Zuzanna Jordan[1]

https://doi.org/10.29316/9788368103359_11

PRAWO A DEZINFORMACJA – ANALIZA REGULACJI DOTYCZĄCYCH BEZPIECZEŃSTWA INFORMACYJNEGO W POLSCE I UE

LAW AND MISINFORMATION – AN ANALYSIS OF INFORMATION SECURITY REGULATIONS IN POLAND AND THE EU

Streszczenie

Dezinformacja stanowi jedno z kluczowych wyzwań dla współczesnych systemów bezpieczeństwa i porządku publicznego. W dobie dynamicznego rozwoju mediów społecznościowych oraz globalnego obiegu informacji, jej skutki wykraczają daleko poza sferę komunikacji, wpływając na stabilność instytucji demokratycznych, procesy wyborcze, oraz bezpieczeństwo narodowe. Rozdział przedstawia analizę regulacji prawnych dotyczących przeciwdziałania dezinformacji w Polsce oraz w Unii Europejskiej, ze szczególnym uwzględnieniem regulacji takich jak Digital Services Act, strategii UE dotyczących bezpieczeństwa informacyjnego oraz krajowych przepisów prawa. Celem rozdziału jest ocena skuteczności obowiązujących rozwiązań prawnych w kontekście zagrożeń bezpieczeństwa informacyjnego. Przeprowadzono

[1] https://orcid.org/0009-0009-2636-8501, email: zuzanna.jordan@protonmail.com

analizę aktów prawnych, literatury przedmiotu oraz strategii instytucjonalnych. Wskazano zarówno mocne strony istniejących regulacji (np. zwiększenie odpowiedzialności platform internetowych), jak i ich ograniczenia (np. brak precyzyjnych definicji i mechanizmów egzekucyjnych). Wnioski wskazują na potrzebę dalszego rozwoju ram prawnych oraz bliższej współpracy między państwami członkowskimi i sektorem prywatnym w celu skutecznego przeciwdziałania dezinformacji.

Słowa kluczowe: dezinformacja, bezpieczeństwo informacyjne, prawo, Digital Services Act, regulacje medialne

Abstract

Disinformation represents one of the key challenges to contemporary security systems and public order. In the era of rapid social media development and global information circulation, its effects extend far beyond communication, influencing the stability of democratic institutions, electoral processes, national security, and social cohesion. This chapter analyses legal regulations addressing disinformation in Poland and the European Union, with a particular focus on the Digital Services Act, EU information security strategies, and national regulations. The aim of the chapter is to assess the effectiveness of the existing legal framework in countering information security threats. Legal acts, relevant literature, and institutional strategies are analysed. The paper identifies both the strengths of the current regulations (e.g., increased accountability of online platforms) and their limitations (e.g., lack of precise definitions and enforcement mechanisms). The conclusions highlight the need for further development of legal frameworks and closer cooperation between EU Member States and the private sector to effectively counter disinformation.

Keywords: disinformation, information security, law, Digital Services Act, media regulation

Wstęp

Zjawisko dezinformacji w ostatnich latach stało się jednym z najpoważniejszych zagrożeń dla bezpieczeństwa informacyjnego zarówno w Polsce, jak i w całej Unii Europejskiej. Informacje rozchodzą się dziś szybciej niż kiedykolwiek wcześniej. Media społecznościowe, komunikatory, różnego rodzaju platformy internetowe umożliwiają błyskawiczne dotarcie z treściami do milionów odbiorców. Niestety, ten sam mechanizm jest

wykorzystywany do szerzenia fałszywych informacji, manipulowania opinią publiczną, czy wpływania na decyzje społeczne i polityczne. Dezinformacja przestała być wyłącznie problemem komunikacyjnym – obecnie stanowi realne zagrożenie dla stabilności instytucji demokratycznych, procesów wyborczych oraz bezpieczeństwa narodowego.

Unia Europejska i poszczególne państwa członkowskie zaczęły podejmować konkretne działania mające na celu przeciwdziałanie temu zjawisku. W ostatnich latach przyjęto m.in. Digital Services Act, który wprowadza nowe obowiązki dla dużych platform internetowych, mające ograniczyć skalę szkodliwych treści i zwiększyć ich odpowiedzialność. Oprócz tego pojawiły się różnego rodzaju strategie bezpieczeństwa informacyjnego na poziomie unijnym i krajowym. W Polsce działania te są prowadzone zarówno w ramach obowiązujących regulacji medialnych, jak i poprzez inicjatywy instytucjonalne, np. NASK czy Rządowe Centrum Bezpieczeństwa. Mimo tych wysiłków wiele problemów pozostaje nierozwiązanych. Wciąż brakuje precyzyjnych definicji pojęć związanych z dezinformacją, skutecznych mechanizmów egzekwowania prawa, a także odpowiedniego balansu między ochroną bezpieczeństwa a poszanowaniem wolności słowa.

Celem niniejszego rozdziału jest analiza obowiązujących regulacji prawnych dotyczących przeciwdziałania dezinformacji w Polsce oraz w Unii Europejskiej, a także ocena ich skuteczności w kontekście zagrożeń bezpieczeństwa informacyjnego. W opracowaniu zostaną omówione główne akty prawne i strategie, przedstawione ich mocne i słabe strony, a także zarysowane wyzwania oraz możliwe kierunki dalszych działań. Tekst opiera się na analizie aktów prawnych, dokumentów strategicznych, literatury naukowej oraz dostępnych raportów instytucjonalnych.

Kontekst prawny i strategiczny UE

Unia Europejska już od kilku lat uznaje dezinformację za realne zagrożenie dla bezpieczeństwa, stabilności politycznej i funkcjonowania demokratycznych instytucji. Szczególnie wyraźnie było to widać po 2016 roku, kiedy to różne kampanie dezinformacyjne zaczęły wpływać na wybory, referenda i debatę publiczną w wielu państwach członkowskich. W odpowiedzi UE rozpoczęła tworzenie ram prawnych oraz mechanizmów koordynacyjnych,

które mają przeciwdziałać rozprzestrzenianiu fałszywych treści i wzmacniać odporność społeczeństwa na manipulacje informacyjne.

Jednym z najważniejszych elementów tych działań jest Digital Services Act (DSA) – akt prawny, który zaczął obowiązywać w 2024 roku i stanowi kompleksową regulację dotyczącą funkcjonowania platform internetowych. DSA nie odnosi się wprost do pojęcia „dezinformacji", ale wprowadza szereg obowiązków, które mają pośrednio ograniczyć jej skalę i wpływ. Duże platformy (tzw. VLOP-y – very large online platforms), takie jak Facebook, YouTube czy X, muszą prowadzić regularne oceny ryzyka związanego z rozpowszechnianiem nielegalnych i szkodliwych treści. Są też zobowiązane do wdrażania skutecznych środków zaradczych, w tym m.in. mechanizmów moderacji, większej przejrzystości algorytmów oraz udostępniania danych niezależnym badaczom. W założeniu ma to zwiększyć odpowiedzialność platform i umożliwić skuteczniejsze reagowanie na kampanie dezinformacyjne (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065).

Kolejnym ważnym dokumentem jest Europejski Plan Działań na rzecz Demokracji (EDAP), przyjęty w 2020 roku. Plan ten zakłada m.in. wzmocnienie regulacji dotyczących reklamy politycznej w sieci, poprawę przejrzystości finansowania kampanii, a także rozwój niezależnych mediów i wsparcie dla organizacji fact-checkingowych (European Commission, 2020). W ramach EDAP duży nacisk położono na zwiększenie odporności społeczeństwa poprzez edukację medialną oraz promowanie krytycznego myślenia. Nie chodzi tylko o walkę z fałszywymi treściami „po fakcie", ale o budowanie długofalowej odporności obywateli na manipulację.

UE powołała również szereg struktur instytucjonalnych, które mają wspierać państwa członkowskie w reagowaniu na zagrożenia informacyjne. Ważną rolę odgrywa tu East StratCom Task Force, działająca w ramach Europejskiej Służby Działań Zewnętrznych (EEAS), która zajmuje się m.in. identyfikowaniem i analizowaniem kampanii dezinformacyjnych, głównie pochodzących z Rosji (European External Action Service, East StratCom Task Force, b.d.). Istotne znaczenie mają też tzw. Rapid Alert System – system szybkiego ostrzegania, który umożliwia wymianę informacji między instytucjami unijnymi i państwami członkowskimi w czasie rzeczywistym (European Commission, b.d.). Ma on pomóc w szybkim reagowaniu na zorganizowane kampanie dezinformacyjne, np. w okresach wyborczych czy podczas kryzysów.

W ostatnich latach UE zaczęła również kłaść większy nacisk na współpracę z sektorem prywatnym. Platformy internetowe są zobowiązane do uczestniczenia w Kodeksie postępowania w zakresie dezinformacji, który choć formalnie ma charakter dobrowolny, w praktyce stał się ważnym narzędziem nacisku regulacyjnego. Kodeks został zaktualizowany w 2022 roku, rozszerzając zakres obowiązków dotyczących przejrzystości reklam, walki z fałszywymi kontami i botami oraz wzmacniania współpracy z organizacjami fact-checkingowymi.

Podsumowując, działania Unii Europejskiej w zakresie przeciwdziałania dezinformacji opierają się na trzech głównych filarach: regulacji platform internetowych, strategiach wzmacniania odporności społecznej oraz koordynacji instytucjonalnej i międzypaństwowej. Choć DSA i powiązane inicjatywy stanowią znaczący krok naprzód, wyzwaniem pozostaje skuteczna egzekucja tych przepisów w praktyce oraz zapewnienie spójności działań między różnymi państwami członkowskimi.

Regulacje krajowe w Polsce

W Polsce nie funkcjonuje jeden kompleksowy akt prawny odnoszący się wprost do zjawiska dezinformacji. Regulacje w tym zakresie są rozproszone i zawarte w różnych aktach prawnych oraz dokumentach strategicznych, obejmujących zarówno sferę mediów, jak i bezpieczeństwa narodowego oraz działalności administracji publicznej. W praktyce przeciwdziałanie dezinformacji odbywa się w sposób pośredni – poprzez regulacje dotyczące rzetelności przekazu medialnego, odpowiedzialności nadawców, ochrony porządku publicznego czy zapewnienia bezpieczeństwa informacyjnego państwa.

Podstawowym aktem prawnym regulującym działalność tradycyjnych mediów w Polsce jest ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji. Nakłada ona na nadawców obowiązek zachowania rzetelności i obiektywizmu, przestrzegania zasady pluralizmu politycznego i społecznego oraz odpowiedzialności za treści przekazywane odbiorcom (Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji). Choć ustawa nie zawiera bezpośrednich przepisów dotyczących dezinformacji, stanowi podstawę do reagowania w przypadkach rozpowszechniania materiałów sprzecznych z prawem lub niezgodnych z zasadami etyki dziennikarskiej. Ważną rolę w tym kontekście

odgrywa Krajowa Rada Radiofonii i Telewizji (KRRiT), która ma uprawnienia nadzorcze i może nakładać sankcje na nadawców łamiących przepisy.

Dla mediów internetowych i prasy elektronicznej istotne znaczenie mają przepisy Prawa prasowego z 1984 r., wielokrotnie nowelizowane (Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe). Określają one m.in. obowiązki redaktorów naczelnych i wydawców w zakresie odpowiedzialności za publikowane treści oraz konieczność zachowania rzetelności dziennikarskiej. Choć prawo prasowe powstało w czasach przedcyfrowych, nadal stanowi punkt odniesienia przy ocenie odpowiedzialności za fałszywe lub wprowadzające w błąd informacje publikowane online.

W ostatnich latach coraz większe znaczenie w kontekście bezpieczeństwa informacyjnego mają również działania instytucjonalne i strategiczne. Ważną rolę odgrywa tu Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK), który prowadzi m.in. zespół CERT Polska zajmujący się reagowaniem na incydenty w cyberprzestrzeni oraz monitoringiem kampanii dezinformacyjnych (NASK – Państwowy Instytut Badawczy, 2022). NASK realizuje także programy edukacyjne i analityczne dotyczące rozpoznawania fałszywych treści, a jego raporty często służą administracji publicznej jako źródło wiedzy o zagrożeniach informacyjnych.

Istotnym elementem krajowego systemu przeciwdziałania dezinformacji są działania Rządowego Centrum Bezpieczeństwa (RCB), które prowadzi monitoring przestrzeni informacyjnej pod kątem pojawiających się narracji dezinformacyjnych, zwłaszcza w okresach kryzysowych (Rządowe Centrum Bezpieczeństwa, 2023). Współpracuje ono z innymi instytucjami państwowymi, służbami oraz mediami w celu szybkiego dementowania fałszywych informacji i ostrzegania społeczeństwa przed zagrożeniami.

Ważnym dokumentem strategicznym jest również Strategia Bezpieczeństwa Narodowego RP z 2020 roku, która wskazuje zagrożenia informacyjne jako istotny element współczesnych wyzwań dla bezpieczeństwa państwa. Strategia podkreśla konieczność wzmacniania odporności społeczeństwa na manipulacje informacyjne, rozwijania kompetencji medialnych oraz prowadzenia działań edukacyjnych i informacyjnych na poziomie centralnym i lokalnym (BBN, 2020).

Podsumowując, regulacje krajowe w Polsce w zakresie przeciwdziałania dezinformacji mają charakter pośredni i rozproszony. Opierają się głównie na istniejących przepisach medialnych, instrumentach nadzorczych oraz

działaniach strategicznych instytucji państwowych. Brakuje jednak jednolitych ram prawnych dedykowanych stricte temu zjawisku, co może utrudniać spójną i skuteczną reakcję na skoordynowane kampanie dezinformacyjne.

Analiza skuteczności regulacji

Ocena skuteczności obowiązujących regulacji prawnych dotyczących przeciwdziałania dezinformacji nie jest prosta. Zarówno w Unii Europejskiej, jak i w Polsce mamy do czynienia z rozbudowanym zestawem instrumentów prawnych, strategicznych i instytucjonalnych. Jednak to, w jakim stopniu te rozwiązania faktycznie przekładają się na ograniczanie szkodliwych treści i wzmocnienie odporności społeczeństwa, budzi sporo wątpliwości. Analiza doświadczeń z ostatnich lat, zwłaszcza w okresach kryzysowych, pozwala wskazać zarówno pozytywne efekty regulacji, jak i ich istotne ograniczenia.

Jednym z największych osiągnięć na poziomie unijnym jest zwiększenie odpowiedzialności dużych platform internetowych. Dzięki Digital Services Act wprowadzono m.in. obowiązek oceny ryzyka i podejmowania działań ograniczających rozprzestrzenianie treści nielegalnych i szkodliwych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065). W praktyce oznacza to, że platformy muszą współpracować z niezależnymi badaczami i instytucjami w celu identyfikowania zagrożeń informacyjnych. Widać to szczególnie po uruchomieniu pierwszych rocznych raportów transparentności – wiele firm zaczęło ujawniać dane dotyczące moderacji treści i stosowanych algorytmów. Choć to krok w dobrym kierunku, mechanizmy egzekucji przepisów wciąż są ograniczone. Komisja Europejska dopiero zaczyna nakładać pierwsze kary finansowe na podmioty łamiące regulacje DSA, a skuteczność tych działań będzie można ocenić dopiero w dłuższej perspektywie (European Commission, 2024).

Na poziomie krajowym działania regulacyjne są znacznie bardziej fragmentaryczne. W polskim porządku prawnym brak jednego kompleksowego aktu odnoszącego się wprost do zjawiska dezinformacji, a przeciwdziałanie jej odbywa się pośrednio poprzez różne regulacje dotyczące mediów, usług pośrednich i bezpieczeństwa informacyjnego. Jednocześnie doświadczenia unijne pokazują, że rozbieżne przepisy krajowe dotyczące dezinformacji online i innych zagrożeń społecznych utrudniają harmonizację oraz budowę spójnego systemu reagowania, co było jedną z przesłanek

przyjęcia Aktu o usługach cyfrowych (Dziedzic, 2024, s. 229-230). Warto przy tym podkreślić, że na gruncie polskich przepisów prawnych brak legalnej definicji dezinformacji (Dziedzic, 2024, s. 228).

Pandemia COVID-19 była jednym z pierwszych momentów, w których skuteczność regulacji została wystawiona na poważną próbę. W 2020 i 2021 roku w sieci pojawiła się ogromna liczba fałszywych treści dotyczących wirusa, szczepień, działań rządu i instytucji międzynarodowych. UE uruchomiła wówczas szereg działań w ramach systemu szybkiego ostrzegania oraz kampanii edukacyjnych, a Komisja Europejska prowadziła dialog z platformami w ramach Kodeksu postępowania w zakresie dezinformacji (European Commission, b.d.). Mimo tych działań, fałszywe informacje rozprzestrzeniały się szybciej niż rzetelne komunikaty. W Polsce wiele narracji dezinformacyjnych dotarło do milionów użytkowników w bardzo krótkim czasie. Widać było brak skutecznych mechanizmów szybkiego demaskowania i ograniczania zasięgu takich treści.

Podobna sytuacja miała miejsce po rozpoczęciu pełnoskalowej agresji Rosji na Ukrainę w lutym 2022 roku. Dezinformacja stała się wówczas jednym z głównych elementów działań hybrydowych, obok cyberataków i presji migracyjnej (European External Action Service, East StratCom Task Force, b.d.). UE uruchomiła m.in. system szybkiego ostrzegania oraz zintensyfikowała działania East StratCom Task Force. W Polsce zaobserwowano wzmożoną aktywność rosyjskich i prorosyjskich narracji, dotyczących m.in. rzekomego zagrożenia dla Polski, „ukrytej mobilizacji" czy deprecjonowania pomocy udzielonej uchodźcom. Choć instytucje państwowe, w tym RCB i NASK, starały się reagować, często były to działania spóźnione lub nie miały odpowiedniego zasięgu. Brakowało jednolitej strategii komunikacyjnej i skoordynowanej reakcji między różnymi podmiotami (NASK, 2022).

Warto też zauważyć, że skuteczność regulacji nie zależy wyłącznie od ich treści, ale także od poziomu edukacji medialnej społeczeństwa i zaufania obywateli do instytucji publicznych. Nawet najlepiej skonstruowane przepisy nie będą działały efektywnie, jeśli odbiorcy nie będą w stanie krytycznie oceniać treści lub nie będą wierzyć w oficjalne komunikaty. W tym zakresie zarówno UE, jak i Polska mają jeszcze sporo do zrobienia. Programy edukacyjne i informacyjne są potrzebne, jednak ich skuteczność zależy od lepszej koordynacji działań, stałych szkoleń oraz wsparcia instytucjonalnego i eksperckiego, zwłaszcza na poziomie lokalnym (Dwojnych, 2025, s. 33-34, 43).

Podsumowując, obecne regulacje prawne stanowią istotny krok naprzód w walce z dezinformacją, ale ich skuteczność jest ograniczona przez brak spójności, trudności w egzekwowaniu przepisów, opóźnienia w reagowaniu oraz niedostateczne działania edukacyjne. Przyszłe reformy powinny skupić się nie tylko na doprecyzowaniu przepisów i wzmocnieniu nadzoru nad platformami, ale także na budowaniu długofalowej odporności społecznej na fałszywe treści.

Wyzwania i rekomendacje

Choć w ostatnich latach zarówno Unia Europejska, jak i Polska podjęły istotne działania w zakresie regulacji przeciwdziałania dezinformacji, wciąż istnieje szereg wyzwań, które ograniczają skuteczność tych rozwiązań. Wyzwania te mają charakter zarówno systemowy, jak i operacyjny. Ich przezwyciężenie wymaga nie tylko zmian prawnych, ale także lepszej koordynacji działań instytucjonalnych oraz inwestycji w edukację i świadomość społeczną.

Pierwszym wyzwaniem jest niespójność i rozproszenie regulacji prawnych. Na poziomie unijnym DSA tworzy stosunkowo jednolite ramy dla dużych platform, ale nie obejmuje wszystkich aspektów walki z dezinformacją, a wiele szczegółów pozostaje w gestii państw członkowskich (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065). W Polsce natomiast brak jest jednego aktu prawnego poświęconego temu zjawisku – regulacje są rozsiane po różnych ustawach i dokumentach strategicznych. Taki stan rzeczy utrudnia stworzenie spójnego i przewidywalnego systemu przeciwdziałania dezinformacji.

Drugim wyzwaniem jest egzekwowanie przepisów w praktyce. Wiele obowiązków nałożonych na platformy w ramach DSA ma charakter ogólny i wymaga doprecyzowania w praktyce stosowania prawa. Komisja Europejska dopiero zaczyna realnie korzystać z uprawnień do nakładania sankcji finansowych, a krajowe organy nadzorcze nie zawsze dysponują odpowiednimi zasobami i kompetencjami, by skutecznie kontrolować przestrzeganie przepisów (European Commission, 2024). W Polsce dodatkowym problemem jest ograniczona jurysdykcja wobec zagranicznych podmiotów i brak szybkich mechanizmów reagowania na kampanie prowadzone z zewnątrz.

Kolejnym istotnym wyzwaniem jest koordynacja działań między różnymi podmiotami. Przeciwdziałanie dezinformacji wymaga współpracy wielu aktorów: instytucji państwowych, sektora prywatnego, organizacji pozarządowych, mediów i środowiska naukowego. W praktyce jednak działania te są często rozproszone i realizowane w sposób nieskoordynowany. Brakuje wyraźnie wyznaczonego centrum odpowiedzialnego za koordynację strategii informacyjnej państwa oraz szybką wymianę informacji między instytucjami (NASK, 2023). Efektem jest powielanie działań, brak spójnych komunikatów oraz trudności w budowaniu jednolitego przekazu wobec społeczeństwa.

Nie można też pominąć czynnika społecznego. Nawet najlepiej skonstruowane przepisy nie będą skuteczne, jeśli obywatele nie będą potrafili krytycznie ocenić ich treści. Poziom edukacji medialnej w Polsce wciąż pozostaje nierówny. W szkołach temat ten pojawia się głównie w formie doraźnych projektów lub fakultatywnych zajęć, a nie jako spójny element programu nauczania (Dwojnych, 2025, s. 33-34, 43). Brakuje też szeroko zakrojonych kampanii społecznych, które w przystępny sposób uczyłyby rozpoznawania fałszywych informacji, np. poprzez porównywanie źródeł, analizę języka emocjonalnego czy rozpoznawanie schematów narracyjnych wykorzystywanych w kampaniach dezinformacyjnych.

Na podstawie powyższych wyzwań można sformułować kilka kluczowych rekomendacji: tworzenie spójnych ram prawnych na poziomie krajowym, np. w formie odrębnej ustawy lub kompleksowej nowelizacji istniejących przepisów, która jasno określiłaby obowiązki instytucji, mechanizmy reagowania oraz współpracy w zakresie bezpieczeństwa informacyjnego. Wzmocnienie egzekucji przepisów DSA i stworzenie krajowego organu nadzorczego z realnymi kompetencjami oraz zapleczem technicznym. Taka instytucja mogłaby współpracować bezpośrednio z Komisją Europejską oraz platformami cyfrowymi. Wyznaczenie krajowego centrum koordynacji działań informacyjnych, które odpowiadałoby za monitoring, analizę i szybką reakcję na kampanie dezinformacyjne, łącząc działania NASK, RCB, służb, mediów publicznych i organizacji pozarządowych. Wzmocnienie edukacji medialnej poprzez wprowadzenie jej jako stałego elementu programu szkolnego oraz realizację ogólnokrajowych kampanii społecznych skierowanych do różnych grup wiekowych.

Podsumowując, przeciwdziałanie dezinformacji wymaga podejścia systemowego. Nie wystarczy samo zaostrzenie przepisów – potrzebne są skuteczne mechanizmy ich egzekwowania, lepsza współpraca instytucjonalna i szerokie działania edukacyjne. Dopiero połączenie tych elementów może realnie zwiększyć odporność społeczeństwa na fałszywe treści.

Podsumowanie

Dezinformacja stała się jednym z kluczowych wyzwań bezpieczeństwa informacyjnego współczesnych państw. Zarówno Unia Europejska, jak i Polska podejmują coraz bardziej zaawansowane działania regulacyjne i instytucjonalne, mające na celu ograniczenie wpływu fałszywych treści na społeczeństwo i system polityczny. W ostatnich latach widać istotny postęp – przede wszystkim dzięki przyjęciu Digital Services Act oraz rozwojowi strategii informacyjnych na poziomie europejskim i krajowym. Powstały także struktury analityczne i mechanizmy wymiany informacji, takie jak East StratCom Task Force czy Rapid Alert System, które wzmacniają zdolność do szybszego reagowania na zagrożenia.

Jednocześnie skuteczność tych rozwiązań pozostaje ograniczona. W praktyce regulacje są często trudne do egzekwowania, działania instytucji są rozproszone, a poziom edukacji medialnej w społeczeństwie nadal nie gwarantuje wysokiej odporności na manipulacje informacyjne. Doświadczenia pandemii COVID-19 i wojny w Ukrainie pokazały, że dezinformacja rozprzestrzenia się szybciej niż systemy państwowe i unijne są w stanie reagować.

Dlatego przeciwdziałanie temu zjawisku wymaga podejścia systemowego i wielowarstwowego. Potrzebne są nie tylko doprecyzowane i spójne ramy prawne, ale także silniejsze instytucje nadzorcze, lepsza koordynacja działań międzysektorowych oraz inwestycje w edukację i świadomość społeczną. Tylko takie połączenie może realnie zwiększyć odporność informacyjną i zmniejszyć wpływ wrogich narracji na społeczeństwo.

Literatura

1. BBN. (2020). *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. Warszawa.
2. Dwojnych, A. (2025). *Przeciwdziałanie dezinformacji w przestrzeni Polski lokalnej – rekomendacje rozwiązań*. Warszawa: Sieć Badawcza Łukasiewicz.
3. Dziedzic, M. (2024). Przeciwdziałanie dezinformacji w kontekście wybranych regulacji Aktu o usługach cyfrowych oraz Aktu o sztucznej inteligencji. *Prawo i Więź*, 6(53), 223-238. https://doi.org/10.36128/PRIW.VI53.1103
4. European Commission. (2020). *European Democracy Action Plan*.
5. European Commission. (2020). *Fighting COVID-19 disinformation*.
6. European Commission. (2024). *First DSA enforcement actions*.
7. European Commission. (b.d.). *Rapid Alert System against disinformation*. Pobrano z: https://commission.europa.eu/strategy-and-policy/policies/media-and-digital/regulation-disinformation/rapid-alert-system_en (dostęp: 01.02.2026).
8. European External Action Service. (b.d.). *East StratCom Task Force*. Pobrano z: https://euvsdisinfo.eu (dostęp: 01.02.2026).
9. NASK – Państwowy Instytut Badawczy. (2022). *Raport o dezinformacji dotyczącej wojny w Ukrainie*.
10. NASK – Państwowy Instytut Badawczy. (2022). *Raport z działalności CERT Polska*.
11. NASK. (2023). *Raport o wyzwaniach w zakresie bezpieczeństwa informacyjnego*.
12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (Digital Services Act), Dz.U. UE L 277 z 27.10.2022.
13. Rządowe Centrum Bezpieczeństwa. (2023). *Raport o zagrożeniach informacyjnych*.
14. Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe, Dz.U. 1984 nr 5, poz. 24 z późn. zm.
15. Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji, Dz.U. 1993 nr 7, poz. 34 z późn. zm.