

Oświadczenie Rady do Spraw Cyfryzacji w sprawie dezinformacji i bezpieczeństwa polskiej przestrzeni informacyjnej.

Rada do Spraw Cyfryzacji z rosnącym niepokojem obserwuje skalę dezinformacji rozpowszechnianej w polskiej przestrzeni cyfrowej oraz coraz bardziej zaawansowane metody jej tworzenia i dystrybucji. Zjawisko to stanowi dziś nie tylko zagrożenie dla indywidualnych użytkowników internetu, lecz także dla jakości debaty publicznej, zaufania społecznego, procesów demokratycznych oraz bezpieczeństwa i odporności państwa.

Szczególne zaniepokojenie Rady budzi wykorzystywanie platform społecznościowych do rozpowszechniania fałszywych lub zmanipulowanych treści, podszywania się pod osoby i instytucje oraz prowadzenia oszustw z wykorzystaniem wizerunku osób publicznych. Rozwój generatywnej sztucznej inteligencji, w tym technik deepfake, znacząco zwiększa skalę i wiarygodność takich działań, umożliwiając masowe i niskokosztowe tworzenie fałszywych materiałów tekstowych, graficznych, głosowych i audiowizualnych¹. Ofiarami tego rodzaju działań są zarówno osoby, których wizerunek lub tożsamość zostały bezprawnie wykorzystane, jak i obywatele wprowadzani w błąd przez pozornie wiarygodne komunikaty. Konsekwencją mogą być straty finansowe, kradzież danych i tożsamości, naruszenie reputacji oraz utrata poczucia bezpieczeństwa w środowisku cyfrowym.

Problem ten ma jednak wymiar znacznie szerszy niż indywidualne przypadki oszustw. Dezinformacja może być wykorzystywana do systematycznego osłabiania zaufania do instytucji państwa, mediów, nauki i procesów demokratycznych, pogłębiania istniejących podziałów społecznych oraz wywoływania poczucia chaosu, zagrożenia i bezradności. Jej skutki należy zatem rozpatrywać również w kategoriach odporności państwa i społeczeństwa.

Rada ds. Cyfryzacji zwraca uwagę na **działania prowadzone lub inspirowane przez podmioty zagraniczne, w tym aktorów państwowych i powiązane z nimi sieci wpływu, których celem może być ingerowanie w polską debatę publiczną, polaryzowanie społeczeństwa, podważanie wiarygodności instytucji państwa oraz wpływanie na postawy obywateli i procesy decyzyjne w Polsce.** Polska, ze względu na swoje położenie geopolityczne, rolę na wschodniej flance NATO oraz jednoznaczne zaangażowanie we wsparcie Ukrainy, pozostaje szczególnie narażona na tego rodzaju działania. **Dezinformacja wymierzona w Polskę nie powinna być traktowana wyłącznie jako problem komunikacyjny lub problem treści publikowanych w internecie. W określonych przypadkach stanowi ona element szerszych działań hybrydowych wymierzonych w odporność państwa.**

Jednocześnie Rada ds. Cyfryzacji podkreśla, że przeciwdziałanie dezinformacji musi odbywać się z **pełnym poszanowaniem wolności słowa, pluralizmu debaty publicznej i prawa**

¹ [Stanowisko Rady do Spraw Cyfryzacji w sprawie optymalizacji zwalczania cyberprzestępczości ukierunkowanej na osiągnięcie korzyści finansowych przez sprawców](#)

obywateli do wyrażania poglądów, także krytycznych wobec władz i instytucji publicznych.

Zwalczanie dezinformacji nie może prowadzić do utożsamiania nieprawdziwych lub celowo zmanipulowanych treści z legalną debatą, opinią czy sporem politycznym.

Odpowiedzialność platform społecznościowych

Rada podkreśla szczególną odpowiedzialność największych platform społecznościowych za bezpieczeństwo środowiska informacyjnego, które tworzą i z którego czerpią korzyści gospodarcze. Problemem nie jest wyłącznie obecność nieprawdziwych treści, ale również mechanizmy ich dystrybucji i amplifikacji. Systemy rekomendacyjne, reklama targetowana, fałszywe konta, skoordynowane sieci oraz mechanizmy premiujące treści wywołujące silne emocje mogą powodować, że materiały fałszywe, manipulacyjne lub skrajnie polaryzujące osiągają bardzo duże zasięgi w niezwykle krótkim czasie.

Rada ds. Cyfryzacji oczekuje od platform społecznościowych **skutecznego wykonywania obowiązków wynikających z Aktu o usługach cyfrowych (DSA), w szczególności w zakresie oceny i ograniczania ryzyk systemowych, transparentności systemów rekomendacyjnych i reklamowych oraz zapewnienia skutecznych i dostępnych mechanizmów zgłaszania nielegalnych treści.** Platformy powinny reagować nie tylko na pojedyncze materiały, lecz również identyfikować i ograniczać skoordynowane działania wykorzystujące ich infrastrukturę do oszustw, manipulacji informacyjnej i zagranicznych operacji wpływu.

Rady ds. Cyfryzacji uważa, że skala i dynamika obecnych zagrożeń wymagają od platform społecznościowych działań wykraczających poza reaktywne usuwanie pojedynczych treści, w szczególności:

1. **skuteczniejszego przeciwdziałania oszukańczym reklamom oraz materiałom wykorzystującym bez zgody wizerunek, głos lub tożsamość innych osób,** w tym treściom typu deepfake. Platformy powinny zapewnić efektywne mechanizmy weryfikacji reklamodawców oraz umożliwić osobom, których tożsamość została wykorzystana, skorzystanie z szybkiej ścieżki zgłoszenia i reakcji;
2. **szybkiego wykrywania i ograniczania skoordynowanych kampanii dezinformacyjnych,** w szczególności prowadzonych przy wykorzystaniu sieci fałszywych lub nieautentycznych kont, automatyzacji, sztucznej inteligencji oraz innych metod sztucznego zwiększania zasięgu treści. Reakcja nie powinna ograniczać się do usuwania pojedynczych materiałów, jeśli istnieją przesłanki wskazujące na szerszą, skoordynowaną operację;
3. **większej przejrzystości mechanizmów rekomendacyjnych i reklamowych oraz działań podejmowanych przez platformy wobec dezinformacji.** Dotyczy to w szczególności informacji o sposobach ograniczania ryzyk systemowych, skali wykrywanych skoordynowanych kampanii, źródłach finansowania reklam oraz kryteriach, według których treści są rekomendowane i osiągają zwiększone zasięgi.

Rada stoi na stanowisku, że podmioty, które projektują systemy rekomendacyjne i reklamowe oraz czerpią korzyści ekonomiczne z rozpowszechniania treści, nie mogą pozostawać neutralne wobec przewidywalnych i powtarzalnych nadużyć tych systemów.

Odpowiedzialność platform społecznościowych powinna obejmować nie tylko reagowanie na skutki, lecz także projektowanie usług w sposób ograniczający ryzyko ich wykorzystania do oszustw, manipulacji i skoordynowanych kampanii dezinformacyjnych.

Potrzeba systemowego podejścia państwa

Rada ds. Cyfryzacji uważa, że zapewnienie bezpieczeństwa polskiej przestrzeni informacyjnej wymaga skoordynowanego działania państwa, sektora prywatnego, środowiska naukowego, mediów i organizacji społecznych.

W szczególności Rada rekomenduje:

1. dalsze wzmacnianie zdolności państwa do wczesnego wykrywania, analizy i atrybucji kampanii dezinformacyjnych, ze szczególnym uwzględnieniem działań skoordynowanych i operacji prowadzonych przez aktorów zagranicznych;
2. stworzenie sprawnego mechanizmu wymiany informacji pomiędzy administracją publiczną, NASK, platformami cyfrowymi, mediami, środowiskiem naukowym oraz przedsiębiorstwami technologicznymi, pozwalającego szybko identyfikować kampanie o istotnym znaczeniu dla bezpieczeństwa państwa i obywateli;
3. zapewnienie skutecznego egzekwowania obowiązków platform społecznościowych wynikających z DSA, w tym w odniesieniu do ryzyk systemowych związanych z dezinformacją, manipulacją procesami demokratycznymi, nielegalnymi reklamami i wykorzystywaniem sztucznej inteligencji;
4. wzmocnienie ochrony osób i instytucji, których tożsamość lub wizerunek są wykorzystywane do oszustw i kampanii dezinformacyjnych, poprzez szybkie i proste procedury zgłaszania, blokowania oraz dochodzenia praw;
5. rozwój kompetencji cyfrowych i edukacji medialnej społeczeństwa, obejmujących umiejętność weryfikowania źródeł, rozpoznawania manipulacji oraz treści generowanych lub modyfikowanych przy użyciu sztucznej inteligencji;
6. rozwijanie badań i dostępu do danych pozwalających oceniać rzeczywistą skalę dezinformacji oraz mechanizmy jej rozpowszechniania w Polsce, z zachowaniem ochrony danych osobowych, tajemnic prawnie chronionych i praw podstawowych;
7. wypracowanie procedur szybkiego reagowania na kampanie dezinformacyjne w sytuacjach szczególnego zagrożenia, w tym podczas wyborów, kryzysów bezpieczeństwa, klęsk żywiołowych, poważnych cyberataków oraz innych zdarzeń mogących wpływać na funkcjonowanie państwa i bezpieczeństwo obywateli.

Rada ds. Cyfryzacji podkreśla, że odporna przestrzeń informacyjna jest dziś jednym z fundamentów odpornego państwa cyfrowego. Nie istnieje przy tym jedno rozwiązanie

technologiczne, prawne czy instytucjonalne, które pozwoli wyeliminować dezinformację.

Potrzebujemy jednocześnie skutecznego prawa, odpowiedzialności platform społecznościowych, sprawnych instytucji publicznych, technologii umożliwiających identyfikację nowych zagrożeń oraz świadomego i odpornego informacyjnie społeczeństwa.

Bezpieczeństwo informacyjne powinno być traktowane jako wspólna odpowiedzialność państwa, przedsiębiorstw technologicznych, mediów, środowiska naukowego, organizacji społecznych oraz samych użytkowników. Szczególna odpowiedzialność spoczywa jednak na podmiotach, których technologie i decyzje dotyczące algorytmów mają bezpośredni wpływ na skalę i tempo rozpowszechniania informacji.

Agnieszka Jankowska
Przewodnicząca Rady do Spraw Cyfryzacji
/podpisano elektronicznie/

