

Magdalena Bigaj, Fundacja „Instytut Cyfrowego Obywatelstwa:

*Przedmiot ekspertyzy*

## **Dostęp dzieci i młodzieży do produktów i usług cyfrowych wysokiego ryzyka jako zadanie dla polityk publicznych**

*Streszczenie*

**Dzieci i młodzież w Polsce mają powszechny dostęp do produktów i usług cyfrowych wysokiego ryzyka, projektowanych z myślą o dorosłych użytkownikach i monetyzacji ich uwagi. Brak skutecznej weryfikacji wieku, niewystarczające mechanizmy ochrony oraz niska egzekucja istniejących przepisów powodują, że odpowiedzialność za bezpieczeństwo dzieci została w praktyce przerzucona na rodziców i szkoły, którzy nie są w stanie sprostać temu wyzwaniu bez wsparcia systemowego. Ekspertyza wskazuje potrzebę systemowej interwencji państwa, ukierunkowanej na obowiązki dostawców i producentów produktów i usług cyfrowych.**

### **OPIS PROBLEMU:**

- Produkty i usługi cyfrowe stały się stałym elementem codzienności dzieci i młodzieży w Polsce. Z badań NASK wynika, że zdecydowana większość nastolatków korzysta z internetu codziennie, a media społecznościowe są jednym z głównych obszarów ich aktywności online. Jednocześnie wiele dzieci uzyskuje dostęp do telefonu i internetu na bardzo wczesnym etapie rozwoju, co oznacza długotrwałą ekspozycję na środowisko cyfrowe bez adekwatnych zabezpieczeń.
- Istotnym elementem problemu jest niski poziom świadomości społecznej rodziców i opiekunów dotyczący mechanizmów działania produktów i usług cyfrowych oraz skali ryzyk, jakie niosą one dla dzieci i młodzieży. Badania NASK pokazują, że dorośli często nie posiadają wiedzy na temat algorytmicznego rekomendowania treści, mechanizmów monetyzacji uwagi ani rzeczywistych zagrożeń obecnych w komunikatorach, grach sieciowych i mediach społecznościowych. W efekcie decyzje rodzicielskie dotyczące dostępu dzieci do internetu podejmowane są w warunkach deficytu informacji, presji społecznej oraz normalizacji wczesnej inicjacji cyfrowej. Oparcie systemu ochrony dzieci wyłącznie na odpowiedzialności rodziców w takiej sytuacji jest nieadekwatne i pogłębia nierówności – skuteczna ochrona dzieci wymaga rozwiązań systemowych, które nie zakładają wysokiego poziomu kompetencji cyfrowych po stronie wszystkich opiekunów.
- Znaczna część produktów i usług cyfrowych, z których korzystają dzieci i młodzież, została zaprojektowana jako produkty wysokiego ryzyka, opierające się na

algorytmicznym zarządzaniu uwagą, personalizacji treści oraz monetyzacji aktywności użytkowników. Raport „Internet Dzieci” pokazuje, że ponad połowa dzieci w wieku 7–12 lat korzysta z platform społecznościowych formalnie przeznaczonych dla osób powyżej 13. roku życia, co wskazuje na systemowy charakter zjawiska obchodzenia progów wiekowych.

- Brak skutecznych mechanizmów weryfikacji wieku sprawia, że granice dostępu do produktów cyfrowych mają w praktyce charakter deklaracyjny. Badania NASK „Sprawdzian 13+” potwierdzają, że dzieci bez większych trudności uzyskują dostęp do usług przeznaczonych dla starszych użytkowników, często poprzez samodzielne podanie nieprawdziwego wieku. Odpowiedzialność za kontrolę wieku została w praktyce przeniesiona na dzieci i ich opiekunów.
- Algorytmiczne systemy rekomendacyjne stosowane w platformach społecznościowych i serwisach wideo wzmacniają ekspozycję dzieci i młodzieży na treści szkodliwe. Raport „Dobre i złe wiadomości” wskazuje, że znaczna część nastolatków styka się w internecie z treściami przemocowymi, seksualizującymi lub dotyczącymi samookaleczania i samobójstw, także wtedy, gdy nie poszukuje ich w sposób intencjonalny.
- Komunikatory i usługi oparte na komunikacji prywatnej stanowią kluczową infrastrukturę dla zjawisk takich jak grooming, przemoc relacyjna i cyberprzemoc. Z danych przywoływanych w raportach NASK i FDDS wynika, że duża część młodych użytkowników utrzymuje kontakt online z osobami, których nie zna osobiście, a doświadczenia przemocy rówieśniczej i seksualnej w środowisku cyfrowym mają charakter powszechny.
- Gry cyfrowe o charakterze społecznościowym stały się ważnym obszarem interakcji społecznych dzieci i młodzieży. Obecność czatów głosowych, trybów online oraz rozbudowanych mechanizmów rywalizacji powoduje, że gry te pełnią funkcję zbliżoną do platform społecznościowych, przy jednoczesnym niskim poziomie świadomości dorosłych dotyczącej ryzyk związanych z ich użytkowaniem.
- Szczególnym obszarem ryzyka są produkty cyfrowe wykorzystujące mechanizmy hazardowe i mikropłatności. Badania pokazują, że dzieci i młodzież mają powszechny dostęp do losowych mechanizmów nagród w grach, mimo że analogiczne formy hazardu w świecie offline podlegają ścisłym ograniczeniom wiekowym.
- Dynamicznie rozwijającą się kategorią produktów wysokiego ryzyka są narzędzia oparte na generatywnej sztucznej inteligencji. Brak jasnych standardów bezpieczeństwa i barier wiekowych sprawia, że dzieci wchodzą w interakcje z systemami symulującymi relacje społeczne lub generującymi treści, których wpływ na rozwój emocjonalny i psychiczny nie jest jeszcze wystarczająco rozpoznany.

## **WYZWANIA:**

- Jednym z kluczowych wyzwań jest rozbieżność między stanem prawnym a rzeczywistymi praktykami rynkowymi. Mimo istnienia regulacji dotyczących ochrony danych osobowych i wieku użytkowników, produkty i usługi cyfrowe wysokiego ryzyka

pozostają powszechnie dostępne dla dzieci, co podważa skuteczność obowiązujących przepisów.

- System ochrony dzieci w środowisku cyfrowym charakteryzuje się rozproszeniem kompetencji instytucjonalnych oraz niską skutecznością egzekwowania prawa. Odpowiedzialność za bezpieczeństwo dzieci została w praktyce przerzucona na rodziców, szkoły i same dzieci, mimo że podmioty rynkowe posiadają największe możliwości techniczne ograniczania ryzyka.
- Edukacja cyfrowa i działania profilaktyczne, choć niezbędne, są niewystarczające w sytuacji, gdy dzieci mają nieograniczony dostęp do produktów projektowanych w sposób ryzykowny. Dane z badań NASK i raportu „Dobre i złe wiadomości” pokazują, że nawet wysoka świadomość zagrożeń nie chroni przed negatywnymi skutkami intensywnego korzystania z usług cyfrowych.
- Istotnym wyzwaniem jest brak spójnych kryteriów identyfikacji produktów i usług cyfrowych wysokiego ryzyka. Obecne regulacje koncentrują się na pojedynczych kategoriach treści lub usług, nie uwzględniając mechanizmów projektowych, takich jak algorytmizacja, monetyzacja uwagi czy symulowanie relacji.
- Konsekwencje niekontrolowanego dostępu dzieci do usług wysokiego ryzyka mają charakter długofalowy i obciążają nie tylko dzieci i ich rodziny, lecz również system edukacji, ochrony zdrowia oraz pomocy społecznej. Brak systemowej reakcji zwiększa koszty społeczne i zdrowotne ponoszone przez państwo w kolejnych latach.
- Wyzwanie dostępu dzieci i młodzieży do produktów i usług cyfrowych wysokiego ryzyka wymaga spójnej interwencji polityk publicznych, opartej na zasadzie przeniesienia odpowiedzialności z użytkowników na dostawców, wzmocnienia mechanizmów regulacyjnych oraz skutecznego ich egzekwowania.

## REKOMENDACJE DLA POLITYK PUBLICZNYCH:

1. **Wprowadzenie powszechnej klasyfikacji wszystkich produktów i usług cyfrowych pod względem wieku i poziomu ryzyka**, na wzór systemów stosowanych w telewizji, VOD oraz w grach cyfrowych (np. PEGI), z jednoczesnym obowiązkowym oznaczaniem produktów wysokiego ryzyka w oparciu o ich mechanizmy projektowe, takie jak algorytmizacja treści, monetyzacja uwagi, komunikacja prywatna czy mikropłatności. Klasyfikacja powinna być czytelna dla użytkowników i stanowić podstawę regulacji oraz nadzoru.
2. **Nałożenie na dostawców usług cyfrowych obowiązku skutecznej i proporcjonalnej weryfikacji wieku użytkowników**, w szczególności w odniesieniu do produktów wysokiego ryzyka, przy jednoczesnym zapewnieniu ochrony danych osobowych dzieci i młodzieży oraz jasnych standardów technicznych.
3. **Wzmocnienie egzekwowania istniejących przepisów prawa**, w tym RODO i DSA, poprzez doprecyzowanie kompetencji instytucji nadzorczych, zwiększenie zasobów kontrolnych oraz realne sankcje wobec podmiotów, które umożliwiają dzieciom dostęp do usług przeznaczonych dla dorosłych.
4. **Przeniesienie ciężaru odpowiedzialności za bezpieczeństwo dzieci z użytkowników na dostawców usług**, poprzez obowiązek oceny ryzyka dla dzieci

(child impact assessment) oraz wdrażania rozwiązań typu safety by design i safety by default w produktach cyfrowych.

5. **Uzupełnienie regulacji o działania wspierające rodziców i szkoły**, w tym spójną strategię edukacji cyfrowej oraz systemowe kampanie informacyjne, traktowane jako element wspierający regulacje, a nie ich substytut.

## BIBLIOGRAFIA:

Bigaj, M., Ciesiołkiewicz, K., Mikulski, K., Miotk, A., Przewłocka, J., Rosa, M., Załęska, A. (2025). *Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w internecie*. Warszawa: Fundacja „Instytut Cyfrowego Obywatelstwa” oraz Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15.

Dębski M., Pyżalski J. Borchet J., Witkowska H. (2025). *Dobre i złe wiadomości – życie online i offline a zdrowie psychiczne polskich nastolatków. Raport z badań*. Gdańsk: Fundacja Dbam o Mój Zasięg.

Ładna, A., Kamiński, K., Roślaniec, K., Wrońska, A., Błażej, M., Jankiewicz, A., Konopczyński, F., Nawrot, M. (2025). *Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców – raport badawczy*. Warszawa: NASK – Państwowy Instytut Badawczy.

Makaruk, K., Drabarek, K., Popyk, A., Wójcik, Sz. (2023). *Diagnoza przemocy wobec dzieci w Polsce 2023*. Warszawa: Fundacja Dajemy Dzieciom Siłę

Wojtasik, Ł., Wójcik, Sz., Kopycka, J. (2025) *Sprawdzian 13+. Ogólnopolska weryfikacja skuteczności ograniczeń wiekowych w mediach społecznościowych z udziałem dzieci z klas I-III szkół podstawowych*. Warszawa: Fundacja Dajemy Dzieciom Siłę

## LICZBY:

58%

Ponad połowa dzieci w wieku 7–12 lat korzysta z platform społecznościowych formalnie przeznaczonych dla osób powyżej 13. roku życia, co pokazuje powszechne obchodzenie progów wiekowych i nieskuteczność deklaratywnej kontroli wieku. („Internet Dzieci”)

45%

Prawie połowa nastolatków deklaruje, że podawała w internecie nieprawdziwy wiek, aby uzyskać dostęp do treści lub usług przeznaczonych dla dorosłych. („Sprawdzian 13+”)

52%

Ponad połowa młodych użytkowników internetu utrzymywała kontakt online z osobami, których nie znała osobiście, co znacząco zwiększa ryzyko groomingu i innych form przemocy. („Dobre i złe wiadomości...”)

26%

Co czwarte dziecko w wieku 13–17 lat doświadczyło przemocy seksualnej bez kontaktu fizycznego w internecie, w tym niechcianego sekstingu, uwodzenia (groomingu) lub werbalnej przemocy seksualnej. ( „Diagnoza przemocy wobec dzieci w Polsce”)