Konstytucjonalizm polski

REFLEKSJE Z OKAZJI JUBILEUSZU
70-LECIA URODZIN I 45-LECIA PRACY NAUKOWEJ
PROFESORA ANDRZEJA SZMYTA

Redakcja naukowa
Agnieszka Gajda, Krzysztof Grajewski, Anna Rytel-Warzocha
Piotr Uziębło, Marcin M. Wiszowaty

WYDAWNICTWO
UNIWERSYTETU GDAŃSKIEGO
GDAŃSK 2020

Recenzenci
dr hab. Monika Urbaniak, prof. UM
dr hab. Andrzej Kulig, prof. UJ
dr hab. Adam Krzywoń

Redakcja, skład i łamanie
Violet Design / Wioletta Kowalska

Projekt okładki i stron tytułowych
Andrzej Taranek

Publikacja sfinansowana przez
Prorektora ds. Nauki Uniwersytetu Gdańskiego
Dziekana Wydziału Prawa i Administracji Uniwersytetu Gdańskiego
Katedrę Prawa Konstytucyjnego i Instytucji Politycznych Uniwersytetu Gdańskiego

ISBN 978-83-7865-969-3

Wydawnictwo Uniwersytetu Gdańskiego
ul. Armii Krajowej 119/121, 81-824 Sopot
tel./fax 58 523 11 37, tel. 725 991 206
e-mail: wydawnictwo@ug.edu.pl
www.wyd.ug.edu.pl

Księgarnia internetowa: www.kiw.ug.edu.pl

Spis treści

Michał Bernaczyk

Propaganda obliczeniowa (*computational propaganda*) jako zagrożenie dla ustroju Rzeczypospolitej Polskiej

I. Wprowadzenie – o potrzebie i trudnościach identyfikacji zjawiska

W 2007 r. dostąpiłem wyjątkowego zaszczytu: prof. Andrzej Szmyt podjął się sporządzenia recenzji mojej rozprawy doktorskiej poświęconej dostępowi do informacji o działalności władz publicznych oraz osób pełniących funkcje publiczne. Wyważone i starannie uzasadnione opinie prawne Jubilata dot. wykładni art. 61 Konstytucji RP w praktyce parlamentarnej towarzyszyły mi na studiach doktorskich i w późniejszej pracy naukowej. Do dziś pozytywnie zaskakują na tle innych poglądów polskiej nauki prawa. Te ostatnie okazały się jednak silniejsze i w okresie 2010–2015 weszły w niebezpieczną synergię z orzecznictwem sądów administracyjnych, Trybunału Konstytucyjnego, stopniowo doprowadzając do tzw. neutralizacji aksjologicznej[1] konstytucyjnych klauzul poświęconych jawnemu działaniu władz publicznych. Problem z dostępem do źródłowej informacji nie zaczął się w Polsce wraz z kryzysem konstytucyjnym, lecz to kryzys gwałtownie ujawnił wcześniejsze pokusy dyskrecjonalnego sprawowania władzy[2]. Dziś te kwestie nadal wydają mi się ważne, ale biorąc pod uwagę obecną sytuację w Polsce i na świecie, nazwałbym je rozterkami uprzywilejowanego, odległego i względnie poukładanego świata. Aktualnym problem demokracji nie jest już (a przynajmniej nie wyłącznie) poszukiwanie optymalnego poziomu transparentności państwa, lecz spadek zaufania do rzetelnych źródeł wiedzy i podatność na masową dezinformację. Nowym, niebezpiecznym instrumentem zdobywania władzy i budowania wpływu staje się tzw. propaganda obliczeniowa (ang. *computational propaganda*).

[1] Za to zgrabne, acz ponure w swej wymowie, sformułowanie dziękuję prof. Jerzemu Zajadło – zob. szerzej J. Zajadło, *Sędziowie i niewolnicy. Szkice z filozofii prawa*, Gdańsk 2017, s. 32.

[2] Zjawisko omawiam w monografii: *„Dokument wewnętrzny" jako ograniczenie konstytucyjnego prawa do informacji. Rozstrzyganie kolizji w teorii i praktyce prawa*, Warszawa 2017, s. XXIII–XXVI, 198–199.

Pojęcie zostało zaproponowane przez badaczy Uniwersytetu Oksfordzkiego. Pierwszą próbę konceptualizacji pojęcia łączy się z osobą Philipa N. Howarda, socjologa tego uniwersytetu, który w 2014 r. publicznie przewidywał wykorzystywanie algorytmów przez elity polityczne do manipulacji opinią publiczną. Zjawisko propagandy obliczeniowej nadal zasługuje na miano groźnego fenomenu. Jej elementy wymagają dalszych badań, chociaż napotyka to istotne przeszkody: dotychczasowe ustalenia w Unii Europejskiej oraz pozaunijnych krajach dotkniętych propagandą obliczeniową dowodzą, że podmioty uprawiające taką formę komunikacji pragną zachować w tajemnicy własną tożsamość i zleceniodawców, aczkolwiek są do pewnego stopnia skłonne dzielić się metodyką działania[3]. Tę aurę tajemniczości oceniam jako świadomą postawę podmiotów prowadzących działalność gospodarczą. Pełni ona zasadniczo trzy funkcje: ukrywa działanie nieetyczne (manipulacja opinią publiczną, m.in. przez dezinformację), umożliwia odcięcie się politycznego zleceniodawcy w przypadku wykrycia manipulacji (ang. *plausible deniability*), utrudnia egzekwowanie odpowiedzialności (co do zasady cywilnoprawnej) za łamanie warunków świadczenia usług drogą elektroniczną na platformach mediów społecznościowych. W przypadku propagandy obliczeniowej finansowanej lub organizowanej przez służby wrogich państw obcych dążenie do ukrycia kraju jej pochodzenia jest zrozumiałe.

Propaganda obliczeniowa może (i powinna być) rozważana jako połączenie dwóch nierozerwalnych płaszczyzn: społecznej (w tym politycznej) oraz technicznej. Na płaszczyźnie technicznej i społecznej Samuel C. Woolley oraz Philip N. Howard definiują propagandę obliczeniową jako „połączenie platform mediów społecznościowych, niezależnych pośredników, algorytmów i [technologii – przyp. M.B.] *big data*[4] w celu manipulacji

---

[3] Dowody na stosowanie propagandy obliczeniowej w Polsce i na Ukrainie zebrano metodą wywiadu swobodnego z zastrzeżeniem anonimowości rozmówców; zob. odpowiednio R. Gorwa, *Unpacking the Ecosystem of Social Media Manipulation: A Polish Case Study* (w:) *Computational Propaganda. Political Parties, politicians, and Political Manipulation on Social Media*, red. S.C. Woolley, P.H. Howard, Oxford 2018, s. 89 oraz M. Zhdanova, D. Orlova, *Ukraine: External Threats and Internal Challenges* (w:) *Computational Propaganda. Political Parties, politicians, and Political Manipulation on Social Media*, red. S. C. Woolley, P.N. Howard, Oxford 2018, s. 50.

[4] Pojęcie *big data* odnosi się do zbiorów danych tak ogromnych i złożonych, że wykorzystanie ich potencjału jest trudne za pomocą dostępnych „od ręki" narzędzi do obsługi baz danych lub tradycyjnych aplikacji, które umożliwiają utrwalenie, przechowywanie, przeszukiwanie, dzielenie (ang. *sharing*), przesyłanie, analizę i wizualizację. Posłużenie się sformułowaniem „zbiór danych" jest celowe, ale nie powinno być redukowane do definicji legalnych takich jak „zbiór danych" (np. osobowych) lub „baza danych" z powodu ww. cech ilościowych. Nie chodzi też o traktowanie danych jako synonimu informacji (a już zwłaszcza o zrównanie z prawnym pojęciem np. „informacji (o sprawie) publicznej" lub „informacji sektora publicznego"), ponieważ użycie technologii przetwarzania (*big data*) tych pierwszych (danych) prowadzi do tych ostatnich (informacji). Chodzi przede wszystkim o rozumienie danych jako „najmniejszego poziomu abstrakcji, z którego wyprowadza się określoną wiedzę" – zob. B. Ubaldi, *Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives*, OECD Working Papers on Public Governance, no. 22, OECD Publishing, s. 5. W celu opisania owego najmniejszego poziomu używa się niekiedy pojęcia „dane surowe" (ang. *raw data*), tj. niepoddane żadnej analizie człowieka lub maszyny. Posłużenie się słowem „zbiór" (ang. *data set* lub *dataset*) nawiązuje zaś do właściwości danych, ich uporządkowania, co z kolei uwydatnia możliwości łączenia z innymi danymi. Owa trudność w przetwarzaniu zestawów (zbiorów) danych bywa obrazowana liczbowo przez przykłady danych osiągające w środowisku cyfrowym wielkość rzędu terabajtów (1 TB, $10^{12} = 1000^4$ bajtów), petabajtów (1 PB, $10^{15} = 1000^5$ bajtów), a nawet zetabajtów (1 ZB, $10^{21} = 1000^7$ bajtów). Są to dane trudne do wyobrażenia dla przeciętnego użytkownika internetu lub innych sieci teleinformatycznych, który z jednej strony jest nieświadomym odbiorcą

opinią publiczną"[5]. Jej społeczne i techniczne korzenie tkwią w cyfrowym marketingu dóbr i usług, ale zastosowanie jej w szeroko pojętym procesie politycznym spowodowało bardzo krytyczną ocenę badaczy: „Polityczne boty, tj. boty społeczne używane do manipulacji społecznej – dają w ten sposób [tzn. błyskawicznie tworząc wiadomości, wchodząc w interakcję z treściami innymi użytkowników, wpływając lub manipulując algorytmami trendów, uchodząc przy tym za ludzkiego użytkownika – przyp. M.B.] efektywne narzędzie do prowadzenia kampanii propagandy i nienawiści on-line. Jedna osoba lub grupa osób mogą łatwo stworzyć i koordynować armię politycznych botów na Twitterze, YouTube lub Instagramie, dając złudzenie szerokiego konsensusu lub zainteresowania daną kwestią. Władze publiczne i uczestnicy życia politycznego na całym świecie wykorzystywali polityczne boty – zaprogramowane, by ukazywać i zachowywać się jak prawdziwi obywatele – do zagłuszania i nękania opozycji oraz promowania własnego przekazu. Kampanie polityczne (wsparte przez zwolenników[6]) korzystały z politycznych botów i propagandy obliczeniowej podczas wyborów, aby zmienić poparcie, zniesławiać oraz zastraszać opozycję. Anonimowi uczestnicy życia politycznego rozpowszechniali fałszywe wiadomości oraz koordynowali kampanie dezinformacji, tłumy trolli, by atakować obrońców praw człowieka, organizacje społeczeństwa obywatelskiego i dziennikarzy. Propaganda obliczeniowa jest nowym, wyjątkowo potężnym narzędziem przekazywania informacji wykorzystywanym przeciwko demokratycznym podmiotom i instytucjom na całym świecie"[7].

Zasadniczym (lecz nie wyłącznym) instrumentem manipulacji jest dezinformacja (dlatego nazwa zjawiska w języku angielskim posługuje się pojęciem „propaganda", które

---

danych, a z drugiej ich wytwórcą. Tytułem przykładu: producent urządzeń i oprogramowania do samochodowej nawigacji satelitarnej przyznaje, że użytkownik tych urządzeń może, jeżdżąc przez godzinę dziennie w godzinach szczytu, wygenerować około 7 MB danych w ciągu miesiąca. Jeśli odnotujemy, że w samej tylko Warszawie w 2014 r. zarejestrowano 1.262.399 pojazdów (podaję za dokumentem *Krajowe ramy polityki rozwoju infrastruktury paliw alternatywnych*, s. 24, http://bip.me.gov.pl/node/26450; dostęp: 1 grudnia 2018 r.), to nawet skromna część kierowców korzystająca z oprogramowania opartego na geolokalizacji wygeneruje ogromne ilości danych o zastosowaniu nie tylko komercyjnym, ale i politycznym. Uzyskane w ten sposób dane mogą ułatwiać nawigację w ruchu drogowym, prognozowanie ekspozycji podróżnych na reklamę zewnętrzną lub poziomu emisji spalin, ale dadzą też obraz potencjalnej grupy kierowców sfrustrowanych korkami. A to już tworzy potencjalną grupę adresatów komunikatu politycznego, np. w kampanii samorządowej.

[5] S.C. Woolley, P.N. Howard, *Political Communication, Computational Propaganda, and Autonomous Agents*, „International Journal of Communication" 2016, nr 10, s. 4886.

[6] Takim przykładem była szeroko opisywana przez niemiecką prasę („Der Spiegel" i „Sueddeutsche Zeitung") sprawa tzw. rekonkwisty Niemiec, tj. kilkutysięcznej grupy internetowych aktywistów, którzy wzywali do poparcia skrajnie prawicowej partii Alternative für Deutschland (AfD) w wyborach parlamentarnych (przeprowadzonych dnia 24 września 2017 r.). Zwolennicy AfD ogłosili wówczas „wojnę memów", ale nie miała ona wiele wspólnego ze spontanicznym działaniem użytkowników sieci, skoro rozpowszechnianie postów na Twitterze atakujących polityczny establishment i Angelę Merkel koordynowały boty. Boty zarządzały również 31 grupami kryptozwolenników AfD na portalu Facebook. Sama partia polityczna dystansowała się wobec takiej działalności – zob. B. Kollanyi, L.M. Neudert, P.N. Howard, *Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter?*, 19 września 2017 r., s. 2, https://comprop.oii.ox.ac.uk/research/junk-news-and-bots-during-the-german-parliamentary-election-what-are-german-voters-sharing-over-twitter/ (dostęp: 16 października 2019 r.).

[7] S.C. Woolley, P.N. Howard, *Introduction: Computational Propaganda Worldwide* (w:) *Computational Propaganda. Political Parties, politicians, and Political Manipulation on Social Media*, red. S.C. Woolley, P.N. Howard, Oxford 2018, s. 24.

pochłania znaczeniowo dezinformację[8]). Komisja Europejska definiuje dezinformację jako „możliwe do zweryfikowania nieprawdziwe lub wprowadzające w błąd informacje, tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną. Szkoda publiczna obejmuje zagrożenia dla demokratycznych procesów politycznych i kształtowania polityki oraz dla dóbr publicznych, takich jak ochrona zdrowia obywateli UE, środowisko naturalne lub bezpieczeństwo. Dezinformacja nie obejmuje błędów sprawozdawczych, satyry i parodii ani wyraźnie oznaczonych stronniczych wiadomości i komentarzy"[9]. Ta definicja została również wykorzystana w ogólnounijnym kodeksie postępowania w zakresie zwalczania dezinformacji opublikowanym dnia 26 września 2018 r.[10], który usiłuje w pierwszej kolejności nakłonić szeroko pojętą branżę informacyjną do samodzielnego wdrożenia środków technologicznych, finansowych oraz edukacyjnych zwalczających dezinformację.

Należy jednak zwrócić uwagę, że propaganda obliczeniowa może wykorzystywać również prawdziwe informacje (np. rozpowszechniać dyskredytujące informacje ze sfery prywatnej uzyskane kryminalnymi metodami[11]), nieprzypadkowo stając się współczesną inkarnacją tzw. kompromateriałów (od niem. *Kompromittierendes Material*, ros. *компрометирующий материал*)[12], stosowanych przez służby bezpieczeństwa państw bloku sowieckiego.

Można założyć, że manipulacja w sferze polityki nie jest niczym nowym i od zawsze towarzyszyła procedurom wyboru kandydatów na stanowiska publiczne bądź też samemu sprawowaniu władzy. Problem tkwi w tym, że dzisiejsza technika obliczeniowa umożliwia znaczne spotęgowanie efektu manipulacji oraz pozwala ukryć architektów oraz wykonawców takiej działalności. Dnia 26 września 2018 r. Państwowa Komisja Wyborcza

---

[8] W rodzimej literaturze T. Kacała wskazał, że pojęcia „dezinformacja" oraz „propaganda" mogą różnić się od siebie pod względem skali odbiorców, powtarzalności czynności (jednorazowość bądź systematyczność) i oczekiwanych efektów (wprowadzenia w błąd lub uzyskanie wpływu), ale nie da się ukryć, że podane przez autora definicje dowodzą krzyżowania się obu pojęć w aspekcie podmiotowym (celowość, umyślność) i informatywnym (jakość informacji jako element wpływu na adresata komunikatu) – zob. szerzej T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2, s. 51–52. W szczególności należy zwrócić uwagę, że propagandę rozumianą historycznie jako technikę wpływu władz państwowych na całe społeczeństwo za pomocą ówczesnych (acz najnowszych) osiągnięć techniki (tamże, s. 51) można już indywidualizować za pomocą tzw. mikrotargetingu.

[9] Zob. Komisja Europejska: Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Bruksela, 26.04.2018, COM(2018) 236 final, pkt 2.1.

[10] Zob. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454 (dostęp: 26 grudnia 2018 r.).

[11] Istnieje związek pomiędzy dezinformacją a naruszeniem cyberbezpieczeństwa lub innymi podobnymi naruszeniami o charakterze kryminalnym wymierzonym w osoby publiczne lub innych uczestników życia politycznego. Narzędziem działań dezinformacyjnych mogą być prawdziwe i poufne informacje wydobyte od partii politycznych, komitetów wyborczych, kandydatów po uprzednim przełamaniu zabezpieczeń i kradzież informacji, dokumentów, poczty elektronicznej itp. Takie głośne wydarzenia nastąpiły w USA (włamanie na serwery Krajowego Komitetu Partii Demokratycznej w 2015 i 2016 r.) i Francji (tzw. #MacronLeaks w 2017 r. – zob. szerzej J.-B. Jeangène Vilmer, *The „Macron Leaks" Operation: A Post-Mortem*, Washington 2019). W tym tekście nie zajmuję się przełamywaniem zabezpieczeń teleinformatycznych i prawnokarną kwalifikacją tych operacji. Interesuje mnie zjawisko wtórne: skala zorganizowanej proliferacji takich materiałów w celu manipulowania społeczeństwem.

[12] E. Matkowska, *System. Obywatel NRD pod nadzorem tajnych służb*, Kraków 2003, s. 30.

(PKW) oficjalnie odniosła się do problemu manipulowania opiniami polskich wyborców w internecie, lecz jest to stanowisko relatywnie ogólne[13]. Nie powinniśmy jednak czynić z tego zarzutu pod adresem PKW, ponieważ podniosła ona głównie problem luki prawnej. Likwidacja luk – co zresztą wyraźnie podkreślono – należy do władzy ustawodawczej. Zasada legalizmu nakazuje rozpatrywanie sankcji za użycie propagandy obliczeniowej wyłącznie w kategoriach naruszenia normatywnych zasad prawa wyborczego, nie zaś jako kwestii wyłącznie etycznej[14]. Aby zwalczać propagandę obliczeniową za pomocą polskiego prawa wyborczego, należałoby wykazać jej ścisły związek z sankcjonowaną normą odnoszącą się do agitacji wyborczej, czasokresem jej prowadzenia lub jawności finansowania. Tymczasem propaganda obliczeniowa może być z łatwością prowadzona poza granicami czasowymi kampanii lub skutecznie zacierać swój związek z komitetem wyborczym lub kandydatem. Nie zmienia to mojej wstępnej oceny, że użycie propagandy obliczeniowej w przytoczonym uprzednio znaczeniu do celów agitacji lub kryptoagitacji, niezależnie od ustawowej luki rzeczywistej bądź pozornej, nie jest zgodne z treścią konstytucyjnej zasady wolnych i uczciwych wyborów[15].

Zagadnienie propagandy obliczeniowej jest wciąż nieobecne w polskiej nauce prawa konstytucyjnego, ponieważ zniechęca dużym stopniem technicyzacji oraz budzi (skądinąd słuszne) skojarzenie z marketingiem narracyjnym i innymi metodami wpływu na elektorat przypadającymi na okres kampanii wyborczej i dzień wyborów[16]. Prawo konstytucyjne interesuje się tym wątkiem głównie w odniesieniu do sytuacji, gdy informacyjna warstwa agitacji wyborczej była prowadzona lub finansowana niezgodnie z zasadami określonymi w ustawie (zob. odpowiednio: art. 494–504 oraz art. 125–151 k. wyb.[17]) lub odwoływała się do informacji nieprawdziwych (zob. art. 111 § 1–6 k. wyb.). Wstępna ocena przepisów dotyczących kampanii wyborczej (w kształcie nadanym nowelizacją kodeksu wyborczego z 2018 r.[18]) skłania mnie do przyjęcia tezy, że polskie prawo nie chroni wyborców przed

---

[13] Zob. Stanowisko Państwowej Komisji Wyborczej w sprawie zasad prowadzenia i finansowania kampanii wyborczej w internecie z dnia 26 września 2018 r., ZKF-811-50/18, https://pkw.gov.pl/pliki/1537988216_1-50-18.pdf (dostęp: 25 grudnia 2018 r.).

[14] Szczególnie wymowne jest określenie niektórych mechanizmów rozpowszechniania informacji w internecie jako „środków powszechnie uznawanych za nieetyczne, czasem zaś naruszających prawo"; tamże, s. 1.

[15] Zob. G. Kryszeń, *Uczciwość wyborów jako zasada prawa wyborczego*, „Studia Wyborcze" 2016, t. 21, s. 27 z powołaniem na wyrok Trybunału Konstytucyjnego z dnia 21 lipca 2009 r., K 7/09 i standardy międzynarodowe. O prawie do bycia poinformowanym w kampanii wyborczej pisze A. Rakowska-Trela, *Prawa wyborców w kampanii wyborczej*, „Studia Wyborcze" 2015, t. 20, s. 8. Zob. także P. Czarny (w:) *Konstytucja RP. Komentarz*, t. 2, *Art. 87–243*, red. L. Bosek, M. Safjan, Warszawa 2016, komentarz do art. 96 Konstytucji RP, teza nr 18 (dot. uzupełnienia zasad wysłowionych wprost w art. 96 ust. 2 przez zasadę wolnych wyborów), s. 250. Zob. również hasło „podstawowe zasady prawa wyborczego" (w:) B. Michalak, A. Sokala, *Leksykon prawa wyborczego i referendalnego oraz systemów wyborczych*, Warszawa 2010, a także L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2017, s. 175.

[16] W Polsce kampania wyborcza rozpoczyna się z dniem ogłoszenia aktu właściwego organu o zarządzeniu wyborów i ulega zakończeniu na 24 godziny przed dniem głosowania. Zjawisko omawiane w niniejszym artykule jest jednak dużo bardziej złożone i z pewnością wykracza swoim zasięgiem poza granice czasowe kampanii wyborczych i referendalnych w polskim prawie.

[17] Ustawa z dnia 5 stycznia 2011 r. – Kodeks wyborczy (tekst jedn.: Dz. U. z 2019 r. poz. 684 ze zm.).

[18] Ustawa z dnia 11 stycznia 2018 r. o zmianie niektórych ustaw w celu zwiększenia udziału obywateli w procesie wybierania, funkcjonowania i kontrolowania niektórych organów publicznych (Dz. U. poz. 130).

dezinformacją z użyciem propagandy obliczeniowej[19]. Pojęcie propagandy występuje w art. 35 ust. 1 u.r.l.[20], ale nie należy go utożsamiać z tytułowym zagadnieniem. Z brzmienia art. 35 ust. 1 u.r.l. wynika, że propaganda referendalna nie dozna ograniczeń, dopóki nie będzie zawierała nieprawdziwych danych i informacji.

Zasadniczo rzecz ujmując, polski system wyborczy pozostawia w sferze autonomii jednostki wybór techniki wpływu i ocenę jakości warstwy informacyjnej agitacji wyborczej, agitacji referendalnej oraz propagandy referendalnej. Ustawodawca zadowala się założeniem, iż jawność pochodzenia komunikatu i sądowa ochrona przed rozpowszechnieniem informacji nieprawdziwych stanowią wystarczające rozwiązania dla prawidłowego kształtowania preferencji wyborczych. Trzeba przyznać, że założenie to było prawidłowe w momencie tworzenia demokratycznego prawa wyborczego po odzyskaniu suwerenności. Nie należy więc przyłączać się do tradycyjnego lamentu nad krótkowzrocznością lub irracjonalnością ustawodawcy – zjawisko, które omawiam w tym artykule, jest relatywnie nowe. Wiarygodne i udokumentowane badania nad zastosowaniem propagandy obliczeniowej w celu manipulacji opinią publiczną sięgają 2012 r. (zob. dalsze uwagi w pkt 2). Łatwość, z jaką przychodzi nam dziś opisywać propagandę obliczeniową w kategoriach realnego zagrożenia dla demokracji, jest podbudowana sześcioletnią obserwacją organizacji i przebiegu wyborów i referendów na świecie. Jeśli mamy powody do krytyki, to raczej wynika ona z zaniechania polskiego ustawodawcy w sytuacji, w której mamy już dowody na wielowymiarowość tego zjawiska[21]. Ewidentnie wykracza ono poza horyzont czasowy i prawny jakiejkolwiek kampanii wyborczej (w rozumieniu polskiego prawa)[22], ponieważ propagandę obliczeniową stosuje się w celu wytworzenia zagrożenia dla porządku publicznego, bezpieczeństwa państwa, jego obywateli i suwerenności. Jej wykonawcami są zarówno wrogie państwa stosujące tzw. wojnę hybrydową, jak i krajowe podmioty (np. partie polityczne lub tzw. GONGO[23]), a nawet

---

[19] M. Bernaczyk, *Polski kodeks wyborczy wobec manipulacji i innych form propagandy obliczeniowej* (w:) *Znaczenie nowych technologii dla jakości systemu politycznego*, red. M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec, Toruń 2019.

[20] Ustawa z dnia 15 września 2000 r. o referendum lokalnym (tekst jedn.: Dz. U. z 2019 r. poz. 741). W praktyce pojęcie agitacji i propagandy bywa utożsamiane – por. postanowienie Sądu Okręgowego w Warszawie z dnia 24 kwietnia 2018 r., XXV Ns 43/15 (nieprawomocne), dotyczące art. 105 k. wyb.: „Agitacja wyborcza jest zamierzoną działalnością propagandową mającą na celu zjednywanie zwolenników dla określonej sprawy lub z chęci zdyskredytowania przeciwników".

[21] Krytycznie o stanie debaty publicznej na temat prowadzenie cyfrowej kampanii wyborczej w Polsce – zob. A. Kaźmierska, W. Brzeziński, *Jak nas lepią demiurgowie*, „Tygodnik Powszechny" z 7 października 2018 r., s. 13–14.

[22] Nie każdy przejaw propagandy obliczeniowej uda się powiązać z pojęciem agitacji wyborczej w rozumieniu polskiego prawa wyborczego. W praktyce stosowania przepisów ustanawiających granice agitacji wymagane jest ustalenie, iż rozpowszechnianie informacji było ewidentnie ukierunkowane „wolą spowodowania określonych zachowań uprawnionych do głosowania" – por. uzasadnienie wyroku Sądu Okręgowego w Warszawie z dnia 13 czerwca 2012 r., II Ns 15/12.

[23] *Government-organized non-governmental organization* (GONGO) to termin ukuty w latach 80. XX w. w celu opisania organizacji pozarządowych (fundacji, stowarzyszeń), które założono przez władze publiczne lub przy ich bezpośrednim bądź pośrednim zaangażowaniu finansowym, w celu imitowania oddolnej inicjatywy społecznej. Obrazowym przykładem takiej działalności państwa jest sprawozdanie Specjalnego Sprawozdawcy Rady Praw Człowieka ONZ z dnia 5 kwietnia 2018 r. (*Report of the Special Rapporteur on the independence*

organy autorytarnej władzy publicznej, funkcjonariusze władzy publicznej szykanujący swych krytyków[24] i opozycję.

Z tego powodu podejmę się ramowej analizy tego groźnego zjawiska, rozpoczynając od identyfikacji zagrożonych konstytucyjnych wartości ze wskazaniem wielowymiarowości i płynności stanów zagrożenia.

II. Zasady i wartości konstytucyjne RP jako punkt odniesienia dla oceny zagrożeń kreowanych przez propagandę obliczeniową

Propaganda obliczeniowa ma pewien szczególny kontekst w krajach Europy Środkowo-Wschodniej, które do końca lat 80. XX w. znajdowały się w radzieckiej strefie wpływów i obecnie są poddawane informacyjnemu oddziaływaniu podmiotów pośrednio bądź bezpośrednio powiązanych z Federacją Rosyjską. Ocenia się, że kampanie dezinformacyjne organizowane i finansowane przez Rosję w cyberprzestrzeni posługują się unowocześnioną metodyką stosowaną w okresie zimnej wojny jako komponent tzw. środków aktywnych. Pojawieniu się tego idiomatu w polskim dyskursie publicznym towarzyszy pewna przewrotność. Jego genezy upatruje się w angielskim sformułowaniu *active measures*, zaś to ostatnie stanowi bezpośrednie zapożyczenie dokonane przez Departament Stanu USA z rosyjskiego żargonu kontrwywiadowczego KGB (*ros. активные мероприятия*)[25]. Amerykańska trawestacja tego sformułowania koncentruje się na pojęciu dezinformacji, które stanowi dominujący element zarówno środków aktywnych, jak i „technologii hybrydowych"[26]. W nomenklaturze NATO (zaadaptowanej przez UE) działania dezinformacyjne zaliczane do środków aktywnych określa się jako komunikację strategiczną. Unia Europejska wprost określa rosyjską komunikację strategiczną jako element działalności wywrotowej, zagrożenie dla współpracy i suwerenności UE oraz niezależności politycznej i integralności terytorialnej Unii i jej państw członkowskich[27].

---

of judges and lawyers on his mission to Poland, A/HRC/38/38). Punkt III.A.19 wskazuje na wykorzystanie majątku pochodzącego od spółek z udziałem Skarbu Państwa do przeprowadzenia przez Polską Fundację Narodową medialnej kampanii pod hasłem „Sprawiedliwe sądy". Wśród fundatorów znalazło się kilka spółek prawa handlowego wymienionych w art. 13 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (tekst jedn.: Dz. U. z 2019 r. poz. 1302 ze zm.). Należy pamiętać, że obok kampanii billboardowej w mediach społecznościowych powstały profile „Sprawiedliwe sądy" (Facebook, Twitter oraz YouTube).

[24] M. Gałczyńska, *Śledztwo Onetu. Farma trolli w Ministerstwie Sprawiedliwości, czyli „za czynienie dobra nie wsadzamy"*, Onet.pl, 19 sierpnia 2019 r., https://wiadomosci.onet.pl/tylko-w-onecie/sledztwo-onetu-farma-trolli-w-ministerstwie-sprawiedliwosci-czyli-za-czynienie-dobra/j6hwp7f (dostęp: 16 grudnia 2019 r.).

[25] J. Darczewska, P. Żochowski, *Środki aktywne. Rosyjski towar eksportowy*, „Punkt Widzenia" 2017, nr 64, s. 12–13. Pojęcie środków aktywnych w języku KGB było znacznie szersze niż dezinformacja. Ta ostatnia stanowi „zaledwie" składową tego pojęcia.

[26] J. Darczewska, *Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18 (10), s. 49.

[27] Zob. pkt 11 rezolucji Parlamentu Europejskiego z dnia 23 listopada 2016 r. w sprawie unijnej komunikacji strategicznej w celu przeciwdziałania wrogiej propagandzie stron trzecich, 2016/2030(INI).

Skuteczna propaganda obliczeniowa – z istoty rzeczy oparta na dezinformacji – użyta jako instrument wrogiego wpływu powoduje, że faktyczne sprawstwo w sferze polityki zostaje przeniesione poza konstytucyjne ośrodki sprawowania władzy. Jeśli wykonywanie kompetencji przez władze publiczne jest konsekwencją ukrytego scenariusza zaplanowanego poza krajowymi organami politycznymi (niezależnie od tego, czy mówimy tu o wrogach „wewnętrznych", czy „zewnętrznych" utożsamianych z innym podmiotem prawa międzynarodowego), to możemy mówić o faktycznym ograniczeniu suwerenności rozumianej jako utrata władzy zwierzchniej w sferze polityki wewnętrznej (całowładności)[28]. Jeśli propaganda obliczeniowa została użyta przeciwko ludności określonego państwa lub jego władzom przez inny podmiot prawa międzynarodowego, to powinna być również analizowana z uwzględnieniem „międzynarodowego" aspektu suwerenności (samowładności) rozumianego jako sfera i metoda układania stosunków z innymi podmiotami prawa międzynarodowego w sposób wolny od zewnętrznych wpływów (zob. art. 5 *ab initio* Konstytucji RP[29]), wyjąwszy te, które są efektem zgody na wkroczenie obcego porządku międzynarodowego lub ponadnarodowego na terytorium danego państwa. Propaganda obliczeniowa użyta w ramach wrogiej doktryny wojennej przeciwko innemu państwu uderza w dwie nierozerwalne konstytutywne cechy suwerenności państwa: władzę zwierzchnią (na określonym terytorium) oraz niepodległość (niezależność od wpływu). Do tych wątków należy dodać trafne spostrzeżenia A. Bień-Kacały, która postuluje rozpatrywanie konstytucyjnego (wieloznacznego, wielopodmiotowego, wieloaspektowego) pojęcia bezpieczeństwa w powiązaniu z zasadą dobra wspólnego (trafnie wiążąc bezpieczeństwo obywateli z art. 5 z art. 1 Konstytucji RP oraz konstytucyjną kategorią obowiązków wobec państwa i innych obywateli)[30]. Podkreślam, że obywatel jest silnie uprzedmiotowiony przez rozpatrywane formy manipulacji: technologie informacyjne zaprzężone na użytek propagandy obliczeniowej pozwalają odwoływać się nawet do jego sfery intymnej, eksploatują naturalną potrzebę bezpieczeństwa, a wywołane zaburzenie obracają przeciwko państwu.

Dostrzeżenie tego zjawiska umożliwia wstępną odpowiedź na pytanie o rodzaje zagrożonych wartości i zasad konstytucyjnych, a także podmioty konstytucyjnie odpowiedzialne za wykrywanie, przeciwdziałanie i zwalczanie zagrożeń wywoływanych propagandą obliczeniową. W szczególności chodzić tu będzie o zasadę suwerenności narodu (art. 4 Konstytucji RP) ze wskazaniem na odzyskanie suwerenności jako zdarzenie kształtujące tożsamość konstytucyjną III RP (zob. drugi wiersz preambuły do Konstytucji RP). Dodatkową wartością konstytucyjną pozostającą w związku merytorycznym z suwerennością jest niepodległość[31], a także różnorodnie klasyfikowane bezpieczeństwo[32].

---

[28] Zwięzły przegląd poglądów nauki prawa dot. pojęcia „suwerenność" jako pojęcia konstytucyjnego i międzynarodowego przygotował K. Działocha (w:) *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, M. Zubik, t. 1, Warszawa 2016, komentarz do art. 4 Konstytucji RP, pkt II.9, s. 194–196.

[29] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.).

[30] A. Bień-Kacała, *Bezpieczeństwo w Konstytucji RP z 1997 r. – wstępna diagnoza*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2, s. 16–17.

[31] K. Działocha (w:) *Konstytucja...*, komentarz do art. 4 Konstytucji RP, pkt II.12, s. 203.

[32] Szerzej na ten temat zob. A. Bień-Kacała, *Bezpieczeństwo...*, s. 18.

Tak stanowcze i silne postawienie sprawy może oczywiście rodzić głosy dezawuujące. Przeciętnemu odbiorcy trudno jest sobie wyobrazić, że np. amerykańska spółka akcyjna Facebook Incorporated (z rocznym dochodem wynoszącym w 2017 r. ponad 40 miliardów dolarów amerykańskich) – będąca właścicielem najpopularniejszego serwisu społecznościowego Facebook, a także świadcząca popularną usługę Instagram czy Whatsapp – może w jakikolwiek sposób wpływać na przebieg procesu politycznego w danym państwie. Podobnym (i równie przezroczystym) zjawiskiem dla prawnej analizy systemu wyborczego jest oszałamiającą kariera mikroblogów, takich jak doceniony przez polską politykę[33] Twitter należący do amerykańskiej spółki Twitter Incorporated (z szacowanym zyskiem operacyjnym w trzecim kwartale 2018 r. 320 milionów dolarów amerykańskich). Próba plastycznego opowiedzenia o zagrożeniach kreowanych za pomocą serwisów społecznościowych lub mikroblogów często napotyka na dość naturalny opór audytorium. W Polsce liczba aktywnych kont Facebooka w 2018 r. przekroczyła 16.000.000, zaś w lutym 2018 r. liczba „realnych" użytkowników Twittera osiągnęła 4.610.000 osób[34].

Użytkownikowi usługi elektronicznej z pewnością nie jest łatwo zaakceptować, że niekiedy sama tylko „pasywna" obecność w serwisach społecznościowych przyczynia się do kreacji, wzmacniania zjawisk niebezpiecznych dla społeczeństwa i państwa. Dostrzega to zresztą sam dostawca usługi[35]. Obecność w mediach społecznościowych stała się częścią stylu życia. Istota ludzkiego zdrowia psychicznego tkwi między innymi w dobrym mniemaniu o sobie[36], więc dyskurs prawniczy, socjologiczny o potrzebie prawnego ograniczenia mrocznej strony serwisów społecznościowych w pewien sposób dotyka bezpośrednio ich użytkownika, pozostawiając go z wrażeniem, iż jego styl życia jest atakowany przez polityków.

---

[33] W 2017 r. na ustawową liczbę 460 posłów Sejmu RP ponad połowa posiadała konto (269), z czego 187 to profile aktywne. Spośród 100 senatorów tylko 36 założyło profile na tym kanale społecznościowym, ale korzystało z nich jedynie 17 – zob. badanie przeprowadzone przez spółkę doradczą Hill and Knowlton Poland „Politycy na Twitterze: kogo obserwują polscy parlamentarzyści?", 19.01.2017 r., http://hkstrategies.pl/pl/PR-News/ (dostęp: 20 stycznia 2017 r.).

[34] Podaję statystyki z badania Gemius/PBI opracowane przez serwis Wirtualnemedia.pl – zob. https://www.wirtualnemedia.pl/artykul/twitter-jacy-sa-jego-polscy-uzytkownicy-przewazaja-mezczyzni-osoby-z-duzych-miast-i-ze-srednim-lub-wyzszym-wyksztalceniem-analiza (dostęp: 30 listopada 2018 r.).

[35] „Poprzez umiejętne wykorzystanie mediów społecznościowych operatorzy informacji mogą podejmować próby zniekształcenia publicznego dyskursu, rekrutowania zwolenników lub finansujących bądź wpływu na polityczne i militarne rezultaty. Te przedsięwzięcia mogą być niekiedy zostać osiągnięte bez istotnych kosztów lub ryzyka po stronie ich organizatorów. Dostrzegamy kilka wiodących czynników w takim działaniu: Dostęp – globalny zasięg stał się możliwy: przywódcy i myśliciele, po raz pierwszy w historii, mogą docierać do globalnego audytorium (i potencjalnie na nie wpływać) poprzez nowe media, takie jak Facebook. Ten zwiększony dostęp daje wiele korzyści, ale i możliwości działania podmiotom działającym w złej wierze, by docierały do globalnych odbiorców w ramach operacji informacyjnych. **Każdy jest potencjalnym wzmacniaczem** [wyróżnienie – M.B.; w ang. oryg. »Everyone is a potential amplifier«]: być może najbardziej krytyczne znaczenie ma to, że każda osoba w medialnie uspołecznionym świecie może działać jako orędownik na rzecz sprawy politycznej, w którą wierzy. To oznacza, że dobrze przeprowadzone operacje informacyjne maja zdolność oddziaływania w sposób naturalny, poprzez autentyczne kanały i sieci, nawet jeśli biorą swój początek z nieprawdziwych źródeł takich jak fałszywe konta" – J. Weedon, W. Nuland, A. Stamos, *Information Operations and Facebook*, Version 1.0, 27 kwietnia 2017 r., s. 4, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf (dostęp: 26 grudnia 2018 r.).

[36] Zob. J.K. Gierowski, T. Jaśkiewicz-Obydzińska, M. Najda, *Psychologia w postępowaniu karnym*, Warszawa 2008, s. 74.

Ten tragiczny wymiar sytuacji widać już w odbiorze społecznym ubiegłorocznych przesłuchań przed amerykańską senacką Komisją ds. Wywiadu[37], badającą wykorzystanie m.in. usług Facebook, Twitter lub Google przez Federację Rosyjską w celu wywarcia wpływu na wybory prezydenckie w 2016 r. Wszelkie próby uregulowania kampanii politycznej w mediach społecznościowych nakręcają pewną spiralę niemocy, gdy zaczynają łączyć się z oskarżeniem o ograniczanie swobody wypowiedzi. Nie należy jednak obciążać portali społecznościowych odpowiedzialnością w oderwaniu od lokalnego kontekstu. Trzeba podkreślić, że same w sobie nie generują dezinformujących treści, ale służą przede wszystkim jej rozpowszechnianiu. Ta ostatnia pojawia się więc dzięki aktywności indywidualnych użytkowników lub botów społecznościowych, którzy starają się włączyć do mainstreamowego przekazu nieprawdziwe lub stronnicze informacje pochodzące z serwisów telewizyjnych lub internetowych (np. afiliowana w Rosji telewizja RT lub serwis internetowy Sputnik w różnych wersjach językowych)[38].

Nie podlega dyskusji, że usługi sieciowe kojarzą się z wolnością, swobodną wymianą informacji, poglądów, rozrywką, autokreacją użytkowników, promocją określonego stylu życia, platformą promocji i sprzedaży dóbr, usług, ale przejście od tych zjawisk do mechanizmów budowania zbiorowych lęków, rozpowszechniania fałszywych informacji i kłamstwa jest wyjątkowo łatwe. Tej łatwości nie mamy już jednak w ocenie zakresu zastosowania norm konstytucyjnych, ponieważ reakcja władz publicznych Rzeczypospolitej związanych prawem musi być proporcjonalna do interesu publicznego (w rozumieniu art. 31 ust. 3 zdanie pierwsze Konstytucji RP). Problem polega na ustaleniu granicy pomiędzy zagrożeniem dla porządku publicznego a zagrożeniem bezpieczeństwa państwa (por. art. 31 ust. 3 zdanie pierwsze Konstytucji RP), ponieważ granica między jednym a drugim determinuje również wybór podmiotów odpowiedzialnych za zwalczanie propagandy obliczeniowej.

Jeśli propaganda obliczeniowa jest używana przez inne państwo do destabilizacji systemu politycznego innego państwa, polaryzacji jego społeczeństwa jako narzędzie wspierające wojnę konwencjonalną (tak jak się to dzieje w przypadku działań Federacji Rosyjskiej przeciwko Ukrainie), to wiodącym podmiotem odpierającym (lub koordynującym tego typu działania ze służbami cywilnymi) wydają się być siły zbrojne[39]. Publicznie wyrażana

---

[37] Obszerny materiał dot. rosyjskich wpływów zebrany dzięki przesłuchaniom analityków, naukowców, wojskowych znajduje się pod adresem https://www.intelligence.senate.gov/hearings/transcripts (dostęp: 30 listopada 2018 r.). Obejmuje on również informacje dot. ekspozycji Polski na rosyjską propagandę, w tym systematycznego podważania legitymacji Sojuszu Północnoatlantyckiego w Polsce i krajach nadbałtyckich.

[38] Przegląd tych i innych źródeł operujących za pomocą dezinformacji w Polsce i innych państwach Grupy Wyszehradzkiej zawiera raport Centrum Stosunków Międzynarodowych: A. Wierzejski (red.), J. Syrovatka, D. Bartha, B. Feledy, A. Rácz P. Macovei, A. Wierzejski, D. Fischer, M. Gontar, *Information warfare in the Internet. Countering Pro-Kremlin Disinformation in the CEE countries. Analysis (2017/6)*, http://www.csm.org.pl (dostęp: 26 grudnia 2018 r.).

[39] Ze względu na konstytucyjnie wyznaczone kierunki działania Sił Zbrojnych Rzeczypospolitej Polskiej (art. 26 Konstytucji RP) taka teza może budzić pewien opór, ale wbrew pozorom nie jest zjawiskiem nowym. Użycie sił zbrojnych do zwalczania zagrożeń kreowanych za pomocą niszczenia lub przejmowania środków przenoszenia informacji wynika z wprowadzenia do polskiego systemu bezpieczeństwa narodowego takich pojęć jak „cyberprzestrzeń" i „cyberbezpieczeństwo". Zostały one zaproponowane w Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej wydanej przez Biuro Bezpieczeństwa Narodowego dnia 22 stycznia 2015 r. jako dokument „wykonawczy" do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, s. 34, http://bip.mon.gov.

opinia prominentnych polskich funkcjonariuszy Sił Zbrojnych jest dość jasna: propaganda obliczeniowa jest częścią wojny *nomen omen* hybrydowej[40]. Rzecz jednak w tym, że oceny propagandy cyfrowej dokonuje się często z perspektywy czasu, kiedy inne elementy sytuacji o charakterze czysto militarnym (np. zbrojna napaść na terytorium) są już znane, zaś rola propagandy obliczeniowej – jako fragment większego planu militarnego napastnika – oczywista.

Warto więc odnotować, że funkcje Sił Zbrojnych w Konstytucji RP (art. 26 ust. 1 wskazuje na zapewnienie bezpieczeństwa bez bliższego określenia jako „wewnętrzne" lub „zewnętrzne") w żaden sposób nie przekreślają możliwości przypisania im kompetencji zmierzających do przeciwdziałania i zwalczania naruszeń bezpieczeństwa wewnętrznego za pomocą propagandy obliczeniowej. Przeciwnie, wewnętrzny aspekt bezpieczeństwa należy uznać za zbieżny z konstytucyjną płaszczyzną działania Sił Zbrojnych. Wojciech Sokolewicz przedstawił nawet silniejszy pogląd, który otwierał drogę do przypisywania „Siłom Zbrojnym i ich organom zadań i kompetencji, które nie mieszczą się w owych funkcjach [chodzi o »funkcje« wymienione w art. 26 ust. 1 Konstytucji RP – M.B.]"[41]. Brak rozróżnienia bezpieczeństwa na wewnętrzne i zewnętrzne impregnował Konstytucję RP na pewien dylemat związany z prawną oceną działań inicjowanych poza terytorium Polski, lecz wywołujących skutki w naszym kraju[42]. Jeszcze trudniejsza sytuacja następuje w momencie, w którym dowody wrogiej, niepożądanej aktywności stwierdza się na terytorium państwa dotkniętego taką aktywnością, ale sprawstwo lub pomocnictwo obcego państwa ma charakter poszlakowy. Widać to m.in. w trudnościach z prawnomiędzynarodową klasyfikacją konfliktu zbrojnego na wschodniej Ukrainie na tle art. 2 lub 3 Konwencji o polepszeniu losu rannych i chorych w armiach czynnych (I konwencja genewska) sporządzonej w Genewie dnia 12 sierpnia 1949 r. (Dz. U. z 1956 r. Nr 38, poz. 171, zał.). Konflikt zbrojny na terytorium Ukrainy – w zależności od wykazania związku separatystów i jego natężenia z Federacją Rosyjską – ocenia się np. jako „nieposiadający charakteru międzynarodowego" w początkowej fazie, lecz – wskutek aktywnego wsparcia Rosji – nabrał on cech „międzynarodowego konfliktu zbrojnego"[43]. Wojciech Sokolewicz sygnalizował podobną trudność na polskiej płaszczyźnie konstytucyjnej następująco: „Nie we wszystkich

---

pl/f/pliki/polityka_bezpieczenstwa/2014/11/Strategia_Bezpieczenstwa_Narodowego_RP.pdf, (dostęp: 27 lipca 2018 r.). Należy je rozumieć jako efekt interpretacji pojęcia „cyberprzestrzeń" wprowadzonego przez art. 1 pkt 2 ustawy z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222, poz. 1323), która weszła w życie dnia 2 listopada 2011 r.

[40] E. Żemała, *Jesteśmy na progu wojny* [rozmowa z generałem Waldemarem Skrzypczakiem], Warszawa 2018, s. 35–40. Podobnie: J. Ćwieluch, *Dlaczego przegramy wojnę z Rosją* [rozmowa z generałem Mirosławem Różańskim], Kraków 2018, s. 8 i 67.

[41] W. Sokolewicz, *Wojsko i Konstytucja*, Warszawa 2015, s. 21.

[42] Por. wypowiedź gen. M. Różańskiego „Kiedy dwa kraje wzajemnie obrzucają się błotem za pośrednictwem swojej telewizji publicznej, to dla mnie jest już wojna. Nieważne, czy jeszcze informacyjna, czy już propagandowa. Ale wojna. Myślę, że coraz częściej można mówić również o cyberwojnie, ale działania w sieci mają to do siebie, że niezwykle trudno odnaleźć źródło ataku. Czasami łatwiej się go domyślić, niż faktycznie wskazać" – J. Ćwieluch, *Dlaczego przegramy...*, s. 15.

[43] R. Heinsch, *Conflict Classification in Ukraine: The Return of the "Proxy War"?*, „International Law Studies" 2015, t. 91, s. 360.

wypadkach jest też łatwe precyzyjne rozróżnienie bezpieczeństwa zewnętrznego i wewnętrznego. Wprawdzie w wypadku bezpieczeństwa zewnętrznego mamy zawsze do czynienia z zagrożeniem militarnym, ale już choćby zagrożenia ze strony międzynarodowego terroryzmu mają wyraźnie charakter mieszany – militarny (»wojna z terroryzmem«), a jednocześnie kryminalny, podobnie jak wojska »zewnętrze« w pewnych sytuacjach wypełniają funkcje »wewnętrznych« (»policyjnych«)"[44].

W naukach społecznych bezpieczeństwo obejmuje zaspokajanie takich potrzeb jak: istnienie, przetrwanie, całość, identyczność, niezależność, spokój, posiadanie i pewność rozwoju[45]. Podobnie jak konstytucyjna kategoria porządku publicznego, bezpieczeństwo państwa nie przybrało bezspornej treści i nie jest wykluczone jego nakładanie się na przesłankę porządku publicznego. W nauce prawa konstytucyjnego starano się jednak oddzielać je od porządku publicznego, wskazując bezpieczeństwo jako przesłankę uzasadniającą ochronę przed zagrożeniami dla podstaw „bytu państwa, integralności jego terytorium, losu jego mieszkańców lub istoty systemu rządów"[46]. W ujęciu Leszka Garlickiego bezpieczeństwo państwa zdaje się korespondować z prewencyjnym lub następczym zwalczaniem zagrożeń o silniejszym stopniu i negatywnych skutkach aniżeli zagrożenia powiązane z porządkiem publicznym[47]. Bezpieczeństwo państwa obejmuje sferę zagrożeń kojarzonych z tzw. bezpieczeństwem narodowym. To ostatnie wiązało się tradycyjnie z „egzystencjalnymi potrzebami i interesami społeczności ludzkich zorganizowanych w państwa"[48]. W takim ujęciu bezpieczeństwo narodowe kojarzone jest głównie z dość klasycznym zagrożeniem w postaci wojny (agresji militarnej) przynoszącej śmierć ludności i zniszczenie mienia, więc instytucje bezpieczeństwa narodowego znajdują swe ucieleśnienie w militarnych strukturach państwa (siły zbrojne). Ten rodzaj bezpieczeństwa orientuje się głównie na zagrożenia zewnętrzne, chociaż badacze tego zagadnienia słusznie podkreślają, że taki podział traci już na ostrości, skoro współcześnie obserwujemy splot czynników wewnętrznych i zewnętrznych (zagrożenie polityczne, ekonomiczne i militarne, terroryzm jako narzędzie tzw. wojen hybrydowych wspieranych rozpowszechnianiem fałszywych informacji przy użyciu narzędzi propagandy obliczeniowej).

Jeśli więc mówimy o działaniach powodujących „tylko" zakłócenie bezpieczeństwa wewnętrznego lub porządku publicznego, których nie jesteśmy w stanie osadzić w ramach szerszego planu, to zasadne wydaje się przesunięcie ciężaru obowiązków na służby

---

[44] W. Sokolewicz, *Wojsko*..., s. 35–36, z odwołaniem do analogicznego wątku u W.J. Wołpiuka, *Bezpieczeństwo państwa i pojęcia pokrewne. Aspekty konstytucyjnoprawne* (w:) *Krytyka prawa*, t. 2, *Bezpieczeństwo*, red. W. Sokolewicz, Warszawa 2010, s. 192–200.

[45] J. Zygmuntowicz, *Bezpieczeństwo w nauce o stosunkach międzynarodowych*, „Problemy Bezpieczeństwa" 2007, nr 1, s. 24.

[46] L. Garlicki (w:) *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, t. 3, Warszawa 2002, komentarz do art. 31 Konstytucji RP, teza nr 22, s. 23.

[47] Porządek publiczny należy kojarzyć z „zapewnieniem prawidłowego funkcjonowania życia społecznego", przez co przesłanka ochrony porządku publicznego „nie jest bezpośrednio czy wyłącznie powiązana z »państwem«, a jest bliższa – niż przesłanka »bezpieczeństwa państwa« – ochronie praw i wolności jednostki przed codziennymi zagrożeniami" – L. Garlicki (w:) *Konstytucja*..., komentarz do art. 31 Konstytucji RP, teza nr 23, s. 25.

[48] J. Zygmuntowicz, *Bezpieczeństwo w nauce*..., s. 31.

informacyjno-wywiadowcze o charakterze ściśle wewnętrznym (np. Agencję Bezpieczeństwa Wewnętrznego), ale metodyka wojen hybrydowych zakłada bardzo dużą płynność przechodzenia z ochrony jednej wartości (porządek publiczny) w drugą (bezpieczeństwo zewnętrzne i wewnętrzne). Negatywny efekt może mieć „kroczący" charakter, co widać m.in. na przykładzie fałszywych wiadomości SMS rozsyłanych dnia 26 listopada 2018 r. w województwie lubelskim[49]. Problem związany z klasyfikowaniem zagrożeń wewnętrznych i zewnętrznych wywołał już zresztą pewien efekt w postaci konceptualizacji modeli zwalczania terroryzmu, który jest zależny od skalowalności stopnia zagrożenia. W nauce o bezpieczeństwie wskazuje się, że eskalacja terroryzmu w XXI w.[50] doprowadziła do wyodrębnienia dwóch zasadniczych modeli jego zwalczania: policyjnego i wojskowego[51]. Pierwszy opiera się na założeniu, że terroryzm powinien być zwalczany środkami charakterystycznymi dla dotychczasowego modelu zwalczania poważnej przestępczości. Drugi zakłada zastosowanie środków (zarówno w prawnym, jak i w potocznym tego słowa znaczeniu) charakterystycznych dla udziału w konflikcie zbrojnym, w przypadku którego sprawca lub osoba podejrzewana o terroryzm są traktowani niczym strona wojująca, napastnik w konflikcie zbrojnym, więc odpieranie sprowadzonego przez nich niebezpieczeństwa następuje z wykorzystaniem procedur i sprzętu typowego dla sił zbrojnych z dopuszczalnością fizycznej eliminacji napastnika[52]).

Powyższe rozważania pokazują, że na wartości związane treściowo z ochroną bytu państwa i obywateli umieszczone w Konstytucji RP z 1997 r. spoglądano przez pryzmat państwa i obywateli według kryteriów przestrzennych, a te są z istoty problematyczne w przypadku wrogiej aktywności prowadzonej w cyberprzestrzeni. Pojęcie cyberprzestrzeni pojawiło się w polskim porządku prawnym relatywnie późno (w 2011 r.) wskutek

---

[49] Tego dnia rozesłano wiadomości SMS udające komunikat Rządowego Centrum Bezpieczeństwa „wzywający mężczyzn w wieku 18–65 lat zamieszkałych na terenie gminy Dukla i Horodło (Woj. Lubelskie) do stawienia się na terenie urzędu gminy w dniu 27.11.2018 o godzinie 10 w związku z sytuacją kryzysową na Ukrainie". Zdarzenie miało w tle atak Rosji na jednostki ukraińskiej marynarki wojennej i związane z tym wprowadzenie stanu wojennego na Ukrainie (26 listopada o godzinie 14:00) na okres 30 dni. Rządowe Centrum Bezpieczeństwa zdementowało informację 27 listopada 2018 r. we wczesnych godzinach porannych, stanowczo zaprzeczając kolportowaniu takich wezwań przez władze (zob. https://twitter.com/RCB_RP/status/1067411901464936448; podaję wg stanu na 1 grudnia 2018 r.) i wskazując, że o zdarzeniu poinformowano Policję oraz Agencję Bezpieczeństwa Wewnętrznego). Niezależnie od źródeł tego incydentu (którego przeprowadzenie jest możliwe relatywnie prymitywnymi środkami, np. darmowymi bramkami SMS dostępnymi w internecie, ale i zaawansowanymi, jak np. przełamaniem zabezpieczeń operatora telekomunikacyjnego lub użyciem przenośnej stacji BTS), w mediach słusznie komentowano, że tego rodzaju wydarzenie obniżyło próg czujności adresatów i wiarygodność oficjalnych komunikatów.

[50] A. Tyburska oraz B. Jewartowski wprost posługują się pojęciem „wojny (szarpanej, podjazdowej, partyzanckiej)" dla określenia działań terrorystycznych, a także obrazują to przykładowym (aczkolwiek wciąż obszernym) zestawieniem zamachów terrorystycznych po 11 września 2001 r. – zob. A. Tyburska, B. Jewartowski, *Ustawa antyterrorystyczna wobec zjawiska współczesnego terroryzmu* (w:) *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, red. W. Zubrzycki, K. Jałoszyński, A. Babiński, Szczytno 2016, s. 263 i 268–278.

[51] Zob. A. Altman, *Introduction* (w:) C. Filkenstein, J.D. Ohlin, A. Altman, *Targeted Killings in an Asymmetrical World*, Oxford 2012, s. 5–6.

[52] Por. np. procedurę specjalnego użycia broni z art. 23 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (tekst jedn.: Dz. U. z 2019 r. poz. 796). Przepis adresuje specjalne użycie broni przede wszystkim do funkcjonariuszy Policji.

wspomnianej ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Wówczas to wszystkie ustawy dot. konstytucyjnych stanów nadzwyczajnych uzyskały jednobrzmiącą definicję legalną cyberprzestrzeni[53], w której mogą ziścić się przesłanki wprowadzenia stanu nadzwyczajnego. Ustawodawstwo nie odnosi się jednak do prewencyjnego zwalczania tych zagrożeń, mimo że np. Parlament Europejski zachęca struktury militarne państw członkowskich do zdecydowanej odpowiedzi na propagandę w cyberprzestrzeni wymierzoną przeciwko NATO, Unii Europejskiej i jej państwom członkowskim[54].

Nie chodzi więc już tylko o ochronę niepodległości utożsamianej z nienaruszalnością terytorialną (zob. art. 5, 26 i art. 126 ust. 2 Konstytucji RP), ale o postrzeganie niepodległości jako niezależności politycznej, swobody działania międzynarodowego, nawet jakości życia[55]. Oczywiście można wyrazić wątpliwości, czy stosowanie propagandy obliczeniowej może obniżać jakość życia, ponieważ nie przynosi widocznych na pierwszy rzut oka namacalnych strat materialnych (np. w infrastrukturze) ani nie zakłóca rutyny porządku społecznego (np. w transporcie publicznym, przesyle energii), jak to się dzieje w przypadku naruszenia cyberbezpieczeństwa. Uważam, że taki efekt jednak występuje, chociaż jest niezwykle trudny do opisu w kategoriach ilościowych, zwłaszcza gdy propaganda obliczeniowa podsyca istniejące uprzedzenia lub traumy. Trudno jest zmierzyć skalę implementowania strachu, niepewności i agresji w życiu prywatnym obywateli, polaryzując ich opinie i poglądy, a w dalszej perspektywie infekując sposób działania organów władzy.

---

[53] Zob. art. 2 ust. 1a ustawy z dnia 28 września 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (tekst jedn.: Dz. U. z 2017 r. poz. 1932); art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (tekst jedn.: Dz. U. z 2017 r. poz. 1928) oraz art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (tekst jedn.: Dz. U. z 2017 r. poz. 1897). Zgodnie z jednobrzmiącą budową ww. przepisów przez „cyberprzestrzeń" rozumie się „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne […], wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Według doktryny Cyberbezpieczeństwa Rzeczypospolitej Polskiej wydanej przez Biuro Bezpieczeństwa Narodowego dnia 22 stycznia 2015 r., uwzględniwszy przepisy odsyłające, cyberprzestrzeń to: „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami".

[54] Zob. pkt 15 i 37 rezolucji Parlamentu Europejskiego z dnia 23 listopada 2016 r. w sprawie unijnej komunikacji strategicznej w celu przeciwdziałania wrogiej propagandzie stron trzecich (2016/2030(INI)).

[55] Rozumiana jako „samodzielny wybór ustroju społeczno-politycznego i systemu gospodarczego, jak również kształtowania własnej przyszłości na tradycji, kulturze oraz innych wartościach narodowych" – J. Zygmuntowicz, *Bezpieczeństwo w nauce…*, s. 32 i literatura tam powołana.

III. Czym jest propaganda obliczeniowa?

Aby zrozumieć rolę propagandy obliczeniowej w obniżeniu poziomu politycznego dyskursu, zaadaptowaniu jej jako narzędzia międzynarodowej konfrontacji destabilizującego system polityczny przeciwnika, należy zwrócić uwagę na mechanizm działania współczesnych sieci komputerowych. Ilość informacji dostępnych człowiekowi przyrasta dziś w nieprzyswajalnym dla niego tempie. Dziennie powstaje 2,5 kwintyliona bajtów danych, zaś popularna wyszukiwarka Google przetwarza 3,5 miliarda zapytań dziennie[56]. Dla porównania warto dodać, że w momencie wejścia w życie Konstytucji RP z 1997 r. dostępność danych w internecie szacowano na 20 gigabajtów. Nad jakością, a zwłaszcza informatywnością danych dla przeciętnego użytkownika lepiej się nie rozwodzić, wystarczy poprzestać na truizmie, że współczesny internet nie byłby atrakcyjny ani możliwy do obsługi dla indywidualnego użytkownika, gdyby nie narzędzia wyszukujące informacje. Kluczowe zagadnienie pokazujące istotę problemu pojawia się w momencie, w którym skonfrontujemy człowieka z efektem pracy wyszukiwarki. Człowiek jest w stanie zapoznać się z ograniczoną ilością wyników, więc narzędzia proponują w pierwszej kolejności zestaw preferowanych wyników (chodzi o optymalizację dla wyszukiwarek internetowych SEO (ang. *search engine optimization)*, zwaną popularnie „pozycjonowaniem"). Kto i według jakich kryteriów proponuje (albo zakłóca) efekty pracy wyszukiwarki (tj. podawanie preferowanych wyników), staje się zasadniczą kontrowersją tkwiącą u podstaw analiz propagandy obliczeniowej. W ujęciu czysto teoretycznym nie jest to zjawisko nowe, ponieważ amerykańskie nauki, np. zarządzanie, prawo, politologia, oparte na różnych teoriach komunikacji, przypomniały dorobek sięgający lat 50. XX w. skoncentrowany na indywidualnym wymiarze, ale przede wszystkim na roli dziennikarstwa w życiu społecznym[57]. Wszystkie dążyły do konceptualizacji teorii komunikacji z uwzględnieniem konkretnych ról społecznych, aczkolwiek nie chodziło tu wyłącznie o wytwórców, nadawców czy odbiorców informacji, ale przede wszystkim o zdolność „strażników" do selekcjonowania nadmiaru informacji i przekazywania ich masowemu odbiorcy. Zjawisko opisywane jest do dziś jako *gatekeeping*[58], co zresztą nie jest przypadkowe: w ten sposób uwypukla się rolę metaforycznego „strażnika", „portiera" (*gatekeeper*). Współczesna koncepcja gatekeepingu polega na stworzeniu siatki pojęciowej adekwatnej do wymiany informacji w środowisku sieciowym, gdzie funkcja strażnika informacji uległa zwielokrotnieniu i hierarchizacji przy walnym wsparciu technologii informacyjnych (*gatekeeping technology*). Zakłada ona

---

[56] B. Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, Forbes, 21 maja 2018 r., https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#41b6751460ba (dostęp: 3 grudnia 2018 r.).

[57] Problem tkwi jednak w tym, że umasowienie dostępu do internetu spowodowało, iż dziennikarstwo sprzed epoki cyfrowej szybko zaczęto nazywać „konwencjonalnym" albo „profesjonalnym". Jego pozycja „strażnika" dobierającego treść dla odbiorcy uległa znacznemu zachwianiu – zob. B. Debatin, *The Internet as a New Platform for Expressing Opinions and as a New Public Sphere* (w:) *The SAGE Handbook of Public Opinion Research*, red. W. Donsbach, M.W. Traugott, London 2008, s. 68.

[58] „Simply put, gatekeeping is the process by which the billions of messages that are available in the world get cut down and transformed into the hundreds of messages that reach a given person on a given day" – P. Shoemaker, *Gatekeeping*, Newburry Park, California 1991, s. 1.

stworzenie normatywnego modelu relacji zachodzących pomiędzy strażnikami, a także pomiędzy strażnikami a osobami, którym ów strażnik dostęp do informacji selekcjonuje tudzież ogranicza[59].

W 2008 r. Karine Barzilai-Nahon zaproponowała, aby taka teoria (i jej nomenklatura) służyła do określenia, wobec „kogo, czego i pod jakimi warunkami" podmioty odpowiedzialne za selekcjonowanie informacji (*gatekeepers*) powinny zachować uwagę. Zasadniczym celem było ukazanie zależności pomiędzy władzą (rozumianą jako zdolność wpływu) a informacją. Ten stosunek władzy mógł zachodzić między określonymi podmiotami, więc zasadniczym elementem teorii stało się badanie relacji z perspektywy odbiorców informacji oraz ich znaczenia dla „strażników" przy uwzględnieniu czterech właściwości: 1) kontroli politycznej nad „strażnikiem"; 2) zdolności odbiorców do tworzenia informacji; 3) związków ze strażnikiem; 4) alternatyw dostępnych odbiorcy w kontekście gatekeepingu[60]. Jeśli przyjrzeć się szczegółowym propozycjom K. Barzilai-Nahon, a w szczególności konceptualizacji pojęć (które przed rewolucją cyfrową siłą rzeczy nie istniały), to można dostrzec, iż autorce nie chodziło jedynie o stworzenie narzędzi do badań strukturalnych. Opis działań, które *gatekeeper* podejmuje w stosunku do informacji, sugeruje, że owe działania poddano wartościowaniu w kategoriach etycznych. O ile niektóre proponowane przez autorkę pojęcia, np. „wybór", „uzupełnienie", „odmowa udostępnienia informacji", a nawet „ukierunkowanie" czy też „kształtowanie" informacji, wydają się neutralne aksjologicznie, o tyle inne, np. „manipulacja", już nie[61]. Uważam, że to również przyczyniło się do atrakcyjności tej teorii dla badaczy propagandy obliczeniowej, ponieważ nazwanie jej *nomen omen* propagandą zakłada, że jej odbiorca jest obiektem manipulacji. Dzisiejszy *gatekeeper* ma jednak do dyspozycji potężniejsze narzędzie niż kiedykolwiek w historii, ponieważ przetwarza informacje za pomocą algorytmów. To właśnie one, użyte przez podmioty rozchwiane etycznie lub najzwyczajniej zwalczające demokratyczny system wartości, dają ogromne pole do manipulowania odbiorcą komunikatu. Nie rozwijając szerzej tego wątku, należy dostrzec echa tych koncepcji w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej, który odrzucił supozycję Google Spain o skromnej roli pośrednika w poszukiwaniach ogólnodostępnych i niekontrolowanych przezeń danych. Ze względu na autonomiczny charakter działań przedsiębranych w stosunku do danych operatorzy wyszukiwarek internetowych zostali uznani za administratorów danych osobowych[62].

---

[59] Z pełną odpowiedzialnością za dobór słów przyznaję, że ograniczenie może mieć w tym wypadku pewien emotywny wydźwięk, ponieważ nieodparcie kojarzy się z faktycznym ograniczeniem wolności tych, którzy informację pozyskują. Wymagałoby to jednak wprowadzenia odrębnego, równoległego wątku, czy mamy tu do czynienia ze świadomym wycofaniem się jednostki ze sfery wolności i wyborem paternalistycznego traktowania przez dostawcę technologii, czy też wyzyskiwaniem swoistego cyfrowego analfabetyzmu przez użytkownika, który nie potrafi lub nie może skorzystać z alternatywnych narzędzi wyszukujących.

[60] K. Barzilai-Nahon, *Toward a theory of network gatekeeping: A framework for exploring information control*, „Journal of the American Information Science and Technology" lipiec 2008 r., vol. 59(9), s. 3.

[61] Tamże, s. 7–8.

[62] Zob. wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-131/12, Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos, Mario Costeja González: „Należy zatem stwierdzić, że operator wyszukiwarki internetowej, przeszukując Internet w zautomatyzowany, stały i systematyczny sposób

W ciągu ostatniej dekady odnotowujemy gigantyczny wzrost oddziaływania na opinię publiczną za pomocą mediów elektronicznych o silnie zindywidualizowanym przekazie, którego wzmocnienia lub proliferacji nie udałoby się osiągnąć bez algorytmu reagującego na określony komunikat tekstowy lub inną aktywność w internecie. Komunikat skierowany do wyborcy za pomocą szeroko pojętych mediów elektronicznych może odwoływać się do bardzo osobistych i niekoniecznie świadomie ujawnianych poglądów, uprzedzeń, które można wzmacniać, a dla uwiarygodnienia przekazu połączyć z innymi informacjami, które adresat niekoniecznie świadomie ujawnił operatorom np. serwisów społecznościowych. Algorytm może zareagować na konkretne sformułowanie, a nawet „odpowiedzieć" treścią wywołującą poczucie strachu lub zagrożenia dla wyznawanych wartości (np. bezpieczeństwa). Sedno tkwi w tym, że w zależności od otwartości interfejsu programistycznego aplikacji (ang. *Application Programming Interface*, API) jedna osoba jest w stanie stworzyć wiele fałszywych kont, by w rezultacie zbudować iluzję poparcia określonego komunikatu przez dziesiątki, setki użytkowników. Jednoznaczne przypadki zastosowania takich metod i technik do politycznych ataków, rozpowszechniania nieprawdziwych informacji, atakowania dziennikarzy odnotowano w wielu państwach świata, zarówno ze wskazaniem na potencjalnych inspiratorów wewnętrznych, jak i krajowe partie polityczne i instytucje publiczne. W 2013 r. w Australii użyto fałszywych kont Twittera do spreparowania poparcia dla bloku partii centroprawicowych (The Coalition) oraz premiera Anthony'ego Johna Abbotta. Spośród 203.000 obserwatorów (followersów) premiera Abotta aż 95% oszacowano jako fałszywych[63]. Przedsięwzięcie nie było zbyt wyrafinowane, a przez to łatwe do wykrycia, ale połączenie fałszywych kont z algorytmami symulującymi zachowania prawdziwego, „żywego" użytkownika przynosi z roku na rok coraz bardziej szkodliwe efekty. Badania wskazują, że połączenie tych elementów następuje często pod auspicjami władz publicznych, które ukrywają swoje zaangażowanie. Czynią tak dla wywołania fałszywego obrazu oddolnego, obywatelskiego, spontanicznego poparcia dla danej sprawy (z ang. tzw. *astroturfing*). Mogą też polegać na znacznie szkodliwszych działaniach niż budowanie pozytywnego wizerunku, np. zastraszaniu, nękaniu, ośmieszaniu, dezinformowaniu. Taką działalność państwa odnotowano np. w Argentynie, Azerbejdżanie, Ekwadorze (gdzie rząd bez większego sukcesu tworzył specjalną stronę Somos Mas [http://www.somosmas.ec/] wymierzoną w użytkowników krytykujących jego poczynania), Iranie, Korei Południowej, Syrii, Turcji, Meksyku, Wenezueli[64].

---

w poszukiwaniu opublikowanych w nim informacji, »gromadzi« takie dane, »odzyskiwane«, »zapisywane« i »porządkowane« przezeń następnie za pomocą oprogramowania indeksującego, »przechowuje« je na swych serwerach oraz, w odpowiednim przypadku, »ujawnia« i »udostępnia« je swym użytkownikom w postaci listy wyników ich wyszukiwań. Ze względu na to, że operacje te zostały wyraźnie i bezwarunkowo wskazane w art. 2 lit. b) dyrektywy 95/46, należy uznać je za »przetwarzanie« w rozumieniu tego przepisu, i bez znaczenia jest przy tym fakt, iż ten operator wyszukiwarki internetowej przeprowadza te same operacje również w odniesieniu do innego rodzaju informacji i nie wprowadza rozróżnienia między nimi a tymi danymi osobowymi". Por. także wyrok Sądu Najwyższego z dnia 13 grudnia 2018 r., I CSK 690/17, www.sn.pl.

[63] T. Peel, *The Coalition's Twitter fraud and deception*, „Independent Australia" z 26 września 2013 r.

[64] S. Bradshaw, P.N. Howard, *Troop, Trolls and Troublemakers: A Global Inventory of Social Media Manipulation*, Computational Propaganda Research Project, Working Paper 2017/12, s. 10–11.

Słowo „manipulacja" nie jest więc ani emocjonalne, ani przypadkowe. Manipulacja zakłada asymetrię pomiędzy manipulowanym a manipulatorem, zaś źródłem tej nierównowagi jest różnica w poziomie wiedzy pomiędzy stronami tej relacji. Manipulator ma do dyspozycji środki oddziaływania na osobę lub grupę, które mogą sprawić, by nieświadomie i z własnej woli realizowała cele manipulatora. Jednym ze środków wpływu na manipulowanego jest dostarczanie mu niepełnego, nieprawdziwego obrazu rzeczywistości, co tłumaczy, dlaczego w pierwszej kolejności do języka codziennego przeniknęły anglicyzmy: *fake news*[65] lub *post-true* (postprawda). To ostatnie sformułowanie zostało słowem 2016 r. *Słownika oksfordzkiego*[66]. Jego niechlubna kariera rozpoczęła się w czerwcu 2016 r., a szczyt zainteresowania przypadł na listopad tego samego roku. Te okresy są nieprzypadkowe, ponieważ zbiegły się w czasie z referendum w sprawie opuszczenia Unii Europejskiej przez Wielką Brytanię (dnia 23 czerwca 2016 r.) oraz wyborami prezydenckimi w Stanach Zjednoczonych Ameryki (dnia 8 listopada 2016 r.).

Ze względu na anglosaską proweniencję zjawiska nie powinno dziwić, że ten okres kojarzy się z narodzinami postprawdy, ale pojęcie nie jest do końca precyzyjne. Przedrostek *post-* w języku angielskim odwołuje się do następnego zjawiska w sekwencji wydarzeń, podczas gdy postprawda uzyskała nieco szersze znaczenie. Jeśli coś przypisujemy do postprawdy lub umieszczamy w czasie (okresie) postprawdy, to sugerujemy tym samym, iż prawda utraciła znaczenie. Nie jest więc ona kryterium rozstrzygającym lub co najmniej nie ma istotnej emotywnej wartości dla oceny zjawisk przyrodniczych, zachowań ludzi, działalności publicznych lub prywatnych instytucji. O ile postprawda jest więc określeniem kondycji społeczeństw wypierających prawdę lub racjonalną ocenę rzeczywistości, o tyle *fake news* jest instrumentem tworzenia takiego stanu. Samo sformułowanie nie jest nowe i istniało już na długo przed rewolucją cyfrową, np. w formie satyry, żartu lub fabrykowanych historii na potrzeby prasy bulwarowej, tabloidowej, tam, gdzie wartość informacji mierzona jej prawdziwością miała znikome znaczenie, liczył się zaś przede wszystkim poziom rozrywki czytelnika i zysk wydawcy.

Aktualna kariera sformułowania *fake news* ma już inny kontekst. Dotyka bowiem bardzo poważnego problemu związanego ze stabilnością systemu politycznego, a w szczególności wykorzystywania fałszywych informacji na skalę tak masową, że wpływa ona na poczucie bezpieczeństwa, interpretację rzeczywistości, a w ostatecznym rozrachunku na preferencje wyborcze. Nie manipuluje się jednostką, ale całymi grupami ludzi (co nie jest nowym zjawiskiem), w skali i z prędkością nienotowaną w dotychczasowej historii ludzkości. Ten ostatni czynnik spowodował przydanie propagandzie przymiotnika „obliczeniowa", ponieważ to technika przetwarzania cyfrowych informacji odgrywa kluczową

---

[65] Sformułowanie *fake news* w języku polskim wciąż nie doczekało się propozycji przekładu i być może się takowej nie doczeka. Anna Niepytalska-Osiecka zaobserwowała, że wyraz *fake* przeniknął z angielskiego slangu internetowego do języka wypowiedzi w polskim internecie, przystosował się pod względem pisowni, zaadaptował do rodzimej odmiany, a następnie na jego podstawie zaczęto tworzyć neologizmy słowotwórcze (np. fejkować) – A. Niepytalska-Osiecka, *O fejku, lajku i hejcie w polszczyźnie internetowej*, „Język Polski" 2014, z. 4, s. 343. W potocznej angielszczyźnie *fake* oznacza fałszerstwo, podróbkę, imitację, a przeniesienie pojęcia *fake news* do języka polskiego z angielskiego kontekstu internetowej komunikacji oznacza, najogólniej mówiąc, sfabrykowane, fałszywe wiadomości (tamże, s. 344).

[66] Zob. https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016 (dostęp: 12 grudnia 2018 r.).

rolę we wzmacnianiu przekazu. Warto więc w tym miejscu powtórzyć za S. Woolleyem i P.N. Howardem, że pojęcie propagandy obliczeniowej nie może być analizowane jako zjawisko czysto techniczne[67]. Nieuchronnie prowadziłoby do dysonansu, skoro środki techniczne są często obojętne pod względem etycznym, moralnym czy prawnym. Problematyczne stanie się dopiero ich użycie do manipulacji przez człowieka o określonej motywacji. Przymiotnik „obliczeniowa" symbolizuje nową formę propagandy, w której pejoratywna ocena technicznych środków przetwarzania informacji (platform społecznościowych, botów, algorytmów itd.) wynika wyłącznie z zaaplikowania ich w celu manipulacji. Nie podważa to jeszcze demokratycznego potencjału takich narzędzi (np. istnieją boty zaprogramowane do wykrywania i zwalczania dziecięcej pornografii).

Do podstawowych cech propagandy obliczeniowej należą więc:

1) umyślne podważanie symboli, znaczeń przez odwołanie się do sfery emocjonalnej i uprzedzeń odbiorcy, pomijające racjonalną ocenę, aby osiągnąć określone cele[68]; może towarzyszyć temu obniżenie jakości informacji za pomocą dość typowych zabiegów redakcyjnych[69];
2) użycie zautomatyzowanych, skalowalnych i anonimowych środków obliczeniowych do stworzenia lub rozpowszechniania informacji nieprawdziwej lub wprowadzającej w błąd[70].

Propaganda obliczeniowa zakłada, że do jej wdrożenia zostanie użyty co najmniej jeden z następujących elementów:

1) internetowy bot („bot" to skrót od słowa „robot") – program komputerowy automatycznie dostarczający treść;
2) fałszywe profile użytkowników portalu społecznościowego, które wymagają jednak ograniczonego nadzoru człowieka;
3) tzw. *junk news* lub *fake news* służące do dezinformowania w sferze polityki lub życia publicznego.

Propaganda obliczeniowa nie jest w pełni manualna ani też w całości zautomatyzowana. Przeciwnie, wskazuje się, że jej efektywne prowadzenie w sposób zautomatyzowany byłoby zależne od zatrudnienia programistów, co siłą rzeczy wymaga większych kosztów i czasu aniżeli zatrudnienie niewykwalifikowanych ludzi (tzw. trolli) do umieszczania

---

[67] S.C. Woolley, P.N. Howard, *Introduction...*, s. 4.

[68] Należy odnotować podobieństwo takich zabiegów do definicji propagandy w literaturze amerykańskiej. Propaganda jest tam rozumiana jako „zręczne posługiwanie się obrazami, sloganami i symbolami, odwołujące się do naszych uprzedzeń i emocji; jest komunikowaniem pewnego punktu widzenia, mającym na celu skłonienie odbiorcy do dobrowolnego przyjęcia tego punktu widzenia za swój" – T. Kacała, *Dezinformacja i propaganda...*, s. 53 z powołaniem na: A. Pratkanis, E. Aronson, *Wiek propagandy*, Warszawa 2004, s. 17.

[69] Na przykład w Czechach odnotowano skoncentrowanie przekazu na sprawach zagranicznych (które z założenia są trudne do weryfikacji, zaś przedstawione w pejoratywny sposób mogą wzmocnić tendencje izolacjonistyczne), korzystając przy tym z ekspresyjnego, a nierzadko wulgarnego języka, manipulacyjnych tytułów i zdjęć wywołujących negatywne emocje, niejasnych lub nieweryfikowalnych źródeł, uogólnień pod adresem grupy społecznej za pomocą indywidualnego przypadku, upozorowanych wypowiedzi eksperckich lub naukowych, nieprawdziwych lub silnie zniekształconych informacji, a także jednostronnej interpretacji wydarzeń – A. Wierzejski (red.), J. Syrovatka, D. Bartha, B. Feledy, A. Rácz P. Macovei, A. Wierzejski, D. Fischer, M. Gontar, *Information warfare...*, s. 9–10.

[70] Tamże, s. 5.

komentarzy zawierających pożądany komunikat polityczny. W efekcie propaganda obliczeniowa łączy oba czynniki[71]. Jest ona przedsięwzięciem, którego kosztów nie można generalizować określeniem „tania", lecz co najwyżej „tańsza". Obiegowa opinia o niskich kosztach takich operacji informacyjnych wynika najprawdopodobniej z roztrząsania kosztów ekonomicznych i logistyki propagandy obliczeniowej na tle konwencjonalnych (i drogich) środków konfrontacji międzynarodowej[72].

Pod względem metodyki działania propaganda obliczeniowa rozpoczyna się od utworzenia licznych profili, kont w mediach społecznościowych[73] (tzw. *fake accounts*). Badania prowadzone w Polsce sugerują, że podmiot prowadzący działalność marketingową jest w stanie pochwalić się kilkudziesięcioma tysiącami takich kont, posiadających m.in. indywidualną historię, opis zainteresowań, dane dotyczące wieku, płci, a zwłaszcza fotografie fikcyjnego użytkownika, co powoduje, że niełatwo jest zdemaskować fałszywą tożsamość. Konta zakładane są za pomocą dużych dostawców poczty, zaś same połączenia są maskowane przy użyciu wirtualnych sieci prywatnych. Proces następuje z odpowiednim wyprzedzeniem, aby stworzyć wrażenie, że profile mają swoją historię i nie powstawały lawinowo tuż przed okresem poprzedzającym zlecone przedsięwzięcie[74]. W polskim internecie oferuje się konta „do prowadzenia działalności reklamowej" (np. konto na portalu Facebook z minimum 200 znajomymi za 70 zł), niekiedy wprost przyznając, że nie towarzyszy im żadna autentyczna tożsamość. Wartość takiego „dobra" jest uzależniona nie tylko od liczby nawiązanych połączeń; czynnikiem zwiększającym wartość jest oczywiście możliwie najdłuższy staż istnienia profilu na portalu społecznościowym. Na Ukrainie i w rosyjskojęzycznym internecie istnieje rynek takich kont (np. darkstore.biz), zaś opisy tego typu ofert nie zawierają nawet żadnych subtelnych niedomówień, a wręcz nie pozostawiają wątpliwości, że chodzi o całe zestawy fałszywych kont. Niekiedy oferty budzą uzasadnione podejrzenia o związki z działalnością przestępczą (np. oferta konta Facebook „porzuconego" przez prawdziwe osoby, których login i hasła zostały ujawnione w niejasnych okolicznościach, rozpoczynająca się od 25 rubli).

W tym miejscu należy jednak stanowczo podkreślić, że usługi tego typu nie byłyby możliwe do przeprowadzenia, gdyby nie prawdziwe osoby zarządzające grupami kont,

---

[71] M. Zhdanova, D. Orlova, *Computational Propaganda in Ukraine*..., s. 263.

[72] Na przykład w 2017 r. udało się potwierdzić, że niesławna petersburska fabryka trolli należąca do rosyjskiego miliardera Jewgienija Prigożyna zmieniła siedzibę z dotychczasowego biura o powierzchni 4000 m^2 na powierzchnię komercyjną o powierzchni 12.000 m^2 w biznesowym kompleksie Łachta, zob. https://www.dp.ru/a/2017/12/29/Fabrika_trollej_perebir (dostęp: 28 grudnia 2018 r.). Dla porównania: nowy budynek Kancelarii Sejmu RP u zbiegu ul. Pięknej i Wiejskiej nie przekracza 10.000 m^2.

[73] Np. pkt 3.1 regulaminu świadczenia usług przez Facebooka przewiduje obowiązek użytkownika „nieudostępniania hasła, nieumożliwiania innym korzystania z własnego konta na Facebooku i nieprzenoszenia własnego konta na Facebooku na inną osobę (bez naszego pozwolenia)", https://www.facebook.com/terms.php?ref=p (dostęp: 28 grudnia 2018 r.). W praktyce obrotu cywilnoprawnego użytkownicy (w szczególności komercyjni) są zainteresowani sprzedażą i nabywaniem kont z pożądaną liczbą kontaktów, więc teoretycznie proces zmiany tożsamości konta jest zależny od zgody serwisu pod rygorem wstrzymania świadczenia usługi. Facebook przyjmuje jednak dość zaskakującą postawę i otwarcie przyznaje, że wymóg nie jest przez niego egzekwowany. Zob. szerzej K. Lejman, *Sprzedaż marki. Social media jako przedmioty obrotu*, „Dziennik Gazeta Prawna" z 27 stycznia 2018 r.

[74] Szerzej na ten temat zob. R. Gorwa, *Unpacking the Ecosystem*..., s. 98.

dbające o możliwie wiarygodny i niepowtarzalny przekaz. Jest to więc przedsięwzięcie wymagające ludzkiego zaangażowania, nadzoru. Boty mogą być narzędziami wspomagającymi ten proces, ale tylko do pewnego stopnia[75]. Istnieją więc osoby fizyczne, które można powiązać z takimi praktykami, aczkolwiek problemem byłoby przypisanie im odpowiedzialności za naruszenie prawa, w szczególności zasad prowadzenia kampanii wyborczej. Nie wyklucza to oczywiście odpowiedzialności za umieszczenie i rozpowszechnienie treści, aczkolwiek tu dochodzimy do zasadniczego problemu: czy należy tworzyć odrębną kategorię bezprawnego zachowania opartego na kryterium treści, opisując ją jako propagandę, dezinformację[76], czy też poprzestawać na karaniu cyfrowej imitacji ludzkich zachowań? Literatura dotycząca propagandy obliczeniowej zakłada niejako apriorycznie, że rozpowszechniane w ten sposób informacje szkodzą, ale niekoniecznie rozwodzi się nad merytoryczną zawartością takich informacji. Wygląda to jak milcząca zgoda autorów co do bezprawności treści, natomiast wachlarz zarzutów jest duży: od rozpowszechniania informacji nieprawdziwych[77], przez mowę nienawiści[78], sztuczne polaryzowanie dyskusji, do tzw. *junk news* o treściach ocennych, zbyt luźno zaczepionych w faktach (co pod pewnymi warunkami rodzi odpowiedzialność prawną w świetle standardów Europejskiego Trybunału Praw Człowieka[79]). Widać więc, że nie wszystkie kategorie informacji rozpowszechniane środkami technicznymi propagandy obliczeniowej kwalifikują się jako bezprawne. Przydanie im takiego charakteru też nie jest łatwe, o czym świadczy nieudany sprzeciw francuskiego senatu[80] wobec projektu stosownej ustawy[81] oraz krytyka niemieckiej ustawy z dnia 1 września 2017 r. o poprawie egzekwowania prawa w sieciach

---

[75] Ze względu na funkcje realizowane w ramach omawianych przedsięwzięć wyróżnia się boty serwisowe (np. oprogramowanie służące do zakładania kont), boty „wzmacniające" (używane do „polubień", dzielenia się i promowania określonej zawartości), boty „śledzące" (wykrywające lub reagujące na określoną aktywność innych użytkowników sieci), a nawet „skarżące" (używane do generowania wniosków w ramach procedur *notice-and-take-down*).

[76] W regionie tylko Litwa podniosła dezinformację do rangi zagrożeń konstytucyjnych, których nie można rozpatrywać w kategoriach wykonywania wolności rozpowszechniania informacji. Zgodnie z art. 25 ust. 4 konstytucji Republiki Litewskiej z dnia 25 października 1992 r.: „Wolność wyrażania przekonań i rozpowszechniania informacji jest niepołączalna z działalnością przestępczą, szerzeniem nienawiści narodowej, rasowej, religijnej i społecznej, przemocy i dyskryminacji, a także z oszczerstwem i dezinformacją" – *Konstytucja Republiki Litewskiej*, tłum. H. Wisner, Warszawa 2006.

[77] Co otwiera spór nad kontekstem prawdy jako pojęcia języka prawnego. Może bowiem chodzić o prawdę jako pojęcie normatywne (tzn. przy ustalaniu prawdziwości odwołujemy się do przepisów określających kryteria uznawania za prawdę) albo faktyczne, zob. pkt 4 uzasadnienia wyroku Trybunału Konstytucyjnego z dnia 12 września 2005 r., SK 13/05, www.trybunal.gov.pl.

[78] Zob. pkt 7 uzasadnienia wyroku Trybunału Konstytucyjnego z dnia 25 lutego 2014 r., SK 65/12, www.trybunal.gov.pl.

[79] Zob. szerzej L. Garlicki (w:) *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności*, t. 1, *Komentarz do art. 1–18*, red. L. Garlicki, Warszawa 2010, komentarz do art. 10 EKPC, s. 642–643.

[80] Zob. https://www.francetvinfo.fr/internet/reseaux-sociaux/facebook/le-senat-rejette-les-propositions-de-loi-sur-les-fake-news-sans-meme-discuter-du-texte_2869295.html (dostęp: 27 grudnia 2018 r.).

[81] Proposition de loi relative à la lutte contre la manipulation de l'information, No. 799, http://www.assemblee-nationale.fr/dyn/15/dossiers/lutte_fausses_informations (dostęp: 27 grudnia 2018 r.). Dnia 20 grudnia 2018 r. francuska Rada Konstytucyjna uznała przyjęte rozwiązania (zob. dalsze uwagi w pkt IV) za zgodne z francuskim blokiem konstytucyjnym – zob. orzeczenie nr 2018-773 DC z dnia 20 grudnia 2018 r., dostępne na stronie Rady, https://www.conseil-constitutionnel.fr (dostęp: 16 grudnia 2019 r.).

społecznościowych[82]. Tymczasem tylko w przypadku nieprawdziwych informacji (*fake news*) kryterium weryfikacji prawdy (rozpatrywanej jako konsekwencja oceny faktu naturalnego, empirycznego) poddaje się względnie łatwej pozytywizacji. Spróbujmy zatem zwięźle podsumować problemy, wyrazić postulaty lub co najmniej określić kierunki dalszych badań.

IV. Podsumowanie

1. Pierwszym i podstawowym założeniem formułowania jakichkolwiek postulatów *de lege ferenda* jest uznanie tezy o prawie państw członkowskich NATO i UE do regulacji swojej cyberprzestrzeni. Jest ono zakorzenione w koncepcji suwerenności, a w przypadku zagranicznego wpływu – w zasadzie nieinterwencji uznawanej za część zwyczajowego prawa międzynarodowego[83]. „Odmaterializowana" komunikacja, wielość połączonych sieci, liczba pośredników przesyłających informacje, staromodna metafora „wirtualnej rzeczywistości" często działają na prawników paraliżująco, prowadząc do apriorycznego założenia o znikomych efektach ewentualnej regulacji. Eksperci prawa międzynarodowego skupieni wokół Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi NATO podpowiadają jednak odmienne podejście. Talińska Instrukcja ws. Prawa Międzynarodowego Znajdującego Zastosowanie do Cyberoperacji (2.0) z 2017 r. wyraźnie stwierdza: „Fakt połączenia cyberinfrastruktury zlokalizowanej na terytorium danego Państwa z cyberprzestrzenią nie może być traktowany jako zrzeczenie się suwerenności. Co więcej, Państwa mają prawo, zgodnie z zasadą suwerenności, odłączyć od Internetu, w całości lub w części, jakąkolwiek cyberinfrastrukturę zlokalizowaną na ich terytorium, zależnie od traktatowego bądź zwyczajowego prawa międzynarodowego, dotyczącego zwłaszcza sfery międzynarodowych praw człowieka" (reguła 1)[84]. Dodatkowo podkreśla się, że z zasady suwerenności (wewnętrznej) wynika kompetencja państw do normowania trzech warstw cyberprzestrzeni: fizycznej, logicznej oraz społecznej. O ile te dwie pierwsze dotykają zagadnień technicznych (wszelkiego rodzaju urządzenia telekomunikacyjne nadawcze, odbiorcze oraz protokoły komunikacyjne, oprogramowanie odpowiedzialne za bezpieczne sterowanie przepływem sygnałów, szyfrowanie itp.), o tyle warstwa społeczna odnosi się do zachowań ludzi i osób prawnych w cyberprzestrzeni (zob. pkt 7 komentarza do reguły nr 2). Eksperci wskazują blokowanie dostępu do treści w mediach społecznościowych jako dozwolone ograniczenie wolności (zwłaszcza swobody wypowiedzi), lecz pod warunkiem zachowania przesłanek wynikających w systemu ochrony praw człowieka (zob. pkt 7 komentarza do reguły nr 2). Należy podkreślić, że kompetencja władzy ustawodawczej RP nie ogranicza się tylko do ochrony swoich interesów, ale musi

---

[82] Gesetz zur Verbesserung der Rechtdurchgesetzung in sozialen Netzwerken (Netzwerkdurchsetzunggesezt) – dalej: NetzDG. Weszła w życie dnia 1 października 2017 r., https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html (dostęp: 16 grudnia 2019 r.).

[83] K.N. Trapp, *State Responsibility for International Terrorism*, Oxford 2011, s. 30.

[84] M.N. Schmitt, L. Vihul (red.), *Tallin Manual 2.0 on The International Law Applicable to Cyber Operations*, Oxford 2017, komentarz do reguły 1, pkt 6.

uwzględniać również okoliczność, iż polska cyberprzestrzeń nie będzie wykorzystywana do podejmowania działań szkodliwych dla innych państw i podmiotów sojuszniczych. Musimy też mieć świadomość, że metodyka składająca się na propagandę obliczeniową znalazła uznanie zarówno krajowych podmiotów działających legalnie (np. komitety wyborcze i podmioty świadczące im różnego rodzaju usługi), jak i zagranicznych, mimo że ich agendę można uznawać za zgoła odmienną. Jedne i drugie sięgają jednak po różne elementy dezinformacji, przede wszystkim w celu eskalowania lęku i niepewności[85]. Ewentualne zmiany prawne powinny być nastawione na zwalczanie dezinformacji w sferze publicznej bez względu na jej wewnętrzny lub zewnętrzny charakter.

2. Szczególna uwaga badaczy propagandy obliczeniowej skupia się na jej związkach z polityką, ale nie redukuje jej wyłącznie do aktów politycznych uosabianych przez wybory i referenda. W rezultacie rozwiązania legislacyjne w tym zakresie słusznie przekraczają horyzont czasowy kampanii wyborczych, ingerując w ustawodawstwo z zakresu świadczenia usług elektronicznych lub ustroju radiofonii i telewizji. Pewnym wyjątkiem jest francuska ustawa organiczna z dnia 22 grudnia 2018 r. „dotycząca walki z manipulacją informacjami" (Loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information)[86] oraz ustawa z dnia 22 grudnia 2018 r. „dotycząca walki z manipulacją informacjami" (Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information)[87], które mają wyraźny cel: ochronę systemu wyborczego przed dezinformacją w internecie, której zasadniczego źródła upatrywano w nieprawdziwych (fałszywych) informacjach. Ustawa nr 2018-1202 znowelizowała kodeks wyborczy (Code électoral), nakładając na dostawcę sieci, mediów społecznościowych obowiązek przejrzystego oznaczenia materiałów wyborczych, reklamy politycznej oraz stworzenia efektywnego systemu *notice-and-take-down*. Użytkownik uzyskuje w ten sposób możliwość oceny wiarygodności informacji ze względu na jej pochodzenie i zgłaszania domniemanych *fake news* dostawcy usługi oraz władzom publicznym. Z kolei kandydaci w wyborach uzyskali możliwość ubiegania się o wydanie (w ciągu 48 godzin) orzeczenia sądowego nakazującego usunięcie nieprawdziwej informacji lub zakazu rozpowszechnianiu przekazów automatycznie zwielokrotnianych. Ustawa znowelizowała również francuską ustawę audiowizualną (tzw. ustawa o swobodzie komunikacji z dnia 30 września 1986 r., Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication[88]), dzięki czemu Wysoka Rada Audiowizualna (Conseil supérieur de l'audiovisuel) uzyskała prawo do odmowy zgody na nadawanie podmiotom kontrolowanym przez obce państwo, jeżeli świadczone przez nich usługi stwarzają poważne ryzyko naruszenia godności istoty ludzkiej, wolności i własności innych, pluralistycznej istoty wyrażania

---

[85] Zob. A. Walecka-Rynduch, *Lęk i niepokój jako elementy politycznych strategii komunikacyjnych. Analiza kampanii prezydenckiej i parlamentarnej w 2015 r.* (w:) *Oblicza kampanii wyborczych 2015*, red. M. Kułakowska, P. Borowiec, P. Ścigaj, Kraków 2016, s. 357.

[86] Zob. https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1201/jo/texte (dostęp: 16 grudnia 2019 r.).

[87] Zob. https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/texte (dostęp: 16 grudnia 2019 r.).

[88] Zob. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068930 (dostęp: 16 grudnia 2019 r.).

myśli i opinii, ochrony dzieci i małoletnich, utrzymania porządku publicznego, wymogów obrony narodowej lub zasadniczych interesów narodu koniecznych do jego normalnego funkcjonowania.

Francuskie i niemieckie doświadczenia ostatnich kilku lat pokazują trudności ze sformułowaniem materialnych kryteriów oceny bezprawnego charakteru informacji, więc np. niemiecka ustawa obejmuje zakresem regulacji rozpowszechnianie w sieciach społecznościowych informacji wyczerpujących znamiona przestępstwa (zob. definicję treści niezgodnych z prawem w § 1 (3) NetzDG). Związek z debatą publiczną lub konkretnym procesem wyborczym nie jest wymagany. W niemieckiej ustawie kwestia zwalczania fałszywych informacji jest niemal pomijana, chyba że problem prawdziwości informacji jest elementem normy prawnokarnej. Ustawa nakłada na dostawców mediów społecznościowych obowiązek stworzenia procedury rozpatrywania skarg na treści niezgodne z prawem (zob. § 3 NetzDG) i kwestia prawdziwości informacji jest do pewnego stopnia uwzględniona w warstwie proceduralnej. Wdrożony tryb musi zapewnić, że dostawca sieci społecznościowych niezwłocznie usunie lub zablokuje każdą treść niezgodną z prawem, najpóźniej w ciągu 7 dni. Termin ten może zostać przekroczony, gdy decyzja dostawcy stwierdzająca bezprawność treści zależy od fałszywości jakiegoś oświadczenia lub innych sprawdzalnych okoliczności faktycznych (zob. § 3 ust. 2 pkt 3 lit. a NetzDG). W pozostałych przypadkach ustawodawca niemiecki milczy na ten temat. Istota tych rozwiązań zmusza (pod rygorem sankcji administracyjnej) do wdrożenia systemu *notice-and-take-down* o wyraźnie określonych cechach i funkcjonalności[89], w którym personel dostawcy sieci społecznościowych musi zbadać zgłoszoną treść pod kątem zgodności z prawem i przedstawić skarżącemu swoje stanowisko[90]. Nie nakłada jednak sankcji za przetwarzanie treści niezgodnych z prawem, chociaż wprowadza dotkliwe grzywny m.in. za niewykonywanie obowiązków sprawozdawczych lub niewdrożenie systemu notyfikacji bezprawnych treści (zob. § 4 ust. 1 NetzDG).

3. W polskim piśmiennictwie prawniczym nie analizowano ani nie formułowano postulatów *de lege ferenda* dotyczących zwalczania propagandy obliczeniowej. Być może wynikało to z faktu, że dopiero po 2015 r. zaczęto badać jej formy, podkreślając trudności z mierzeniem jej wpływu na decyzje wyborcze[91]. Dotychczasowy stan wiedzy w prawie konstytucyjnym poprzestaje więc na znanych postulatach, mimo że polityka UE wzywa państwa

---

[89] Polskie prawo nie nakłada takiego obowiązku. Artykuł 14 ust. 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn.: Dz. U. z 2019 r. poz. 123 ze zm.) zawiera w swojej hipotezie sformułowanie „uzyskał wiarygodną wiadomość", ale nie precyzuje, jak ma wyglądać mechanizm komunikacji pomiędzy podmiotem świadczącym usługę a podmiotem zgłaszającym wiadomość o domniemanej bezprawnej treści.

[90] Na pierwszy rzut oka wydaje się, że jest to połowiczne rozwiązanie, ale musimy mieć świadomość, że w przeszłości dostawcy nie reagowali wcale lub w sposób nieadekwatny do okoliczności. W Polsce szerokim echem odbił się przypadek kradzieży tożsamości sędzi Trybunału Konstytucyjnego w stanie spoczynku, który ujawnił rażące niedostatki procedur notyfikacji przyjmowanych na zasadzie dobrowolności lub branżowej samoregulacji – zob. E. Siedlecka, *Facebook ma gdzieś twoją twarz. Wnioski po kradzieży tożsamości prof. Ewy Łętowskiej*, „Gazeta Wyborcza" z 13 stycznia 2015 r., http://wyborcza.pl/1,75398,17245749,Facebook_ma_gdzies_twoja_twarz__Wnioski_po_kradziezy.htm (dostęp: 27 grudnia 2018 r.).

[91] R. Gorwa, *Unpacking the Ecosystem…*

członkowskie do dalej idących wysiłków[92]. Ze względu na specyfikę internetu formułuje się krytykę przepisów dot. agitacji, postuluje się zniesienie ciszy wyborczej w internecie[93], a nawet – wbrew uprzednio powołanym globalnym tendencjom ograniczania swobody mediów społecznościowych – postulowano „wprowadzenie normy, która zagwarantowałaby administratorom stron internetowych wolność od odpowiedzialności za wykroczenia [zob. art. 498 k. wyb. – M.B.] popełniane przez innych użytkowników, ponieważ nie zawsze są oni w stanie kontrolować przebieg wirtualnej »dyskusji«"[94]. Pomijano przy tym całkowicie zagadnienie wykorzystywania sieci społecznościowych do manipulacji wyborcą przez strony trzecie (krajowe lub zagraniczne), a zwłaszcza sam model działania sieci społecznościowych, polegający na uzyskiwaniu wpływów z reklam i powiązanych usług bez względu na jakość lub legalność rozpowszechnianych treści[95]. W aktualnym stanie wiedzy (wymagane są oczywiście dalsze badania) uważam, że wyłączenie zakazu agitacji w internecie w całości lub w części po pierwsze, pozbawiłoby PKW i organy wymiaru sprawiedliwości jakichkolwiek mechanizmów zwalczania finansowania, gratyfikacji osób lub podmiotów prowadzących ukrytą propagandę obliczeniową zlecaną przez komitety wyborcze lub samych kandydatów, a po drugie, byłoby „liberalizacją" agitacji tylko z nazwy. W istocie byłaby to faktyczna rezygnacja z ciszy wyborczej wobec rosnącego dostępu do sieci i przenośnych urządzeń telekomunikacyjnych. Jest coś przewrotnego w polskim prawie wyborczym, skoro więcej miejsca poświęca ono szczegółowym przepisom dot. rozklejania materiałów wyborczych na urządzeniach telekomunikacyjnych (zob. art. 110 § 1 k. wyb.) aniżeli rozpowszechnianiu audiowizualnego materiału wyborczego za pomocą tych urządzeń w sieciach teleinformatycznych.

4. Zgodnie z art. 105 § 1 k. wyb. agitacja wyborcza polega na „publicznym nakłanianiu lub zachęcaniu do głosowania w określony sposób, w tym w szczególności do głosowania na kandydata określonego komitetu wyborczego". W świetle postanowienia SN z dnia 17 kwietnia 2018 r., IV KK 296/17, www.sn.pl, ogólnodostępne[96] portale, sieci społecznościowe, fora internetowe, blogi, wideoblogi są miejscami publicznymi (niezależnie od lokalizacji obsługujących je urządzeń). Rzeczywistym problemem jest powiązanie treści rozpowszechnianych w internecie z „nakłanianiem lub zachęcaniem". Podmioty

---

[92] Zob. obszernie na temat ochrony wyborów: punkty a–al zalecenia Parlamentu Europejskiego z dnia 13 lutego 2019 r. dla Rady oraz wiceprzewodniczącej Komisji/wysokiej przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa, zawierające podsumowanie działań podjętych przez Europejską Służbę Działań Zewnętrznych (ESDZ) dwa lata po sprawozdaniu PE w sprawie unijnej komunikacji strategicznej w celu przeciwdziałania wrogiej propagandzie stron trzecich (2018/2115(INI)).

[93] Zob. M. Borski, *Agitacja wyborcza jako ważny element kampanii wyborczej – wybrane zagadnienia*, „Roczniki Administracji i Prawa" nr XVII (zeszyt specjalny), s. 49.

[94] Zob. R. Balicki, K. Piech, *Ograniczenia swobody prowadzenia kampanii wyborczej w świetle regulacji Kodeksu wyborczego*, „Polityka i Społeczeństwo" 2015, nr 3 (13), s. 39. Dziś ten postulat można ocenić jako sprzeczny z aktualną polityką UE, chociaż należy nadmienić, że omawiane zjawiska były już znane w 2015 r.

[95] Na temat wpływu modelu marketingowego sieci społecznościowych na rozpowszechnianie się tzw. *junk news* zob. szerzej S. Bradshaw, P.N. Howard, *Why does junk news spread so quickly across social media? Algorithms, advertising and exposure in public life*, Miami 2018, s. 11.

[96] Problemem może być rozumienie owej ogólnej dostępności, co omawiam w odrębnym opracowaniu: M. Bernaczyk, *Polski kodeks wyborczy…*

prowadzące kampanie w mediach społecznościowych oparte na tzw. marketingu szeptanym lub partyzanckim (z założenia imitującym spontaniczne, naturalne zachowania, a w istocie ukrywającym związek z rzeczywistym beneficjentem przekazu) starają się postępować w taki sposób, aby ich symboliczne manifestacje zachowań (lajki, emotikony) lub wypowiedzi nie podawały odbiorcy „określonego sposobu głosowania". Dąży się do stworzenia psychologicznych warunków poparcia poglądów, idei większości (tzw. *bandwagon effect*), przy czym autentyczność takiego „dominującego" poglądu staje się dyskusyjna z chwilą powzięcia pełnej wiedzy o metodyce działania. Rzecz w tym, że postronny użytkownik, a tym bardziej PKW nie posiadają takiej wiedzy ani nie mają technicznych środków weryfikacji sieciowej aktywności interlokutorów. Robert Gorwa ustalił, że podmioty prowadzące tego rodzaju aktywność (podkreślmy: z wykorzystaniem fałszywych, nieistniejących kont użytkowników) z rozmysłem stosują strategię wpływu na „liderów opinii", dziennikarzy, polityków, blogerów, aktywistów[97]. Kandydat lub jego przekaz nie jest więc popierany wprost, lecz popiera się jego zwolennika (zwolenników). Taktyka bezpośredniego wpływu na dyskutowany wątek (wedle oświadczenia samych wykonawców) nie jest stosowana, ponieważ zbyt łatwo narażałaby trolla, bota czy influencera na wykrycie, zaś zleceniodawcy usługi dawałaby możliwość wyparcia się wiedzy o takich metodach[98].

Zapoznawszy się z opisanymi wyżej metodami, trudno się oprzeć wstępnej hipotezie, że tego typu działania dążyły do obejścia zasady przejrzystego prowadzenia kampanii wyborczej, w szczególności zerwania identyfikacji z określonym komitetem wyborczym (zob. art. 109 § 1–2 k. wyb.). Zrealizowanie wymogu oznaczenia materiału wyborczego niweczyłoby cały sens metodyki, która ma wytworzyć iluzję oddolnej, spontanicznej bazy społecznej. Ponadto istotne wątpliwości nasuwa propozycja egzekwowania odpowiedzialności prawnej za zaniechanie obowiązków określonych w art. 109 § 2 k. wyb. w odniesieniu do niektórych przekazów cyfrowych. W szczególności pojęcie utrwalonego przekazu wcale nie jest dostosowane do specyfiki kampanii lub innych form aktywności politycznej w mediach społecznościowych[99]. Czy masowe „polubienia" postów, dzielenie się treścią (np. prawidłowo oznaczonym materiałem wyborczym) przez boty lub człowieka wykorzystującego fałszywe tożsamości, generowanie agresywnej polemiki, treści znieważającej, zniesławiającej interlokutora niechętnego promowanemu kandydatowi lub sposobowi głosowania mieszczą się w pojęciu „nakłaniania lub zachęcania do głosowania w określony sposób"?

5. Aktualna polityka rządu odznacza się bardzo dużym stopniem zaufania wobec sieci społecznościowych, które – co zrozumiałe – preferują indywidualną lub branżową samoregulację. Poza deklaracjami dostawców tych usług – przytaczanymi (i to samo w sobie jest

[97] R. Gorwa, *Unpacking the Ecosystem...*, s. 98.

[98] Tamże.

[99] Spostrzeżenia J. Skrzypczaka sugerują, że było tak już od chwili jego uchwalenia – J. Skrzypczak, *Kampania wyborcza w nowych mediach – aspekty prawne*, „Środkowoeuropejskie Studia Polityczne" 2012, nr 2, s. 54–56. Podobnie M.M. Wiszowaty, *Instytucja ciszy wyborczej – geneza, regulacja prawna, ratio existendi*, „Studia Wyborcze" 2012, nr 14, s. 22, 25.

znamienne) przez przedstawicieli ministra ds. informatyzacji[100] – nie ma jednak namacalnych dowodów na aktywne zwalczanie procederu wykorzystywania botów, fałszywych tożsamości lub rozpowszechniania nieprawdziwych informacji. Władza ustawodawcza w niedostateczny sposób reaguje na proliferację dezinformacji, zaniechawszy przede wszystkim ochrony najbardziej newralgicznego elementu polskiego systemu konstytucyjnego, jakim jest prawo wyborcze. Ten stan rzeczy wymaga natychmiastowej dyskusji oraz interdyscyplinarnych badań nauk prawnych, nauk o bezpieczeństwie i technologii informacyjnych.

dr hab. Michał Bernaczyk, prof. UWr – Katedra Prawa Konstytucyjnego,
Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego,
ORCID: 0000-0001-7683-8852

[100] Zob. zapis z posiedzenia Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu VIII kadencji (nr 116) z dnia 5 grudnia 2018 r. rozpatrującej informację Ministra Cyfryzacji na temat „Zagrożenia wynikające z wykorzystania botów i fake newsów do manipulacji w Internecie (ze szczególnym uwzględnieniem mediów społecznościowych)".