doi 10.26343/0585556X11803 STUDIA SOCJOLOGICZNO-POLITYCZNE. SERIA NOWA
NR 1(18)/2023 ■ ISSN 0585-556X

Robert Pawlita
Uniwersytet Opolski
Wydział Nauk o Polityce i Komunikacji Społecznej[1]
ORCID: 0009-0009-6076-0427

PODEJŚCIE UNII EUROPEJSKIEJ DO DEZINFORMACJI – OD MONITOROWANIA ZJAWISKA DO REGULACJI USŁUG CYFROWYCH

■ WPROWADZENIE

Dezinformację zaczęto traktować jako realne zagrożenie w drugim dziesięcioleciu XXI wieku. W literaturze przedmiotu zjawisko dezinformacji często przytacza się w analizach poświęconych referendum w Wielkiej Brytanii (WB) oraz wyborom prezydenckim w USA w 2016 roku. Znane są również przypadki ingerencji w procesy demokratyczne, jak chociażby w wybory parlamentarne w Niemczech, wybory prezydenckie we Francji oraz w trakcie referendum w Hiszpanii w 2017 roku (Bennett, Livingston 2020: 3 i 4, 10–12). W wymienionych państwach uwidoczniła się wówczas dezinformacyjna aktywność państw trzecich – zorientowana na tworzenie chaosu informacyjnego. Dodatkowo w WB i USA wykorzystano zjawisko *microtargetingu* (Robaczyński 2022: 157–160).

W Europie postrzega się Rosję oraz Białoruś za dominujące podmioty szerzące dezinformację. Rosyjskie działania informacyjne, których celem jest narzucenie swojej narracji, wzmogły się jeszcze przed aneksją Krymu w 2014 roku. W listopadzie 2013 roku rosyjska działalność nasiliła się w momencie, kiedy miało dojść do umowy stowarzyszeniowej między Ukrainą a Unią Europejską (UE) (Kobernjuk, Kasper 2021: 174 i 175). Białoruskie działania zintensyfikowały się m.in. po wyborach prezydenckich w 2020 roku oraz w trakcie polsko-białoruskiego kryzysu granicznego w 2021 roku. Dla obu państw dezinformacja stanowi narzędzie komunikowania strategicznego (Darczewska 2017; Bryjka, Legucka 2021). Obok Rosji i Białorusi jako państwa szerzące dezinformację wymienia się Chiny oraz Iran. Są to państwa, którym zależy na destabilizacji sytuacji w Europie oraz w Stanach Zjednoczonych. Szczególnie obawy mogą budzić Chiny ze względu na potencjał technologiczno-ekonomiczny. Chiny są państwem zamkniętym, jeśli chodzi o wpływy z zewnątrz w infosferze – kontrolują media i podawane w nich treści. Jednocześnie

[1] E-mail: robert.pawlita2a@gmail.com

Państwo Środka korzysta z możliwości otwartej gospodarki światowej i globalizacji. Chińska aktywność widoczna była m.in. w trakcje pandemii COVID-19 oraz po napaści Rosji na Ukrainę (Pamment 2020: 2–4, 10 i 11; Kupiecki, Bryjka, Chłoń 2022: 94–97).

Wybory do Parlamentu Europejskiego (PE) zostały przeprowadzone w dniach 23–26 maja 2019 roku. Przy tego typu wydarzeniach działania informacyjne są zintensyfikowane. Zauważalna jest wzmożona aktywność w mediach społecznościowych. W czasie trwania kampanii wyborczych można zaobserwować tendencję do wzrostu aktywności fałszywych kont, botów w mediach społecznościowych, które rozpowszechniają wprowadzające w błąd informacje (Rosińska 2021: 172–182). Według danych Komisji Europejskiej (KE) z grudnia 2018 roku aż 73% osób korzystających z Internetu w UE obawia się dezinformacji w okresach przedwyborczych. (Komisja Europejska 2018). Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) przestrzega przed dezinformacją i sztuczną inteligencją jako zagrożeniami dla państw członkowskich i Unii. Zdaniem agencji tendencja wykorzystania narzędzi będzie przez najbliższe lata jedynie rosnąć (ENISA 2023).

Celem niniejszego artykułu jest przedstawienie zagrożeń w aspekcie dezinformacji, która może mieć wpływ na procesy wyborcze, relacje wewnątrz państwa, a także organizacje międzynarodowe. Zaprezentowane zostaną przypadki dezinformacji przed wyborami do PE w 2019 roku. Niniejsza analiza zwraca uwagę na aktywność KE pod kątem przeciwdziałania dezinformacji w okresie od marca 2015 roku do lutego 2024 roku.

Postawione zostały 3 pytania badawcze: 1) Jakie są zagrożenia dezinformacji w aspekcie wyborów? 2) Jakie działania podjęła Komisja Europejska w celu zwalczania zjawiska? 3) Jak zmieniło się podejście do dezinformacji na szczeblu UE? Przy tak sformułowanej problematyce badawczej istotna jest próba oceny podjętych działań na szczeblu unijnym w aspekcie przeciwdziałania dezinformacji.

Warstwa metodologiczna pracy opiera się na analizie instytucjonalno-prawnej oraz na metodzie decyzyjnej. Podstawę do analizy stanowią dokumenty unijne, akty prawne oraz raporty Komisji Europejskiej. Z kolei metoda decyzyjna odnosi się do kwestii implementacji środków zwalczających dezinformację. Strukturę wewnętrzną artykułu tworzą trzy główne zagadnienia: pojęcie oraz cechy dezinformacji, dezinformacja jako zagrożenie dla demokracji, działania Unii Europejskiej w aspekcie zwalczania dezinformacji.

POJĘCIE ORAZ CECHY DEZINFORMACJI

Według KE wątpliwe informacje tworzone, publikowane i rozpowszechniane w celu osiągnięcia korzyści politycznych lub ekonomicznych, są czynnikiem zakłócającym debatę publiczną, podważając zaufanie obywateli do instytucji oraz mediów. Dla KE dezinformacja stanowi zjawisko, które zakłóca procesy demokratyczne,

destabilizuje funkcjonowanie państwa oraz polaryzuje społeczeństwo (Komisja Europejska 2018).

Dezinformacja jest jednym ze sposobów manipulacji, której celem jest zmiana w postrzeganiu rzeczywistości wśród odbiorców, co ma wywołać pożądaną zmianę w zachowaniu bądź przy podejmowaniu decyzji (NASK PIB 2023: 3). Dezinformacja nie wynika tylko z rozwoju technologii. Rozprzestrzenianie wątpliwych informacji jest również napędzane czynnikami społeczno-psychologicznymi (Kapantai i in. 2021: 1301, 1304). Dezinformujący przekaz odwołuje się do emocji, takich jak strach, wrogość, niepewność. Charakterystyczne dla dezinformacji jest nadawanie zjawiskom, przedmiotom w komunikacie negatywnych cech (Batorowska, Klepka, Wasiuta 2019: 167). Dezinformacja to nie tylko fałszywe informacje, ale także prawdziwe stwierdzenia, które zostały wyrwane z kontekstu, a ich nadużywanie ma spowodować, iż odbiorcy będą wyciągać sugestywne wnioski (Bendiek, Schulze 2019: 2 i 3). Dezinformacja jest czynnością powtarzającą się, tzn. znamienne jest powtarzanie komunikatów przez ten sam podmiot bądź przez innych (Domalewska 2020: 157). Często do osiągnięcia celów stosuje się takie techniki manipulacyjne, jak: negacja faktów, odwrócenie faktów, pomijanie informacji, modyfikacje okoliczności, nadmiar informacji, uogólnienia, przytoczenie różnych wariacji na ten sam temat (Volkoff 2022: 150–158). W tym miejscu należy już przywołać obiegowe pojęcie *fake news*. *Fake news* definiuje się jako formę, dezinformację zaś jako treść, gdzie fake newsy służą do rozprzestrzeniania się dezinformacji (Ivancik, Mullerova 2022: 119–123). Dla podmiotu, który posługuje się dezinformacją, jest ona korzystna ze względu na szybkość przekazu, liczbę dostępnych kanałów przekazu, możliwość szerokiego powielania. Dezinformacja jest czynnikiem wpływającym na nastroje i świadomość społeczną, który może maskować faktyczne zamiary i działania, w tym tworzyć grunt pod scenariusze planowanych działań (Kupiecki, Bryjka, Chłoń 2022: 24–26, 98 i 99).

DEZINFORMACJA JAKO ZAGROŻENIE DLA DEMOKRACJI

Zagrożenia dezinformacyjne mogą mieć charakter długotrwały. Dotyczy to zarówno przestrzeni informacyjnej, jak tworzących ją podmiotów i obywateli. Wcześniej przywołane Rosja oraz Białoruś powielają wątpliwe treści, usiłując narzucić odbiorcom zmanipulowany obraz rzeczywistości. W szczególności Polska oraz państwa bałtyckie stanowią cele oddziaływań dezinformacyjnych obu wymienionych wyżej państw. Działalność informacyjna Rosji wzmogła się w czasie aneksji Krymu w 2014 roku. Wówczas dezinformację szerzono w sposób systematyczny, skoordynowany i ukierunkowany. Na szeroką skalę wykorzystywano social media i media tradycyjne. Jednym z podnoszonych tematów było krymskie referendum ws. przyłączenia do Rosji. W rosyjskich przekazach manipulowano informacjami dotyczącymi frekwencji oraz skali poparcia mieszkańców Krymu dla przyłączenia

do Federacji Rosyjskiej. Celem Rosji było zdezorientowanie międzynarodowej opinii publicznej i pokazanie zgody mieszkańców do idei zjednoczenia (Zolotukhin 2020: 6–10). Charakterystyczne dla przekazu obu ww. państw jest powtarzalność narracji w mediach, w których opowiada się te same historie, a rozbudowuje jedynie kontekst. Biorąc pod uwagę kwestie historyczne, ideologiczne, ekonomiczne, polityczne, przewiduje się, iż nie ustaną skomasowane oddziaływania, których celem będzie destabilizacja sytuacji wewnątrz państw, funkcjonowania UE i NATO (CAPD 2018; Myhre 2019: 12–16).

Czynnikiem mogącym oddziaływać na opinię publiczną jest wspomniane zjawisko microtargetingu zaobserwowane w czasie wyborów prezydenckich w USA oraz referendum w Wielkiej Brytanii w 2016 roku. *Microtargeting* polega na dotarciu z komunikatem politycznym do określonej grupy społeczeństwa bądź grupy elektoratu, która została wyodrębniona na podstawie cech socjodemograficznych i przy przypisaniu kategorii psychologicznych. Kluczowe w tym aspekcie jest gromadzenie danych nt. preferencji osób w oparciu o metadane (Wojtasik 2022: 255 i 256). Działalność Cambridge Analytica podczas referendum w Wielkiej Brytanii uwidoczniła możliwości wynikające z pozyskiwania i wykorzystywania danych osobowych do microtargetingu. W marcu 2018 roku światło dzienne ujrzała afera niekontrolowanego uzyskiwania danych przez firmę Cambridge Analytica. Ważnym elementem w tej sprawie było oferowanie przez firmę zainteresowanym osobom pieniędzy w zamian za wypełnienie ankiety internetowej, gdzie do dostępu należało pobrać konkretną aplikację, w tym wyrazić zgodę na dostęp do informacji użytkownika. Był to sposób kupna danych na rzecz skutecznych kampanii. Zebrano dane około 50 milionów użytkowników, tworząc bazę wyborców dla Cambridge Analitica. Informacje były wykorzystywane do wpływania na poglądy odbiorców oraz do rozprzestrzeniania dezinformacji (Kulik 2018).

Dwa lata po referendum, w lipcu 2018 roku, brytyjski Komitet ds. Kultury, Mediów i Sportu Izby Gmin opublikował raport pn. „Disinformation and fake news". W raporcie wykazano zaangażowanie Rosji w kampanię przedreferendalną za pośrednictwem mediów społecznościowych poprzez rozpowszechnianie m.in. treści kampanii popierającej Brexit „Vote Leave" i kampanii „Leave.EU" Partii Niepodległości Zjednoczonego Królestwa (Komitet ds. Kultury, Mediów i Sportu Izby Gmin 2018, pkt. 160–163).

W tym samym raporcie podaje się dowody na rosyjską ingerencję w katalońskie referendum w Hiszpanii w 2017 roku (dotyczyło niepodległości Katalonii). Rosyjska kampania dezinformacyjna miała zaostrzyć wewnętrzny konflikt w Hiszpanii, a także przyczynić się do jej dezintegracji z UE i innymi państwami członkowskimi. Wówczas rosyjska dezinformacja odnosiła się do krytyki demokratycznego systemu w Hiszpanii (Komitet ds. Kultury, Mediów i Sportu Izby Gmin 2018, pkt. 193). Równolegle przy referendum partie polityczne aktywnie wykorzystywały propagandę obliczeniową, aby treści dotarły do jak najszerszego grona odbiorców.

Katalońska partia niepodległościowa, Esquerra Republicana de Catalunya, była powiązana z nieautentycznymi kontami na Twitterze. W Hiszpanii w 2019 roku podczas wyborów również zauważalne było użycie propagandy obliczeniowej, kiedy Partido Popular wykorzystało boty do wzmocnienia swoich treści na Twitterze, Facebooku i Instagramie. Partia Podemos wysyłała zaś zautomatyzowane wiadomości do swoich zwolenników za pośrednictwem WhatsApp (DemTech 2020: 362–366).

W 2020 roku Uniwersytet Oksfordzki opublikował raport dotyczący „zindustrializowanej" dezinformacji w 81 państwach na świecie. W 62 z nich wykazano działalność partii politycznych lub rządowych agencji w kreowaniu opinii publicznej, w tym z wykorzystaniem strategii dezinformujących. Wśród wskazanych państw było 12 państw członkowskich UE, w tym Polska. W badanych przypadkach partie polityczne i agencje rządowe posługiwały się platformami internetowymi, mediami społecznościowymi i komunikatorami na rzecz kształtowania postaw społecznych (Wojtasik 2022: 245). W raporcie opisano, iż w Polsce w okresie poprzedzającym wybory do PE w 2019 roku około 21% treści, które polskojęzyczni internauci mogli ujrzeć na Twitterze, miało charakter dezinformujący. Instytut Dialogu Strategicznego w tym okresie zidentyfikował co najmniej 803 fałszywe konta i boty, które były aktywne przed wyborami do PE i rozpowszechniały dezinformację o narracji antysemickiej i prorosyjskiej. Instytut zidentyfikował również sieć grup, stron oraz kont na Facebooku, promujących partię Konfederacja oraz polski rząd, które masowo zamieszczały antysemickie treści skierowane do młodych osób (DemTech 2020: 2–4, 309–313).

Problem rosnących napięć politycznych był zauważalny również w innych państwach członkowskich. W Niemczech eurosceptyczna partia Alternative für Deutschland (AfD), głosząca radykalne poglądy, również rozprzestrzeniała spreparowane treści, często rozprowadzane przez oficjalne kanały mediów społecznościowych tego ugrupowania. Ma to szczególne znaczenie, ponieważ radykalne i antyimigranckie nastroje przenikają do społeczeństwa oraz sprzyjają przestępstwom z nienawiści (DemTech 2020: 145).

Dezinformacja, jak wcześniej wspomniano, wpływa na postawy, poglądy oraz przekonania. Innym obszarem, którego dotyka, jest zdrowie jednostek. Nieprawdziwy obraz rzeczywistości powoduje podejmowanie nieracjonalnych decyzji, wypacza proces analizy. Dezinformacja wpływa na procesy poznawcze. Pod koniec 2019 i w 2020 roku ludzkość zmagała się z pandemią COVID-19. W literaturze okres ten nazywa się mianem *infodemii*, kiedy każdego dnia pojawiały się zmanipulowane treści na temat teorii spiskowych, wirusa, szczepień, i efektów ubocznych itp. Dodatkowo dezinformacyjny przekaz obniżał poziom zaufania do instytucji publicznych. Wśród społeczeństwa zwiększał się niepokój oraz pojawiała się frustracja. Za chaos, za nieład informacyjny, za sytuację w placówkach medycznych obwiniano rządy (Bąkowicz 2023: 133–139).

Wyzwaniem dla demokracji stały się media społecznościowe i ich regulacja prawna. Media społecznościowe, jako źródło i środek przekazu, funkcjonują według własnych polityk czy wewnętrznych regulaminów i posiadają znaczną siłę oddziaływania. Wieloczynnikowy aspekt wyzwania dezinformacji w social mediach obejmuje funkcjonowanie i regulaminy mediów, spektrum narzędzi dezinformacji (w postaci wyodrębnionych grup, wykorzystywanych algorytmów, stosowania kont fikcyjnych i botów), problem zdefiniowania i regulacji prawnych (Rosińska 2021: 212–217).

DZIAŁANIA UNII EUROPEJSKIEJ W ASPEKCIE ZWALCZANIA DEZINFORMACJI

Początek działań przeciwko dezinformacji na szczeblu unijnym sięga marca 2015 roku, kiedy to Rada Europejska wystosowała wezwanie do wspólnego zwalczania trwającej rosyjskiej kampanii dezinformacyjnej. W ramach Europejskiej Służby Działań Zewnętrznych została powołana grupa zadaniowa East StratCom. Grupa zadaniowa składa się z ekspertów z zakresu komunikacji, mediów i dziennikarstwa. W tym samym roku grupa zadaniowa utworzyła projekt EUvsDisinfo. Jednym z celów projektu było przeciwdziałanie i prostowanie rosyjskiej dezinformacji, która nasiliła się w związku z aneksją Krymu. W ramach projektu EUvsDisinfo w okresie od 2015 do 2019 roku zidentyfikowano i skatalogowano 7252 przypadków dezinformacji, poszerzając wiedzę na temat sposobów działania, narzędzi oraz celów tychże działań (Komisja Europejska 2018; euvsdisinfo.eu.pl, 24 lutego 2024). Obecnie w bazie danych projektu zgromadzono ponad 16 600 przypadków, z czego 1500 przypadków dotyczy samej wojny w Ukrainie od 24 lutego 2022 roku. Od daty powstania w bazie skatalogowano 1980 przypadków dezinformacji dotyczących Unii Europejskiej, z czego 212 przypadków stanowi dezinformację w okresie przygotowań do wyborów do PE od stycznia do maja 2019 roku[2] (stan na 24 lutego 2024, euvsdisinfo.eu.pl).

W kwietniu 2018 roku KE opublikowała komunikat dotyczący zwalczania dezinformacji w Internecie. Komunikat był następstwem raportu Grupy Ekspertów tzw. wysokiego szczebla (ang. High-Level Group of Experts – HLEG). Raport HLEG pn. „A multi-dimensional approach to disinformation" przyczynił się do tego, iż KE wytypowała główne obszary, których funkcjonowanie ma znaczenie przy zwalczaniu dezinformacji. W komunikacie podkreślono znaczenie przejrzystego ekosystemu internetowego w kwestii odpornych i bezpiecznych procesów wyborczych. Przy zwalczaniu dezinformacji niezbędne jest wsparcie umiejętności korzystania

[2] Baza dezinformacji EUvsDisinfo umożliwia zweryfikowanie, czy dany przekaz stanowi dezinformację. Podane liczby stanowią ilość przypadków po zastosowaniu filtrów w bazie danych, przy uwzględnieniu ram czasowych oraz tzw. tagów.

z mediów, wsparcie rzetelnego dziennikarstwa, a także zwalczanie zewnętrznych i wewnętrznych zagrożeń poprzez komunikację strategiczną (NASK PIB 2019).

Kolejny ważny krok w kierunku zwalczania dezinformacji poczyniono we wrześniu 2018 roku. Przyjęto wówczas Kodeks postępowania w zakresie zwalczania dezinformacji. Propozycja ta była formą samoregulacji sektora biznesowego, platform internetowych i social mediów. Należy podkreślić, iż platformy, media dobrowolnie mogły przystąpić do Kodeksu, albowiem nie był obowiązującym aktem prawnym. Kodeks został opracowany przez przedstawicieli branży reklamowej, mediów czy platform internetowych, którzy byli wspierani przez środowisko akademickie. W dokumencie kładziono nacisk m.in na identyfikację fałszywych kont, na transparentność sponsorowanych treści, przejrzystość algorytmów i możliwość weryfikacji reklam. Sygnatariuszami Kodeksu zostały takie korporacje, jak Google, Twitter, Facebook, Mozilla (NASK PIB 2019: 7 i 8).

Następnie KE wystosowała, 12 września 2018 roku, komunikat w sprawie wolnych i uczciwych wyborów europejskich. Zaproponowane środki miały przyczynić się do zapewnienia bezpiecznego i uczciwego ich przebiegu. KE rekomendowała zwiększenie przejrzystości reklam politycznych w Internecie, utworzenie krajowych sieci współpracy związanych z wyborami, ochronę systemów informatycznych przed cyberatakami czy stosowanie unijnych przepisów o ochronie danych osobowych. Przypadek zbierania danych osobowych przed referendum w WB był jednym z impulsów do wprowadzenia Rozporządzenia o Ochronie Danych Osobowych (RODO), które ma zastosowanie od 25 maja 2018 roku. Dla UE oraz dla państw członkowskich jest to narzędzie do zwalczania bezprawnego wykorzystywania danych osobowych również w aspekcie wyborów. *Microtargeting* w cyberprzestrzeni byłby wówczas możliwy, gdyby strony internetowe czy media społecznościowe informowały o zamiarze zbierania danych celem profilowania, a dalej idąc internauta musiałby wyrazić na to zgodę (Orędzie o stanie Unii 2018)[3].

Kolejną inicjatywą w walce z dezinformacją było ogłoszenie 5 grudnia 2018 roku Planu działania przeciwko dezinformacji. W planie określono cztery główne obszary działania. Było to: określenie skoordynowanych działań i reakcji instytucji unijnych wraz z państwami członkowskimi przeciwko dezinformacji, poprawienie zdolności instytucji unijnych do ujawniania przypadków dezinformacji tudzież ich analizowanie, włączenie do walki z dezinformacją sektora prywatnego, prowadzenie kampanii społecznych i uświadamianie społeczeństwa na temat szkodliwości dezinformacji (Plan działania przeciwko dezinformacji 2018: 5). Plan zakładał 10 podobszarów działań: 1. Utworzenie grup zadaniowych ds. komunikacji w państwach członkowskich z oddelegowanego unijnego personelu, które miały pomóc w ujawnianiu i analizie działań dezinformacyjnych; 2. Większe wsparcie grup

[3] Zob. pkt. 24, 60, 70, 71 oraz art. 21 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) z 27 kwietnia 2016 roku.

zadaniowych na Bałkanach; 3. Utworzenie systemu szybkiego reagowania (System RAPID) celem przeciwdziałania kampaniom dezinformacyjnym, włączając w to PE, komórki NATO oraz łącząc z systemem szybkiego reagowania grupy G7; 4. Wymianę informacji między państwami członkowskimi i UE odnośnie przypadków dezinformacji; 5. Poprawę komunikacji strategicznej państw członkowskich z państwami poza Unią; 6. Monitorowanie wdrożenia Kodeksu przez sygnatariuszy; 7. Przeprowadzenie akcji informujących społeczeństwa nt. wyborów oraz prowadzenie szkoleń mediów w zakresie dezinformacji, a także wsparcia jednostek naukowych celem poznania zjawiska; 8. Stworzenie multidyscyplinarnych zespołów z niezależnymi osobami weryfikującymi fakty w danym regionie, aby zbadać lokalną charakterystykę zjawiska; 9. Wdrożenie dyrektywy dot. audiowizualnych usług medialnych w aspekcie umiejętności korzystania z mediów; 10. Wdrożenia pakietu wyborczego celem przejrzystości kampanii wyborczych (Plan działania przeciwko dezinformacji 2018: 6, 8, 9, 11).

Po wyborach w czerwcu 2019 roku KE opublikowała Sprawozdanie z realizacji Planu działania przeciwko dezinformacji. W sprawozdaniu z 14 czerwca wskazano działania platform Twitter, Facebook i Google, które odnosiły się do zapobiegania kampanii dezinformacyjnych, w tym działania podjęte wspólnie z władzami krajowymi, dziennikarzami oraz fact-checkerami. W pierwszej połowie 2019 roku ujawniono wiele prób wpływu na wybory i manipulacji debatą publiczną. Platforma Google poinformowała, iż w ramach działań usunęła 3,39 mln kanałów w serwisie YouTube. Facebook zakomunikował, że w okresie pierwszych trzech miesięcy 2019 roku usunął 1574 stron i grup spoza Unii Europejskiej oraz 168 stron i grup mających lokalizację na terenach UE. Usunięcia nastąpiły wskutek aktywności politycznej ingerującej w procesy wyborcze w ramach UE. Serwis Twitter podał liczbę 77 mln usuniętych fałszywych kont.

Tuż przed wyborami do PE platformy we współpracy tudzież zgodnie ze wskazaniami niezależnych dziennikarzy, zidentyfikowały i usunęły konta rozpowszechniające dezinformację. Zgłoszonych zostało blisko 600 stron i grup na platformie Facebook, które funkcjonowały w Polsce, Niemczech, Francji, Hiszpanii i we Włoszech[4]. W tych przypadkach dotyczyło to manipulacji zachowaniem wyborców. Wskazuje się, iż poziom zaangażowania platform w zwalczanie dezinformacji był różny, niejasności pojawiały się wokół przejrzystości reklam politycznych i ich źródeł finansowania. Podczas gdy platforma Facebook rozszerzyła transparentność

[4] We Włoszech, Hiszpanii, Niemczech, Francji i Polsce wykazano wysoką aktywność dezinformacyjną. Są to państwa członkowskie UE, które mogły wprowadzić do PE ponad połowę eurodeputowanych (razem 362 z 705 – po wyjściu WB z UE) w 2019 roku. W wyborach w 2024 roku liczba posłów do PE zwiększy się do 720. Francja, Hiszpania, Holandia otrzymają po dwa dodatkowe miejsca, podczas gdy Austria, Dania, Belgia, Polska, Finlandia, Słowacja, Irlandia, Słowenia i Łotwa otrzymają po jednym (Parlament Europejski 2024).

polityki reklam, podobnych rozwiązań nie wprowadziły Twitter i Google (Sprawozdanie Komisji Europejskiej… 2019: 1, 5 i 6).

We wrześniu 2020 roku KE przedstawiła dokument pn. „Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement", który dotyczył oceny wdrożenia i skuteczności Kodeksu (Zegarow 2020). KE oceniła pozytywnie funkcjonowanie Kodeksu przez pierwsze 12 miesięcy, mimo pewnych niespójności. Kodeks przyczynił się do ograniczenia umieszczania reklam rozpowszechniających dezinformację w Internecie, zwiększenia transparentności reklam politycznych przez ich oznaczenie i stworzenie możliwości wyszukiwania wraz z udostępnieniem repozytoriów reklam, a także ograniczenia wykorzystania technik manipulacyjnych poprzez usługi platform internetowych. Elementy, które wymagały poprawy w Kodeksie, według Komisji to: ograniczenie dostępu do gromadzonych przez platformy danych, które umożliwiłyby ocenę trendów, brak jednoznacznych procedur i określonych zobowiązań sygnatariuszy (albowiem każda firma i platforma miała pod tym względem dowolność działań w celu ograniczenia dezinformacji), brak wskaźników skuteczności z działań platform internetowych (podawane przez platformy liczby usuniętych kont czy grup nie jest samym wyznacznikiem), konieczność współpracy między środowiskiem akademickim a platformami (współpraca przez 12 miesięcy funkcjonowania nie istniała) (Assessment of the Code of Practice on Disinformation 2020: 19, 21 i 22).

Działania Unii Europejskiej w aspekcie zwalczania dezinformacji przed wyborami do Parlamentu Europejskiego 2019 roku były pierwszymi tak zmasowanymi działaniami osłonowymi. Ówczesny wysiłek Unii, państw członkowskich i platform internetowych był zadowalający, albowiem udało się ograniczyć dezinformację pochodzącą z zewnątrz, a kampania i głosowanie przebiegły bez większych zakłóceń (Mierzyńska 2019).

Z drugiej strony pojawiały się głosy stanowiące, iż działalność przeciwko dezinformacji na szczeblu unijnym należy rozszerzyć. Działania z 2019 roku poddano dalszym kontrolom, w wyniku których stwierdzono, iż należy usprawnić monitorowanie i rozliczalność platform internetowych, poprawić rozliczalność działań unijnych przeciwko dezinformacji, zacieśnić współpracę między państwami członkowskimi oraz powiązanymi grupami zadaniowymi (Europejski Trybunał Obrachunkowy 2021: 4–6). W kontrolach zwracano również uwagę na to, iż brakuje harmonijnych rozwiązań odnośnie dezinformacji i wyznaczonych norm prawnych dotyczących platform internetowych (Mazur, Chochia 2022: 32–34) Sygnatariusze Kodeksu mogli stosować się do punktów według uznania, a platformy mogły raportować te dane, które uznały za słuszne. Brakowało m.in. mechanizmu monitorowania i możliwości udostępnienia informacji dla ośrodków badawczych (Kobernjuk, Kasper 2021: 183–186).

Po majowych wyborach w 2019 roku nowo wybrana KE ogłosiła konkurs ofert utworzenia Europejskiego Obserwatorium Mediów Cyfrowych (EDMO). Spośród

zgłoszeń do prowadzenia EDMO wybrano Europejski Instytut Uniwersytecki we Florencji. Do zadań EDMO należy m.in. wspieranie organów władz publicznych w monitorowaniu polityk platform internetowych, tworzenie huba wymiany informacji dla mediów, organizacji fact-checkingowych i ośrodków badawczych. Koordynowane przez EDMO projekty ukierunkowane są na identyfikację dezinformacji, jej źródła i zniwelowanie wpływu. Rozpoczynające działalność w czerwcu 2020 roku EDMO było jednym z założeń Planu KE przeciwko dezinformacji z 2018 roku (edmo.eu).

Sytuacja z pandemią COVID-19 pokazała, iż państwa oraz UE zmagają się nie tylko z zagrożeniem wirusa, a także z zagrożeniem dezinformacji. Wówczas KE postanowiła, iż należy prowadzić działania na rzecz udoskonalenia Kodeksu oraz w zakresie rozwiązań prawnych o usługach cyfrowych. Zaprosiła też kolejnych sygnatariuszy do współpracy. Przystąpiły do niej łącznie 34 firmy. W 2021 roku KE w uzgodnieniu z sygnatariuszami wyznaczyła nowe ramy Kodeksu, które zakładały zwiększenie przejrzystości reklam politycznych, demonetyzację dezinformacji, tj. ograniczenie korzyści z reklam politycznych dla platform, zwiększenie roli naukowców i społeczności weryfikującej fakty. Prace nad rozwiązaniami trwały do czerwca 2022 roku. Efektem prac był udoskonalony Kodeks postępowania w zakresie zwalczania dezinformacji oraz akt o rynkach cyfrowych (Digital Markets Act – DMA), a także akt o usługach cyfrowych (Digital Service Act – DSA), które weszły w życie kolejno w 2023 i w 2024 roku (Zegarow 2022; digital-strategy.ec.europa.eu/.

DSA oraz DMA stanowią pakiet legislacyjny dla ochrony praw podstawowych oraz stworzenia uczciwego rynku w przestrzeni cyfrowej dla przedsiębiorstw. DMA normuje rynki cyfrowe, na których działają platformy, nakładając na nie określone obowiązki techniczne. DSA koncentruje się natomiast na obowiązkach sprawozdawczych platform z działalności, odpowiedzialności za decyzje moderowania i usuwania treści oraz na przejrzystości dla użytkowników. Choć w aktach nie ma zdefiniowanych pojęć takich jak dezinformacja czy nielegalne treści, to przepisy odsyłają do właściwych aktów w państwach członkowskich oraz innych przepisów UE. Przepisy DSA mają charakter asymetryczny względem platform internetowych, tj. nakłada się dodatkowe zobowiązania na duże platformy (tzw. VLOP), które liczą co najmniej 45 mln użytkowników obywateli z państw UE[5]. Jednymi z zobowiązań platform są: obowiązek oceny ryzyka, przeprowadzanie corocznych audytów i kontroli algorytmów oraz zakaz profilowania osób niepełnoletnich. DSA ustanawia także możliwość nadzoru nad tekstami dla wyeliminowania treści wprowadzających w błąd. Wprowadza w tym celu mechanizm zgłaszania treści. Szczególną formą mechanizmu zgłaszania treści są zaufane podmioty sygnalizujące.

[5] Zob. DSA: art. 6 (Hosting), art. 9 (Nakaz podjęcia działań przeciwko nielegalnym treściom), art. 15 (Obowiązki sprawozdawcze w zakresie przejrzystości spoczywające na dostawcach usług pośrednich), art. 16 (Mechanizmy zgłaszania i działania). W artykule przywołano jedynie część z katalogu rozwiązań, które zostały zawarte w DSA.

O status zaufanego podmiotu sygnalizującego może ubiegać się podmiot, który jest niezależny od dostawców platform internetowych, posiada szczególną wiedzę ekspercką z danej dziedziny oraz dysponuje kompetencjami do wykrywania niewłaściwych treści. Wniosek o status zaufanego podmiotu rozpatruje koordynator ds. usług cyfrowych w danym państwie członkowskim. Zgłoszenia zaufanych podmiotów winny być traktowane priorytetowo przez platformy internetowe. Jednakże pojawiają się obawy, iż może dochodzić do nadużywania mechanizmu zgłaszania, a przepisy są zbyt prewencyjne, tzn. treści mogą zostać usunięte zapobiegawczo bez głębszej analizy (Leiser 2023: 4–11).

2015

Marzec 2015 r. – Wezwanie wystosowane przez Radę Europejską do podjęcia działań w związku z rosyjską dezinformacją. Powołanie grupy zadaniowej East StratCom przy ESDZ. Utworzenie projektu EUvsDisinfo.

Kwiecień 2016 r. – Przyjęcie przez KE wspólnych ram dotyczących przeciwdziałaniu zagrożeniom hybrydowym. Utworzenie Komórki Unii Europejskiej ds. Syntezy informacji o Zagrożeniach Hybrydowych.

Styczeń–marzec 2018 r. – Powołanie Grupy Ekspertów Wysokiego Szczebla (HLEG) jako organu doradczego KE w sprawie inicjatyw mających na celu przeciwdziałanie rozprzestrzennianiu się fake newsów i dezinformacji. Pracę grupy kończy raport wydany w dniu 12 marca 2018 r.

Kwiecień 2018 r. – Komunikat KE w sprawie zwalczania dezinformacji w Internecie. W komunikacie zwrócono uwagę na środowisko internetowe, które winno być przejrzyste, godne zaufania i odpowiedzialne. Zaproponowano m.in. kodeks postępowania samoregulacyjnego w zakresie dezinformacji.

Maj 2018 r. – Do życia wchodzi Ogólne Rozporządzenie o Ochronie Danych (RODO), określające przepisy dot. przetwarzania, ochrony i przepływu danych osobowych. Prace nad RODO trwały do kwietnia 2016 r.

Wrzesień 2018 r. – Przyjęcie Kodeksu postępowania w zakresie zwalczania dezinformacji. Wystosowanie Komunikatu przez KE w sprawie wolnych i uczciwych wyborów do Parlamentu Europejskiego.

Grudzień 2018 r. – Ogłoszenie Planu działania przeciwko dezinformacji, w którym określono 10 podobszarów działań.

Czerwiec 2019 r. – Opublikowanie Sprawozdania z realizacji planu działania przeciwko dezinformacji.

Czerwiec 2020 r. – Powstanie Europejskiego Obserwatorium Mediów Cyfrowych.

Wrzesień 2020 r. – Przedstawienie przez KE dokumentu pn. Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement, który dotyczył oceny wdrożenia i skuteczności Kodeksu.

Maj 2021 r. – czerwiec 2022 r. – Prace nad udoskonalonym Kodeksem postępowania w zakresie zwalczania dezinformacji. Do Kodeksu przystąpiło 34 sygnatariuszy. W 2019 r. do Kodeksu przystąpiło 6 sygnatariuszy.

Luty 2023 r. – Wydanie przez ESDZ raportu na temat zagrożeń związanych z zagraniczną manipulacją i ingerencją informacyjną (FIMI). W raporcie ukazano analizę stu przypadków dezinformacji w okresie październik–grudzień 2022.

Grudzień 2023 r. – Porozumienie Parlamentu Europejskiego z Radą dot. aktu ws. sztucznej inteligencji (AI Act). Propozycję regulacji sztucznej inteligencji wysunęła KE w kwietniu 2021 r.

Luty 2024 r. – Wejściew życie Aktu o usługach cyfrowych. DSA nakłada na dostawców usług szereg zobowiązań, m.in. cykliczne sprawozdania z działalności, audyty algorytmów, umożliwienie zgłaszania nieprawidłowych treści dla użytkowników, współpracę z podmiotami zaufania publicznego.

2024

Rycina 1. Unijne inicjatywy na rzecz walki z dezinformacją
Źródło: Opracowanie własne na podstawie: Leiser 2023; NASK PIB 2019; euvsdisinfo.eu; edmo.eu.

W aspekcie regulacji prawnych należy również wspomnieć o akcie ws. sztucznej inteligencji (AI). W kwietniu 2021 roku KE zaproponowała wprowadzenie unijnych ram legislacyjnych dotyczących AI. W grudniu 2023 roku osiągnięto zaś wstępne porozumienie w Radzie oraz w PE. Projekt rozporządzenia zakłada m.in. konieczność poinformowania, iż obrazy, dźwięki, treści wideo zostały wygenerowane przy pomocy systemu sztucznej inteligencji. Oznaczanie AI przy wygenerowanych treściach ma ostrzegać użytkowników, ażeby niesłusznie nie uznawali treści za autentyczne, np. *deepfake*[6] (europarl.europa.eu).

ZAKOŃCZENIE

Podjęte kroki, mające na celu zwalczanie dezinformacji na szczeblu unijnym w latach 2015–2019, okazały się słuszne. Zaimplementowane w 2018 roku RODO oraz zaproponowany przez KE Plan działania przeciwko dezinformacji oraz Kodeks postępowania w zakresie zwalczania dezinformacji stanowiły narzędzia ograniczające dezinformację w sieci. Wówczas firmy takie jak Google, Twitter, Facebook, Mozilla podjęły współpracę z KE. Należy podkreślić, iż Kodeks nosił miano samoregulującego, tzn. platformy i social media dobrowolnie do niego przystępowały. Współpracujące korporacje same wyznaczały, w jakim stopniu przyczynią się do walki z dezinformacją bez odgórnych ram działania, o ile to nie zostało wcześniej uregulowane prawnie w państwie członkowskim. Media w różnym stopniu przyczyniały się do ograniczenia dezinformacji. Wątpliwa okazała się również ich współpraca z ośrodkami naukowymi i analitykami w zakresie badania trendów.

Sama KE po tych wydarzeniach nie kryła, iż należy zacieśnić współpracę między podmiotami oraz doprecyzować regulacje. W okresie 2020–2024 zauważalna była zmiana w podejściu do problemu dezinformacji. Kluczowe w tym aspekcie okazały się prace nad udoskonalonym Kodeksem oraz nad unormowaniem usług cyfrowych. Zdano sobie sprawę, iż monitorowanie zjawiska i współpraca nie są wystarczające do zmniejszenia zjawiska rozprzestrzeniania się wątpliwych treści. DSA obliguje platformy do nadzorowania algorytmów oraz cyklicznych sprawozdań, a także umożliwia użytkownikom oraz zaufanym podmiotom weryfikację treści. Do tego prace nad AIA przybliżają perspektywę kontroli nad treściami generowanymi przez sztuczną inteligencję.

[6] Zob. art. 52 Rozporządzenia Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (AIA).

LITERATURA PRZYWOŁANA

Albrycht Izabela, Felici Faustine (red.) (2021), Raport *Europa wobec dezinformacji – budowa odporności systemowej w wybranych krajach*, Kraków: Wydawnictwo Instytutu Kościuszki.

Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement (2020), Komisja Europejska, https://cyberpolicy.nask.pl/wp-content/uploads/2020/09/Assessment-of-the-Code-of-Practice-on-Disinformation.pdf (dostęp 30.04.2023).

Batorowska Hanna, Klepka Rafał, Wasiuta Olga (2019), *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Kraków: LIBRON.

Bąkowicz Katarzyna (2023), *Dezinformacja. Instrukcja obsługi*, Warszawa: CeDeWu.

Bendiek Annegret, Schulze Matthias (2019), *Desinformation und die Wahlen zum Europäischen Parlament,* Berlin*:* Stiftung Wissenschaft und Politik, doi: 10.18449/2019A10.

Bennett W. Lance, Livingston Steven (2020), *Information Wars and the Decline of Institutional Authority*, w: W. Lance Bennett, Steven Livingston (red.), *The Disinformation Age. Politics, Technology, and Disruptive Communication in the United States*, New York: Cambridge University Press, s. 3–40, https://doi.org/10.1017/9781108914628.

Bryjka Filip, Legucka Agnieszka (2021), *Dezinformacja i propaganda Rosji oraz Białorusi w kontekście polsko-białoruskiego kryzysu granicznego*, https://www.pism.pl/publikacje/dezinformacja-i-propaganda-rosji-oraz-bialorusi-w-kontekscie-polsko-bialoruskiego-kryzysu-granicznego (dostęp 24.02.2024).

CAPD (2018), *Nowe zagrożenia informacyjne dla Polski nie muszą pochodzić z zewnątrz*, https://capd.pl/pl/komentarze/201-komentarz-nowe-zagrozenia-informacyjne-dla-polski-nie-musza-pochodzic-z-zewnatrz (dostęp 22.01.2023).

Darczewska Jolanta (2017), *Dezinformacja – rosyjska broń strategiczna*, https://archiwum.rcb.gov.pl/dezinformacja-rosyjska-bron-strategiczna/ (dostęp 22.12.2023).

DemTech (2020), Raport *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*, Oksford: Uniwersytet Oksfordzki, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/03/Case-Studies_FINAL.pdf (dostęp 28.04.2023).

Domalewska Dorota (2020), *Wielowymiarowość komunikacji w kontekście bezpieczeństwa. Komunikacja w sytuacjach kryzysowych i komunikacja strategiczna*, Warszawa: Akademia Sztuki Wojennej.

ENISA (2023), *Foresight 2030 Threats*, https://www.enisa.europa.eu/publications/foresight-2030-threats (dostęp 25.02.2024).

Europejski Trybunał Obrachunkowy (2021), *Dezinformacja w UE – pomimo podejmowanych wysiłków problem pozostaje nierozwiązany*, Bruksela: Urząd Publikacji Unii Europejskiej.

EUvsDISINFO (2024), *Baza dezinformacji*, https://euvsdisinfo.eu/pl/disinformation-cases-pl/?date=23.01.2022%20-%2023.01.2024&disinfo_keywords[]=keyword_77110&numberposts=50&_=1706020452143 (dostęp 24.02.2024).

Ivancik Radoslav, Mullerova Jana (2022), *Disinformation, propaganda and fake news as non-military security threats for contemporary modern human society*, „Security Dimensions", no. 40, s. 116–132, DOI:10.5604/01.3001.0015.8158.

Kapantai Eleni, Christopoulou Androniki, Berberdis Christos, Peristeras Vassilios (2021), A *systematic literature review on disonformation: Toward a unfieled taxonomical framework*, „New Media & Society", vol. 23 (5), s. 1301–1326, https://doi.org/10.1177/1461444820959296.

Kobernjuk Anna, Kasper Agnes (2021), *Normativity in the EU's Approach towards Disinformation*, „TalTech Journal of European Studies", vol. 11, no. 1 (33), doi:10.2478/bjes-2021-0011.

Komitet ds. Kultury, Mediów i Sportu Izby Gmin (2018), *Disinformation and fake news*., https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm#_idTextAnchor033 (dostęp 24.04.2023).

Komisja Europejska (2018), *Zestawienie dotyczące dezinformacji*, https://ec.europa.eu/commission/presscorner/detail/pl/MEMO_18_6648 (dostęp 6.03.2023).

Kulik Wojciech (2018), *Afera Facebook i Cambridge Analytica*, https://www.benchmark.pl/aktualnosci/afera-facebook-i-cambridge-analytica-o-co-chodzi.html (dostęp 2.02.2023).

Kupiecki Robert, Bryjka Filip, Chłoń Tomasz (2022), D*ezinformacja międzynarodowa: pojęcie, rozpoznanie, przeciwdziałanie*, Warszawa: Wydawnictwo Naukowe Scholar.

Leiser Mark (2023), *Reimagining Digital Governance: The EU's Digital Service Act and the Fight Against Disinformation*, Social Science Research Network, https://dx.doi.org/10.2139/ssrn.4427493.

Mazur Viktoria, Chochia Archil (2022), *Definition and Regulation as an Effective Measure to Fight Fake News in the European Union*, European Studies – the Review of European law, „Economics and Politics", vol. 9, nr 1, s. 16–40.

Mierzyńska Anna (2019), *Miliardy fake'owych kont, boty na polskich portalach. Analiza kampanii do PE w sieci*, https://oko.press/miliardy-fakeowych-kont-i-boty-na-polskich-portalach-analiza-kampanii-do-pe-w-sieci (dostęp 2.05.2023).

Myhre Eric (2019), *Supranational or Compartmental: Applying the Question of European Union Identity to the Topic of Disinformation*, JMU Scholary Commons, Harrisonburg: James Madison University.

NASK PIB (2019), Raport *Zjawisko dezinformacji w dobie rewolucji cyfrowej*, https://cyberpolicy.nask.pl/raport-zjawisko-dezinformacji-w-dobie-rewolucji-cyfrowej-panstwo-spoleczenstwo-polityka-biznes/, (dostęp 25.01.2023).

NASK PIB (2023), *Bezpieczne wybory – raport otwarcia*, https://bezpiecznewybory.pl/baza-wiedzy/bezpieczne-wybory-raport-otwarcia (dostęp 27.12.2023).

Orędzie o stanie Unii 2018*,* https://ec.europa.eu/commission/presscorner/detail/pl/IP_18_5681 (dostęp: 24.04.2023).

Pamment James (2020), Raport *The EU's Role in Fighting Disinformation: Taking Back the Initiative. Future Threats, Future Solutions #1*, Washington: Carnegie Endowment for International Peace, https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf (dostęp 24.02.2024).

Plan działania przeciwko dezinformacji z 5 grudnia 2018 r., Komisja Europejska, https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf (dostęp 24.04.2023).

Robaczyński Jakub (2022), *Rola mikrotargetingu w komunikacji marketingowej w polityce oraz innych branżach*, Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne, Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego, 39, s. 147–164, https://doi.org/10.19195/1733-5779.39.9.

Rosińska Klaudia (2021), *Fake news: geneza, istota, przeciwdziałanie*, Warszawa: Wydawnictwo Naukowe PWN.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych).

Sprawozdanie Komisji Europejskiej z realizacji Planu Działania Przeciwko Dezinformacji (2019), https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52019JC0012&from=ES (dostęp 7.02.2023).

Ustawa z 1 września 2017 r. Netzwerkdurchsetzungsgesetz (NetzDG), https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html (dostęp 4.05.2023).

Volkoff Vladimir (2022), *Krótka historia dezinformacji. Od konia trojańskiego do internetu*, tłum. Marian Miszalski, Warszawa: Wektory.

Wojtasik Waldemar (2022), *Manipulacje wyborcze*, Katowice: Wydawnictwo NOA.
Zegarow Paweł (2020), *Ocena unijnego Kodeksu postępowania w zakresie zwalczania dezinformacji*, https://cyberpolicy.nask.pl/ocena-unijnego-kodeksu-postepowania-w-zakresie-zwalczania-dezinformacji/ (dostęp 30.04.2023).
Zegarow Paweł (2022), *Nowy Kodeks postępowania w zakresie zwalczania dezinformacji*, https://cyberpolicy.nask.pl/nowy-kodeks-postepowania-w-zakresie-zwalczania-dezinformacji/ (dostęp 26.02.2024).
Zolotukhin Dymytro (2020), *Biała Księga specjalnych operacji informacyjnych wobec Ukrainy w latach 2014–2018*, w: W. Baluk (red.), *Rosyjska propaganda wobec Polski i Ukrainy*, Lublin: Uniwersytet Marii Curie-Skłodowskiej.
https://www.europarl.europa.eu/news/en/press-room/20200130IPR71407/redistribution-of-seats-in-the-european-parliament-after-brexit, 31 stycznia 2020 (dostęp 30.04.2023).
https://www.europarl.europa.eu/topics/pl/article/20230601STO93804/akt-ws-sztucznej-inteligencji-pierwsze-przepisy-regulujace-ai (dostęp 1.03.2024).
https://digital-strategy.ec.europa.eu/pl/policies/code-practice-disinformation (dostęp 26.02.2024).
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206 (dostęp 1.03.2024).

Robert Pawlita

THE EUROPEAN UNION'S APPROACH TO DISINFORMATION – FROM MONITORING THE PHENOMENON TO REGULATING DIGITAL SERVICES

The following article provides an overview of the risks of disinformation in the context of the 2019 European Parliament elections. The aim of the article was to identify possible solutions to combat disinformation online. At the European Union level, it was realised that disinformation had been present on a larger scale since 2014, so steps were already taken in 2015 to counter it. From 2015 to 2019, tools to fight it were developed like the General Data Protection Regulation, the Code of Practice on Disinformation and the Action Plan against Disinformation. According to experts, the 2019 EP elections went without major incidents and the effect of the adopted regulations was satisfactory, despite inaccuracies in the transparency of advertisements and scant cooperation between online platforms and research centres. However, the EU and the work did not stop there. The EU authorities began to analyse the existing tools, as well as analysing further cases of emerging disinformation. After 2019, the approach of the EU authorities has changed. It was necessary to find out a certain legal framework that would define fake news, disinformation and the activities of online platforms. Briefly, the EU's actions can be characterised: from alerting, over cooperation with the media, researchers and fact-checkers, to the definition of legal acts for digital services. Work on disinformation has intensified. It is likely that further work on normalising the phenomenon will follow in the coming years.

Słowa kluczowe: dezinformacja; ataki informacyjne; zagrożenia; przeciwdziałanie; Unia Europejska

Keywords: disinformation; information attacks; threaths; counteratacking; European Union