.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku, CSIRT GOV, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html.

Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, https://rm.coe.int/0900001680726f6f.

Recommendation No. R(97)20 of the Committee of Ministers to member states on "hate speech", https://www.coe.int/en/web/freedom-expression/comm Committee-of-ministers-a.

Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendation.

Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, Brussels, 19.2.2020, COM(2020) 64 final, https://op.europa.eu/en/publication-detail/-/publication/4ce205b8-53d2-11ea-aece-01aa75ed71a1/language-en.

Rezolucja Parlamentu Europejskiego z dnia 12 września 2018 r. w sprawie autonomicznych systemów broni (2018/2752), Dz.U.UE.C.2019.433.86.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. L 151 z 7.06.2019.

Rulka Marcin, *E-voting a zasady prawa wyborczego*, „Przegląd Sejmowy" 2017, nr 3.

Rulka Marcin, *Orzecznictwo dotyczące konstytucyjności regulacji umożliwiających głosowanie elektroniczne (Niemcy, Austria, Estonia, Indie)*, „Przegląd Sejmowy" 2015, nr 6.

Sacewicz Kamila, *Niemiecka strategia ochrony cyberprzestrzeni*, Agencja Bezpieczeństwa Wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7.

Sajduk Błażej, *Czy w nauce o stosunkach międzynarodowych możliwe jest efektywne prognozowanie?*, https://www.omp.org.pl/artykul.php?artykul=274.

Stanowisko Fundacji Panoptykon i Fundacji Centrum Cyfrowe w sprawie koncepcji stworzenia Kodeksu usług cyfrowych (Digital Services Act), https://panoptykon.org/sites/default/files/stanowiska/digital_services_act_stanowisko_panoptykon_i_centrum_cyfrowe_19_09_2019.pdf.

Statystyka użytkowania internetu. Światowi użytkownicy internetu i statystyki dotyczące populacji w 2020 r., https://www.internetworldstats.com/stats.htm.

Strategia Bezpieczeństwa Narodowego RP, przyjęta przez Radę Ministrów, zatwierdzona przez Prezydenta RP w dniu 13 listopada 2007 r., http://192.168.0.116/dokumenty/SBN_RP.pdf.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020, załącznik do postanowienia Prezydenta Rzeczypospolitej Polskiej z dnia 12 maja 2020 r. w sprawie zatwierdzenia „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej", M.P. z 2020 r., poz. 413.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej zatwierdzona przez Prezydenta Rzeczypospolitej Polskiej 5 listopada 2014 r. na wniosek Prezesa Rady Ministrów, Warszawa 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 przyjęta przez Radę Ministrów w uchwale nr 125 z 29 października 2019 r., M.P. z 2019 r., poz. 1037.

Szostak Piotr, *Stary kontynent w erze cyfrowej. Czy Polska odzyska technologiczną suwerenność?*, wyborcza.pl/naszaeuropa z 27.04.2019.

Szymielewicz Katarzyna, Iwańska Karolina, *Cyfrowa propaganda czy „normalna" polityczna polaryzacja? Studium debaty politycznej na polskim Twitterze (wrzesień–październik 2017)*, Raport Fundacji Panoptykon, Warszawa 2018.

Tarkowski Alek i in., *Analiza strategii i działań mających na celu rozwój kompetencji cyfrowych w państwach Unii Europejskiej*, https://cppc.gov.pl/images/Analiza_strategii_i_dzia%C5%82an_majacych_na_celu_rozwoj_kompetencji_cyfrowych_w_panstwach_Unii_Europejskiej.pdf.

The AIM Initiative: A Strategy for Augmenting Intelligence using Machines, https://www.dni.gov/index.php/newsroom/reports-publications/item/1940-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines.

The Great Hack, reż. Karim Amer, Jehane Noujaim, prod. USA 2019, Netflix.

Uchwała nr 157 Rady Ministrów z dnia 25 września 2012 r. w sprawie przyjęcia Strategii Rozwoju Kraju 2020. Aktywne społeczeństwo, konkurencyjna gospodarka, sprawne państwo, M.P. poz. 882.

Uchwała nr 16 Rady Ministrów z dnia 5 lutego 2013 r. w sprawie Długookresowej Strategii Rozwoju Kraju. Polska 2030. Trzecia Fala Nowoczesności, M.P. poz. 121.

Uchwała nr 17 Rady Ministrów z dnia 12 lutego 2013 r. w sprawie przyjęcia strategii „Sprawne Państwo 2020", M.P. poz. 136.

Uchwała nr 67 Rady Ministrów z dnia 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022", M.P. z 2013 r. poz. 377.

Uchwała nr 8 Rady Ministrów z dnia 14 lutego 2017 r. w sprawie przyjęcia Strategii na Rzecz Odpowiedzialnego Rozwoju Kraju do roku 2020 (z perspektywą do 2030 roku), M.P. poz. 260.

Uchwała nr 52 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa.Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, tekst jedn. Dz.U. z 2019 r., poz. 1781.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560 (tekst jedn. Dz.U. z 2020 r., poz. 1369).

White Paper. On Artificial Intelligence a European approach to excellence and trust, Brussels, 19.2.2020, COM(2020) 65 final, https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

Założenia do strategii AI w Polsce. Plan działań Ministerstwa Cyfryzacji, Warszawa 2018, mc.gov.pl.

Zbieranek Jarosław, *Głosowanie przez internet (i-voting) w wybranych państwach*, Biuro Analiz Sejmowych, „Zeszyty Prawnicze BAS" 2018, nr 1 (57).

Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, red. M. Wrzosek, https://akademia.nask.pl/badania/Raport_CP_Dezinformacja_ONLINE.pdf.

Zobowiązanie w sprawie obrony cybernetycznej przyjęte na szczycie NATO w Warszawie w dniu 8 lipca 2016 r., http://www.nato.int/cps/en/natohq/ official_texts_133177.htm?selectedLocale=en.

Zwalczanie dezinformacji w internecie: podejście europejskie, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów COM(2018) 236 final, https://ec.europa.eu/transparency/regdoc/rep/1/2018/PL/COM-2018-236-F1-PL-MAIN-PART-1.PDF.

Wyniki badań społecznych

Bezpieczne wybory. Badanie opinii o (dez)informacji w sieci, red. Rafał Lange, https://www.nask.pl/pl/raporty/raporty/2592,Bezpieczne-wybory-raport-na-temat-dezinformacji-w-internecie.html?search=8771219.

Korzystanie z internetu, CBOS, komunikat z badań nr 85 z 2020 r. (badanie przeprowadzono w dniach 15–25 czerwca 2020 r. w ramach procedury mixed-mode na reprezentatywnej imiennej, liczącej 1378 osób, próbie pełnoletnich mieszkańców Polski, wylosowanej z rejestru PESEL).

Korzystanie z internetu, CBOS, komunikat z badań nr 95 z 2019 r. (badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 16–23 maja 2019 r. na liczącej 1079 osób reprezentatywnej próbie losowej dorosłych mieszkańców Polski).

Korzystanie z telefonów komórkowych, CBOS, komunikat z badań nr 99 z 2017 r. (badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 29 czerwca – 6 lipca 2017 r. na liczącej 977 osób reprezentatywnej próbie losowej dorosłych mieszkańców Polski).

Mowa nienawiści, CBOS, komunikat z badań nr 139 z 2019 r. (badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 4–11 lipca 2019 r. na liczącej 1077 osób reprezentatywnej próbie losowej dorosłych mieszkańców Polski).

Odbiór kampanii wyborczej i aktywność polityczna w internecie przed wyborami prezydenckimi, CBOS, komunikat z badań nr 108 z 2020 r. (badanie przeprowadzono w dniach 18–27 sierpnia 2020 r. w ramach procedury mixed-mode na reprezentatywnej imiennej próbie pełnoletnich mieszkańców Polski, wylosowanej z rejestru PESEL).

Odbiór kampanii wyborczej i aktywność polityczna w internecie przed wyborami parlamentarnymi, CBOS, komunikat z badań nr 152 z 2019 r. (badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 7–17 listopada 2019 r. na liczącej 944 osoby reprezentatywnej próbie losowej dorosłych mieszkańców Polski).

Odbiór kampanii wyborczej i aktywność polityczna w internecie przed wyborami do Parlamentu Europejskiego, CBOS, komunikat z badań nr 86 z 2019 r. (badanie przeprowadzono metodą wywiadów bezpośrednich wspomaganych komputerowo w dniach 6–13 czerwca 2019 r. na liczącej 1073 osoby reprezentatywnej próbie losowej dorosłych mieszkańców Polski).

Sztuczna Inteligencja w społeczeństwie i gospodarce. Raport z badań społecznych. Analiza wyników ogólnopolskiego badania opinii polskich internautów, red. Rafał Lange, https://www.nask.pl/pl/raporty/raporty/2594,Sztuczna-inteligencja-w-oczach-Polakow-raport-z-badan-spolecznych.html.

Indeks osobowy

Indeks nie obejmuje wykazu literatury

Indeks wybranych zagadnień

(kontekst rządzenia w epoce informacji, cyfryzacji i sztucznej inteligencji)[1]

---

[1] W poszczególnych przypadkach wskazano kwalifikację dominującą.

Summary

At the beginning of the third decade of the 21st century, there can no longer be any doubt that the rising power of information, social communication and electronic technology is bringing about strategic changes in the world. The Internet and digitalisation shape society, ideologies as well as economic and political solutions. A new balance of forces and competition is emerging in the world. We witness the appearance of new dividing lines and conflicts driven primarily by dominance in the area of digital technologies.

Online and offline phenomena and processes mix together and spread to all spheres of life. Public e-reality emerges, with ever more prominent elements such as e-state, e-administration, e-procedures and e-citizens. The web begins to prevail over hierarchy. Due to the blockade of direct contact resulting from the pandemic that enveloped the world in 2020, individuals, states and institutions have moved ever more of their activities online. The constantly refined, ever faster and increasingly integrated mechanisms of electronic communication as well as solutions such as smart homes and smart cities offer people new aids, shortcuts and possibilities.

Transformations in the area of digital technology and artificial intelligence (AI) are accompanied by completely new problems and threats, whose essence and extent have not been fully recognised yet. Technology and politics increasingly intertwine, and their relation often puts values, standards and mechanisms of the democratic world at risk. Information technology tools have already been used to combat hostile political actors and institutional structures. Human-machine relations become ever more numerous and replace or at least fundamentally alter direct human-human relations. Human-made technological products swiftly acquire new skills by using information obtained from online resources. Data collected in cyberspace become a raw material for building tools of artificial intelligence. Today, all the changes in digital space are still in human hands. However, doubt grows whether this will always be the case or whether the increasingly intelligent products of human scientific and technical thought and advanced technologies will not escape the power of their creators.

Three fundamental facts seem to me to be so essential in this context that I believe they justify a publication in book form. Firstly, in terms of thinking about the future, politicians have been considerably outdistanced by engineers, biologists and researchers of other specialities as well as by visionaries and creators of social communication networks operating outside the state structures. For a long time, governments have included the development of electronic machines and algorithms in their agendas and in state budgets – mainly with a view to creating a new type of weapon that could be used in an armed confrontation. Secondly, politicians fail at drawing sufficient conclusions from the fundamental changes in society that give a new shape to the immediate environment of their activities. This situation results in attempts to continue to govern and make political decisions in a mainly anachronistic fashion – one based on a social model that is becoming a thing of the past. In consequence, the dangerous gap between the model of expressing and aggregating political interests and giving legitimacy to and functioning of public authorities and the model of society keeps widening. Thirdly and finally (this is the leitmotif of the present considerations), political sciences need to carry out a more thorough review of strategic scenarios depicting a rational vision of the future of governance and political decision-making. Political sciences cannot look only towards the past and the present. The need to gaze into the future is becoming rather obvious in the situation when a new, technocybernetic world is emerging.

Among the challenges facing political decision-making and governance, which have been proliferating over the last years and which need to be taken into account in any attempt to determine the directions, methods and ways of further action in both these areas of activity, the increasing power of communication and the expansion of new information technologies and digital solutions are essential. When predicting the future shape – or the direction of evolution – of politics, political decision-making and governance, it is worth drawing from not only knowledge and experience, but also intuition. It can namely suggest which of the scenarios under consideration has the best chance of coming true. Yet, given the numerous uncertainties, sometimes we have to limit ourselves to presenting possibilities or variants of scenarios – without predicting which would win. It will definitely not satisfy those who expect unambiguous answers that leave no room for doubt. By deciding to share my predictions about the future of politics and governance, I am taking a certain risk. I treat these predictions as a possible point of reference in the debate about the prospective changes to the surrounding reality.

In the successive parts of the book, I present: the essence and characteristics of governance; the conditions and a strategic forecast of changes in governance at the beginning of the 2020s; the consequences

for governance resulting from the emergence of an information network society; the significance of the emergence and development of the Internet, social media and digital technologies for governance; global competition in the area of new communication and digital technologies; the use of digital tools for the purposes of political game and manipulation; regulatory and security challenges faced by governance related to the expansion of IT and digitalisation; the state of e-government and e-governance in Poland and the strategic dilemmas with regard to the future of governance and politics in the conditions of further expansion of digitalisation.

Based on a detailed analysis, I present ten points containing my assessment, opinions and forecasts as well as recommendations.

I.

The world is growing more digital. This depends on the following factors: the development of online social communication tools that combine mass scale with individualisation, the emergence of network society, the intensity of works on new solutions in the area of smart digital technologies, and the huge financial resources allocated to this field. The qualitative change brought about by digitalisation will impact all areas of human life and the operation of institutional structures, including the area of public authority. It is widely known that governance strongly depends on the events that surround it. This is why digitalisation is a sphere of cooperation, competition and confrontation between states. At the same time, in a situation when instant messengers have become a new tool in politics, it is evident that states take steps to maintain a dominant position in the fields of information and communication on their territories. All the above indicates that digitalisation will swiftly gain significance in strategies, regulations and day-to-day operation of international entities and individual states.

II.

The power of information, communication and technology is growing stronger. The expansion of information, online social communication and digitalisation already strongly affects the model and way of exercising power in the political sphere. At the same time, digitalisation has become an area of implementing policies as well as a task and a tool of politics and governance. Social media reveal difficulties in reconciling the free nature of online communication with privacy and data protection requirements. The owners of social media and the producers and administrators of computer software are gradually becoming independent actors in the political game, mainly on account of their decisions concerning the use of algorithms and the principles of monitoring online activity and blocking user accounts. Yet the commercial character of

those entities renders their politically significant decisions (concerning e.g. political advertising and restrictions on hate speech) dependent on financial objectives, such as profit maximisation. It becomes necessary to subject those entities to external scrutiny.

Research and implementation in the area of artificial intelligence push the limits of technological possibilities. The design of autonomous artificial intelligence is now within those limits. If we want this area to be guided by universal values and common human interests, it has to be subject to constant supervision as well as collectively developed and effectively enforced legal regulations.

III.

The intensity and universality of qualitative change surrounding politics will enforce a systemic revision of governance mechanisms. The current model of gaining and exercising power in the public sphere will face a fundamental challenge: a radical modification of its technical instruments. It should be noted at this point that the emergence of the possibility of using new systemic solutions is not tantamount to their actual use. The possibilities that we are gaining thanks to the digital technological change are but one of the factors influencing transformations within governance mechanisms. Social factors will be crucial in this area: changes in awareness, the pace of development of the digital society and the reduction of fears caused by the digitalisation of politics. Electronic solutions will become a standard first in administration and in decision-making processes in the institutional structures of the state. We can expect essential modifications in the manner of implementing public policies. A great deal of changes are already being made in these areas. This process was accelerated by the 2020 pandemic, which caused a rapid popularisation of electronic procedures in all areas of human life and work.

IV.

In light of the rapid development of machine learning, questions about the future of democracy remain topical. Even though it is technically possible, mechanisms of electronic legitimisation are unlikely to be implemented in politics any time soon. This is particularly true of general elections as any fundamental change in this area would require overcoming the barrier of social awareness (including the fear of vote-rigging), and those in power do not seem ready to take the risk involved. Most probably, the ideas of digital democracy and electronic elections of public authority bodies will come true only in the distant future. The pace and extent of their implementation will be the subject of major controversy. Perhaps only successive partial solutions consisting in the auxiliary use of electronic technology in general

elections will be developed for a long time to come. In the debate about the introduction of electronic voting, the related obstacles and hazards are often highlighted. Thus, perforce, the focus is also on measures aimed at reducing the risk of disinformation on the Internet and threats to the security of IT systems. Accusations of digital disinformation spread online are often a tool of political manipulation. New possibilities offered by information and communication technology tools will continue to be used to create virtual political circles, to shape images and to build support as well as to fight political rivals for a long time to come. There is already a new model of policy making in this area and further professionalisation is to be expected. More centrally, creating solutions for civic democracy networks as a part of information society will strengthen various forms of political participation. Along with the growing readiness in society to join in the current public decision-making by means of electronic mechanisms of direct democracy, the current model of representative democracy will begin to diminish in importance.

V.

Digitalisation has a great positive potential: it is a lever for progress and it helps improve the quality of activities. Yet is has another facet, as well: it carries serious risks and has numerous adverse effects and a destructive influence on certain social phenomena and behaviour patterns. One such increasingly acute problem is people's dependence on electronic devices and processes. New technologies have already permeated the world of politics, where they are sometimes used by those who want to play dirty. Various pathologies related to social communication and digitalisation come to light, including cybercrime, disinformation and manipulation. It is the duty of public authorities to make society aware of the threats related to using digital communication tools and to proof it against disinformation and manipulation on the Internet. The governments need to bear in mind that IT and information security is becoming a permanent and increasingly vital element of state security. Strengthening the power of communication and increasing the power of available digital tools, algorithms and artificial intelligence create the need to subject them to careful observation and analysis. We need to refine the methods of counteracting the adverse effects of using digital tools resulting from bad intentions of their users or from technical failures. The risks posed by digitalisation stem also from their use for military purposes. Armed conflicts can – and in certain cases already do – move into cyberspace. Worse still, the advance of digitalisation entails the risk of lowering the threshold of conflict involving the use of lethal autonomous weapon systems.

We need global cooperation in order to channel and standardise works on new artificial intelligence solutions and devices. Social, economic and political success will increasingly hinge upon cooperation between humans and artificial intelligence. The present situation has been accurately summed up by Garri Kasparov, a famous Russian chess player, who said that we are already playing a game against the machines.

VI.

Digital data resources are becoming a strategic factor in governance. They have already become as important for the functioning of people and the operation of institutional structures as raw materials, energy sources and financial capital. Thus, gaining and maintaining access to them will continue to be the objective of overt and covert measures taken by public authorities and non-governmental actors, including commercial entities. These measures should be expected to entail various dysfunctions: abuse, threat to rights and freedoms as well as conflicts of interests. Global systems of storing, processing and distributing digital data provide less and less room for privacy protection. The fight for privacy will become one of the key issues discussed in connection with digitalisation. Another major political challenge will be to find a balance between the needs of freedom and the needs of security in the use of personal data, especially biometric data. A real threat resulting from the development of new supervision techniques on the one hand and the lack of necessary legal regulations on the other is the continuous surveillance of individuals and entire societies. It corresponds to Bentham's design of the panopticon, in which the modern thought saw an allegory of society and the world as a global prison. The thesis that digitalisation would serve only to support democratic solutions proved to be wrong. Autocracies soon learned how to employ digital tools to supervise social life and strengthen their power.

The data collected in cyberspace, and more precisely: the knowledge contained in them, have – at least potentially – political significance (according to the slogan 'knowledge is power') and at the same time a market value. That is why access to these data is so critical. Unequal access to electronic data, manifesting itself among others in the so-called asymmetry of information, results from a new global power structure and at the same time helps to shape and preserve this structure.

VII.

Digitalisation and artificial intelligence form new power relations in the world and become the subject of political and business competition on a global scale. In the area of digitalisation, we need to take advantage of the experiences gathered when programming, monitoring and modifying as

well as managing processes in businesses. A common practice in the field of business is strategic and operational controlling. It involves regular analysis of changes and emerging threats and deviations from the adopted objectives. As a result, necessary corrections and development stimulants are introduced where appropriate. The objectives themselves, and not only the solutions that implement them become the subject of thorough observation, analysis and – if necessary – modification. In the context of political decision-making and governance, a similar strategic and operational controlling should cover also the phenomena of expansion of information and communication technologies and advances in the area of digitalisation.

VIII.

The development of individualised, electronic mass communication and the expansion of digitalisation and artificial intelligence have a geopolitical significance. They affect the criteria of assessment of sovereignty of individual states and the position of international and interstate structures. It is to be expected that the role of the technological context of sovereignty will grow. The emergence of a new, cybernetic world order brings with it the threat of increasing social and economic inequalities and of political confrontation. Cyberspace becomes an ever more vital area of competition and confrontation between states. Geopolitics is gaining a digital dimension. The ability to use digital data and new methods will be an increasingly significant factor of political power and will translate into a new configuration of economic influences in the world. Participation in the supervision of global networks and electronic communication nods is already crucial. There is a growing awareness that artificial intelligence is the 'industry of the future' that will determine one's position in the world of tomorrow.

States become ever more engaged in the development of smart technologies. In the US, they have the status of a strategic task of paramount importance for the position and security of the state. In China, they constitute an element of a comprehensive national programme. In the European Union, which is trying to make up for its backwardness in this regard, the participation of the member states in works on the development of artificial intelligence has been recognised as a priority task. Competition for primacy in AI projects is increasing. In fact, it has morphed into an open conflict, a technological war between China and the US. As third states are being dragged into the US-Chinese conflict about the fifth generation mobile network (5G network), it becomes evident that there is no room for an isolated clash between the two powers in the area of smart technologies.

Digital exclusion is already becoming a political factor. Development strategies which do not take the use of digital capabilities sufficiently

into consideration cannot meet the needs of sustainable and responsible development and are unable to face security challenges.

IX.

The fundamental role in relations between political decision-making and governance on the one hand and new digital technologies and tools on the other will continue to be played by people and the public structures they create. It depends on the humans – and probably will continue to depend on them in the future – how the growing possibilities offered by digital technologies will be used and how their development will be channelled and monitored. Humans constitute the primary element of the system of governance, and at the same time one that is most susceptible to malfunctions. Human errors and omissions can strengthen the already visible and reveal the new consequences of the 'dark side' of digitalisation. In the long term, they can even lead to the emergence of tensions between humans and their ever more autonomous products of digital technology.

X.

Enhancing the positive impact and reducing the adverse effects of digitalisation and artificial intelligence require global cooperation. Above all, those in power are responsible for carrying out these tasks. Yet, success is contingent on cooperation between politicians, scientists and technologists working on new solutions, financial and business actors as well as leaders of civic organisations and movements. This is a great challenge for international law and for national legal systems. It is crucial for people to be able to develop common norms of conduct that will go beyond particular views on specific matters and divergent interests. We need to build an efficient system of supervision and intervention, equipped with appropriate implementation tools, to guard the adopted standards. This is one of the greatest challenges, but even now, when watching attempts at positive action, one can be a 'conscious optimist,' to use an expression from Max Tegmark's book.

***

When it comes to scenarios for the future – or 'visions of future possibilities and directions of development' (http://infuture.institute/scenariusze-przyszlosci), it is not advisable to focus on concrete details. A fairly responsible way of making a detailed forecast is only possible in the short term. This is particularly true for areas involving dynamic changes, such as governance, social communication, digitalisation, or artificial intelligence. Bearing that in mind, I have focused on problems and tendencies that are strategic in

the light of current knowledge. As I announced in the introduction to the present book, I would like it to be not only an image or a balance sheet of the current changes at the interface of new technologies and governance, but also an invitation to think together about the challenges that the future has in store for us.

Nota o autorze

Prof. dr hab. Grzegorz Rydlewski specjalizuje się w naukach o polityce i administracji oraz naukach o bezpieczeństwie. Jest absolwentem i pracownikiem Uniwersytetu Warszawskiego, twórcą i wieloletnim kierownikiem Zakładu Nauk o Państwie i Administracji Publicznej, a obecnie profesorem w Katedrze Nauk o Państwie i Administracji Publicznej na Wydziale Nauk Politycznych i Studiów Międzynarodowych UW. Jest badaczem systemów politycznych i administracyjnych, relacji między polityką i administracją, problemów jakości i prakseologii decydowania publicznego w Polsce i innych państwach europejskich, w tym w zakresie strategii bezpieczeństwa narodowego oraz zarządzania kryzysowego. Przez ponad dziesięć lat działał w administracji rządowej, m.in. jako sekretarz Rady Ministrów, szef Kancelarii Prezesa Rady Ministrów oraz szef doradców Prezesa Rady Ministrów. Był promotorem i recenzentem w licznych przewodach doktorskich oraz postępowaniach habilitacyjnych i profesorskich. Występował jako referent na licznych konferencjach krajowych i międzynarodowych. Jest autorem ponad stu publikacji, w tym kilkunastu monografii. Ważniejsze autorskie publikacje monograficzne: *Rządy i rządzenie w Polsce 1918–2018. Ciągłość i zmiany* (2018), *Coś więcej niż spór o model rządzenia. Kilka kwestii do przemyślenia nie tylko przez politologów* (2017), *Megasystem bezpieczeństwa narodowego w Polsce. Ujęcie procesowe i funkcjonalno-decyzyjne* (2017), *Modernizacja administracji. Studium polityk administracyjnych w Polsce* (2016), *Polska polityczna 2012/2013. Sfera publiczna jako środowisko decydowania politycznego* (2014), *Rządzenie w świecie megazmian. Studium politologiczne* (2009), *Systemy administracji publicznej w państwach członkowskich Unii Europejskiej* (2007), *Polityka i administracja w rządach państw członkowskich Unii Europejskiej. Studium politologiczne* (2006), *O skutecznym działaniu w polityce. Dziesięć przykazań nie tylko dla ludzi polityki* (2004), *Rządowy system decyzyjny w Polsce. Studium politologiczne okresu transformacji* (2002), *Służba cywilna w Polsce. Przegląd rozwiązań na tle doświadczeń innych państw i podstawowe akty prawne* (2001), *Rządzenie koalicyjne w Polsce. Bilans doświadczeń lat dziewięćdziesiątych*, Warszawa (2000). Ważniejsze książki redagowane: *Modernizacja Policji* (2013), *Decydowanie publiczne. Polska na tle innych państw członkowskich Unii Europejskiej* (2011).

Przenikanie kultury sieci do przestrzeni publicznej • Wzmocnienie powiązań między technologią i polityką • Wejście w epokę internetowej wojny informacyjnej • Polityka w świecie fake newsów, farm trolli i hakerów • Rozwój cyfryzacji, internetu rzeczy i internetu ciała • Konfrontacja, podziały i nierówności związane z zimną wojną technologiczną • Przyspieszony przez pandemię koronawirusa proces tworzenia cyfrowego państwa • Rosnące uzależnienie państw i ludzi od narzędzi cyfrowych • Nowe napięcia między wolnością a prywatnością i bezpieczeństwem • Cyfrowe zagrożenia bezpieczeństwa • Niedostosowanie starych regulacji prawnych do nowych wyzwań • Nieuchronność zmian w stosunkach społecznych i rynku pracy • Niepewna przyszłość obecnego modelu demokracji • Pytanie o dalsze panowanie człowieka nad produktami technologicznymi

Wydział Nauk Politycznych
i Studiów Międzynarodowych
Uniwersytet Warszawski

ISBN 978-83-8017-369-9
9 788380 173699