Rekomendacja Rady ds. Cyfryzacji w sprawie walki z dezinformacją jako zagrożeniem cyberbezpieczeństwa Państwa z 14 kwietnia 2022 r.

Internet stał się miejscem tworzenia własnych przestrzeni informacyjnych, będąc jednocześnie nową formą mediów i nową sferą publiczną, która nie zna granic terytorialnych, językowych czy narodowych. Ten wymiar często niekontrolowanej ekspansji przestrzeni medialnej wymaga nowego podejścia regulacyjnego w zakresie metod i technik związanych z zapewnianiem bezpieczeństwa w cyberprzestrzeni. Kampanie dezinformacyjne prowadzone na masową skalę przy wykorzystaniu mediów społecznościowych w celu kontrolowania dyskursu politycznego lub radykalizowania postaw, rekrutacji „grup-przykrywek" i kierowania nimi mogą być nośnikiem zagrożeń hybrydowych. W warunkach dynamicznego rozwoju sytuacji międzynarodowej, w tym nasilających się działań hybrydowych, bardzo trudne, a w praktyce wręcz niemożliwe, jest odróżnienie przez zwykłych obywateli działań aktorów publicznych (ekspertów, doradców, czy naukowców komentujących dane zagrożenie) od celowych działań inspirowanych przez obce służby specjalne, organizacje terrorystyczne czy wrogo nastawione państwa, oraz zapobieżenie tym działaniom i ich skutkom przez instytucje państwa.

W Deklaracji Brukselskiej z 2018 r. szefowie państw i rządów sojuszniczych przyznali, że stoją w obliczu "wyzwań hybrydowych, w tym kampanii dezinformacyjnych i złośliwych działań cybernetycznych", a w Deklaracji Londyńskiej z 2019 r. zobowiązali się do wzmocnienia "zdolności NATO do przygotowania się, powstrzymywania i obrony przed taktykami hybrydowymi, które dążą do podważenia bezpieczeństwa NATO i społeczeństw". Nowe podejście do przeciwdziałania dezinformacji ma dwa cele: z jednej strony kluczowe staje się „rozumienie" nowego środowiska informacyjnego (analiza informacji, narracji, sentymentów, atrybucja), z drugiej strony istotne staje się dostarczanie informacji opartych na faktach (komunikacja strategiczna) oraz demaskowanie dezinformacji.

Z kolei zgodnie z komunikatem Komisji do Parlamentu Europejskiego, Rady Europejskiej i Rady *Dziewiętnaste sprawozdanie z postępu prac na rzecz skutecznej i rzeczywistej Unii Bezpieczeństwa COM/2019/353 final,* ochrona procesów i instytucji demokratycznych przed dezinformacją stanowi główne wyzwanie dla społeczeństw na całym świecie. Aby sprostać temu wyzwaniu, niezbędne jest **wprowadzenie solidnych ram skoordynowanych działań przeciwko dezinformacji, przy pełnym poszanowaniu wartości i praw podstawowych**. Dwie główne kategorie, które uznano wtedy za mogące wyrządzić szkodę społeczeństwu, to celowa dezinformacja mająca na celu wywarcie wpływu na wybory oraz politykę imigracyjną. Zaraz za nimi uplasowały się dezinformacja w dziedzinie zdrowia, środowiska i polityki bezpieczeństwa. Wydarzenia ostatnich dni, pozwalają jednak z całą pewnością stwierdzić, że dezinformacja jest **bronią,** narzędziem w rękach autorytarnych

krajów, wykorzystywanym do realizacji ich strategicznych geopolitycznych celów, towarzyszącym działaniom wojennym, których skutki widzimy teraz w Ukrainie.

Wyróżnić można cztery elementy działań w walce z dezinformacją:

(1) gromadzenie większej wiedzy o taktykach stosowanych w manipulacji informacją;
(2) budowanie świadomości;
(3) rozwijanie umiejętności korzystania z mediów na wszystkich poziomach
(4) stosowanie sankcji[1].

Jednocześnie należy podkreślić, że system polskiego prawa karnego nie jest przystosowany do ścigania tego typu działań z uwagi na niedostateczne zawężenie konstrukcji przestępstwa dezinformacji. Pomijając fakt, że definicja dezinformacji w prawie karnym została sprowadzona do wprowadzania w błąd polskich organów państwowych, to nadal należy ją wiązać ze świadczeniem usług wywiadowczych na rzecz Rzeczypospolitej Polskiej (dezinformacja wywiadowcza). Element *actus reus* przestępstwa dezinformacji, opisany w art. 132 kodeksu karnego w żaden sposób nie uwzględnia intencjonalnego wpływu mediów na opinię publiczną i władzę publiczną.

Głównym wyzwaniem w obszarze bezpieczeństwa środowiska informacyjnego jest uzyskanie syntetycznej **diagnozy potrzeb regulacyjnych w sferze bezpieczeństwa mediów cyfrowych**, uwzględniającej zarazem odmienność i różnorodność w polskim, europejskim i międzynarodowym porządku prawnym. Wprowadzenie przepisów prawnych definiujących działania dezinformacyjne i ustalających sankcję w warunkach szczególnie istotnych dla zachowania demokracji i suwerenności Państwa, to podstawowy element przyszłych regulacji. Nowe regulacje powinny mieć charakter jak najbardziej uniwersalny i ukierunkowany na cel, a także być technologicznie neutralne z uwagi na dynamiczne zmiany związane z innowacyjnością w sferze technologii mających wpływ na kształt środowiska informacyjnego (np. prawdopodobny rozwój *metaversum*).

Nowe rozwiązania regulacyjne odnoszą się przede wszystkim do:

- zakresu i zasad działania administracji publicznej w obszarze mediów cyfrowych,
- wzorca zadań wynikających z polskiego porządku prawnego i prawa międzynarodowego,
- prawno-administracyjnych podstaw odpowiedzialności za działania dezinformacyjne,
- prawno-administracyjnych podstaw w zakresie dochodzenia wzajemnych roszczeń – jurysdykcja.

[1] J. Kalenský, Rosyjskie ataki dezinformacyjne na wybory: Lessons from Europe, Testimony to the Foreign Affairs Subcomm. on Europe, Eurasia, Energy, and the Environment, US House of Representatives, July 16, 2019.

Mniej radykalnym sposobem kontroli rozprzestrzeniania się dezinformacji jest regulacja prasy, mediów cyfrowych oraz środowiska cyfrowego, które w ramach platform internetowych są głównymi wektorami manipulacji informacją. Działania takie służą na ogół wzmocnieniu uprawnień organów regulujących środowisko cyfrowe.

Przykładem działań organizacyjnych jest łączenie rozproszonych kompetencji poprzez tworzenie grup eksperckich. Większość krajów europejskich posiada obecnie podobne jednostki organizacyjne. Istnieją także rozwiązania polegające na **powołaniu nowej jednostki**, ponieważ przeciwdziałanie dezinformacji i jej wpływom zewnętrznym ma z natury charakter międzyresortowy. Zorganizowane działania powinny obejmować, poza działaniami regulacyjnymi i organizacyjnymi, także aspekt edukacyjny, z wykorzystaniem kampanii informacyjnych dotyczących sposobów weryfikowania źródeł informacji oraz rozpoznawania przekazów dezinformacyjnych.

Z uwagi na aktualne napięcie geopolityczne i towarzyszące temu działania dezinformacyjne prowadzone przez Federację Rosyjską, w tym propagandę, operacje wpływu oraz operacje psychologiczne, pilne wydaje się wdrożenie w Polsce zwłaszcza skutecznych działań organizacyjnych, regulacyjnych, edukacyjnych i finansowych pomagających zapobiec zagrożeniom w sferze informacyjnej.

Mogą mieć one charakter doraźny, jak i długoterminowy, prowadzący do zmian systemowych. Proponowana lista działań:

1. Zainicjowanie „okrągłego stołu" przedstawicieli rządu, biznesu, trzeciego sektora, środowisk akademickich i mediów. Celem mogłoby być przede wszystkim stworzenie programów ramowych walki z dezinformacją,
2. Opracowanie strategicznych programów finansowania badań nad dezinformacją i monitorowania sieci,
3. Zainicjowanie kampanii społecznej, obecnej w telewizji i prasie, która przedstawiałaby imigrantów z sąsiednich krajów postsowieckich jako kulturowo bliskich, pracowitych, dobrze asymilujących się, o ciekawej kulturze, zwyczajach, historii, kuchni, sztuce, etc.
4. Stworzenie profesjonalnych szkoleń z zakresu walki z zagrożeniami hybrydowymi, komunikacji strategicznej, operacji informacyjnych i psychologicznych. W ograniczonym zakresie takie szkolenia istnieją, ale są zarezerwowane dla urzędników lub żołnierzy,
5. Rozszerzenie programu edukacji publicznej w obszarze rozwoju kompetencji medialnych, krytycznego myślenia, Internetu i niebezpieczeństw w sieci,
6. Pilne sfinansowanie nowoczesnych narzędzi analitycznych do monitorowania cyberprzestrzeni, które będą oparte na big data, wyposażone w analizę sentymentu, analizę audiowizualną, umożliwiającą wieloplatformowe i

wielojęzykowe badania. Narzędzie powinno być udostępnione jako open source lub na szerokiej licencji dla badaczy.

Wprowadzenie przepisów prawnych definiujących działania dezinformacyjne i ustalających sankcję w warunkach szczególnie istotnych dla zachowania demokracji i suwerenności państwa jest kluczem do podjęcia ustaleń co do kompetencji i zadań właściwych organów zwalczających dezinformację i prowadzących komunikację strategiczną państwa. Diagnoza, regulacje i określenie kompetencji organów publicznych w cyfrowej przestrzeni informacyjnej to kroki niezbędne w zapewnieniu cyberbezpieczeństwa Państwa Polskiego.