

Bezpieczeństwo dzieci w internecie

OCHRONA MAŁOLETNICH I WZMOCNIENIE ICH POZYCJI
W CYFROWYM ŚWIECIE

SPRAWOZDANIE WSPÓŁPRZEWODNICZĄCYCH

SPECJALNEGO PANELU DS. BEZPIECZEŃSTWA DZIECI W INTERNECIE

Prof. dr Jörg M. Fegert i dr Maria Melchior



Przedmowa

W marcu 2026 r. przewodnicząca Komisji Europejskiej Ursula von der Leyen powierzyła dwóm specjalnym doradcom – prof. dr Jörgowi M. Fegertowi i dr Marii Melchior – współprzewodniczenie specjalnemu panelowi ds. bezpieczeństwa dzieci w internecie i potencjalnych ograniczeń wiekowych w mediach społecznościowych. Współprzewodniczącym powierzono zadanie sporządzenia sprawozdania na temat ustaleń panelu oraz przedstawienia zaleceń, w jaki sposób UE może najlepiej zadbać o bezpieczeństwo dzieci w internecie.

Panel, którego utworzenie przewodnicząca Komisji zapowiedziała po raz pierwszy w orędziu o stanie Unii w 2025 r., zgromadził czołowych przedstawicieli środowisk akademickich, osoby zawodowo zajmujące się tą dziedziną, młodzież i rodziców oraz innych specjalistów z różnych dziedzin z całej Europy. Wspólnie mieli oni ocenić wpływ mediów społecznościowych na osoby małoletnie.

*„A we wszystkich tych działaniach będziemy kierować się potrzebą wzmocnienia pozycji rodziców i budowania bezpieczniejszej Europy dla naszych dzieci. **Ponieważ jeśli chodzi o bezpieczeństwo naszych dzieci w internecie, Europa wierzy w rodziców, a nie w zyski**”.*

Przewodnicząca Komisji Ursula von der Leyen

Orędzie o stanie Unii z 2025 r.

Posiedzenia specjalnego panelu odbyły się trzykrotnie i za każdym razem uczestniczyli w nich różni specjaliści. Pierwsze posiedzenie specjalnego panelu odbyło się 5 marca 2026 r. Przeanalizowano wtedy istniejące dowody naukowe dotyczące wpływu mediów społecznościowych, a w szerszym ujęciu środowiska cyfrowego, na dzieci i nastolatki.

Drugie posiedzenie specjalnego panelu odbyło się 16 kwietnia 2026 r. Omówiono na nim istniejące przepisy i narzędzia UE oraz krajowe podejścia polityczne do kwestii bezpieczeństwa dzieci w internecie. Trzecie posiedzenie specjalnego panelu odbyło się 16 czerwca 2026 r. Skupiono się wtedy na krajowych podejściach politycznych i potencjalnych zaleceniach dotyczących ochrony i wzmocnienia pozycji dzieci i nastolatków w świecie cyfrowym.

Główne tematy omawiane podczas posiedzeń panelu obejmowały:

- pozytywne i negatywne skutki wprowadzenia konkretnych ograniczeń wiekowych w odniesieniu do mediów społecznościowych i innych usług cyfrowych;
- ukierunkowane podejście do ochrony i wzmocnienia pozycji małoletnich, dostosowane do różnych grup wiekowych, statusu społeczno-ekonomicznego i zagrożeń typowych dla danego wieku;

- zapewnienie bezpieczeństwa na etapie projektowania/domyślnego bezpieczeństwa oraz odpowiedzialność dostawców mediów społecznościowych i innych usług cyfrowych;
- działania edukacyjne i uświadamiające mające na celu promowanie odpowiedzialnego korzystania z internetu wśród dzieci i nastolatków, rodziców i opiekunów, a także nauczycieli i wychowawców;
- sposoby wspierania rodziców i wychowawców oraz sposoby wzmocnienia pozycji dzieci i nastolatków, aby były w stanie czerpać korzyści z możliwości, jakie oferują technologie cyfrowe.

Analiza i zalecenia zawarte w niniejszym sprawozdaniu opierają się na istotnych opiniach różnych specjalistów zaproszonych na poszczególne posiedzenia panelu oraz na liczne dodatkowe spotkania z przedstawicielami państw członkowskich, zwłaszcza te zorganizowane przez irlandzką prezydencję Rady UE i Luksemburg (posiedzenie ministerialne D9+), z państwami trzecimi (m.in. z Australią i Brazylią), z Parlamentem Europejskim i europosłami, zwłaszcza członkami Zespołu Międzypartyjnego ds. Praw Dziecka, z przedstawicielami branży internetowej, ze społeczeństwem obywatelskim, z ośrodkami analitycznymi i z innymi organizacjami, takimi jak Biuro Wysokiego Komisarza NZ ds. Praw Człowieka (OHCHR) i Europejska Rada Ochrony Danych (EROD).

W następstwie tych spotkań i dyskusji współprzewodniczący opracowali swoje zalecenia na podstawie zebranych dowodów. Odpowiedzialność za te zalecenia spoczywa wyłącznie na współprzewodniczących. Należy jednak zaznaczyć, że oparli się oni w dużym stopniu na pracy innych uznanych specjalistów, przedstawicieli rodziców i młodzieży oraz na wiedzy fachowej zapewnianej przez Komisję Europejską.

Sprawozdanie ma stanowić podstawę przyszłych działań, jakie ma zaproponować Komisja Europejska i państwa członkowskie UE w celu poprawy bezpieczeństwa dzieci w internecie. Ta niezależna ocena analityczna zawiera zalecenia i inspiracje dla dzieci i nastolatków, rodziców i opiekunów, nauczycieli i wychowawców oraz dla dostawców mediów społecznościowych i innych usług cyfrowych, mające umożliwić lepszą ochronę i wzmocnienie pozycji małoletnich w internecie.

Ramka: Zakres i terminologia

Zgodnie z zaleceniem przewodniczącej Ursuli von der Leyen główne zadanie specjalnego panelu polegało na omówieniu kwestii bezpieczeństwa dzieci w internecie oraz ewentualnych ograniczeń wiekowych dotyczących korzystania z mediów społecznościowych. Zakres niniejszego sprawozdania jest zgodny z powierzonym zadaniem. Dyskusje prowadzone podczas posiedzeń specjalnego panelu i inne wydarzenia polityczne (np. apel o bezpieczniejszą przestrzeń cyfrową

dla małoletnich, jaki 17 czerwca 2026 r. wystosowali przywódcy G-7) wskazują na potrzebę doprecyzowania terminologii stosowanej w niniejszym sprawozdaniu.

Bez uszczerbku dla wszelkich międzynarodowych, unijnych lub krajowych aktów prawnych w niniejszym sprawozdaniu stosuje się następujące terminy i odpowiadające im definicje:

- **Media społecznościowe i inne usługi cyfrowe (w skrócie „media społecznościowe+”)** – W niniejszym sprawozdaniu terminy „media społecznościowe+” oraz „media społecznościowe i inne usługi cyfrowe” są stosowane do szerokiego zdefiniowania usług, do których mogą mieć dostęp małoletni i które oferują nieodpowiednie do wieku lub ryzykowne treści i funkcje (np. uzależniające lub szkodliwe funkcje, takie jak możliwość niekończącego się przewijania treści, automatyczne odtwarzanie, algorytmy rekomendacji czy ciągłe powiadomienia). Pojęcie dostawców mediów społecznościowych i innych usług cyfrowych obejmuje platformy internetowe pełniące rolę pośredników w dostarczaniu treści pochodzących od osób trzecich, takie jak media społecznościowe, a także sklepy z aplikacjami. Obejmuje też systemy sztucznej inteligencji (AI) stwarzające zagrożenie dla bezpieczeństwa i rozwoju małoletnich, w tym wirtualnych asystentów AI, gry wideo narażające dzieci na szkodliwe praktyki handlowe lub niebezpieczne kontakty oraz platformy udostępniania plików wideo umożliwiające małoletnim dostęp nieodpowiedni do ich wieku.
- **Małoletni, dzieci i nastolatki** – Bez uszczerbku dla stosowania prawnie zdefiniowanego terminu „dzieci” (np. w Konwencji ONZ o prawach dziecka) w niniejszym sprawozdaniu opowiedziano się za przyjęciem podejścia do ochrony osób małoletnich w internecie, które uwzględnia ich rozwój oraz szczególne ryzyka i podatności na zagrożenia w zależności od wieku. Do celów niniejszej analizy autorzy posługują się terminem „małoletni” (lub „osoby małoletnie”) w odniesieniu do wszystkich dzieci i nastolatków poniżej 18 roku życia (czyli poniżej wieku, w którym osiąga się pełnoletność). Termin „nastolatki” stosowany jest w sprawozdaniu w odniesieniu do wszystkich małoletnich w wieku od 13 do 18 lat, natomiast termin „dzieci” – do wszystkich małoletnich poniżej 13 roku życia. Z kolei termin „prawa dziecka” odnosi się do praw wszystkich dzieci poniżej 18 roku życia, jak określono w tekstach prawnych. Termin „bezpieczeństwo dzieci w internecie”, jakim posłużono się w mandacie specjalnego panelu, stosowany jest jako termin ogólny oznaczający ochronę i wzmocnienie pozycji małoletnich w świecie cyfrowym.

Wstęp: Bezpieczne dorastanie w świecie mediów społecznościowych+

Szybki rozwój technologii cyfrowych radykalnie zmienił sposób, w jaki dzieci i nastolatki dorastają, wchodzą w interakcje z rówieśnikami, rodzicami, nauczycielami i otaczającym ich światem. Jednocześnie aktywność w środowisku pozacyfrowym jest im nadal niezbędna, aby mogły nawiązywać wartościowe relacje oraz zdobywać wiedzę i doświadczenia, które kształtują ich rozwój.

Świat mediów społecznościowych+ oferuje dzieciom i nastolatkom **wiele możliwości** edukacyjnych, towarzyskich i twórczych, jak również możliwości uczestnictwa. Aby móc w pełni je wykorzystać, małoletni potrzebują jednak odpowiedniej wiedzy oraz silniejszej pozycji.

Przestrzeń mediów społecznościowych+ stwarza też jednak szereg zagrożeń dla zdrowego rozwoju i dobrostanu małoletnich. Należą do nich: ryzyko nadmiernego korzystania z takich usług związane z ich uzależniającymi cechami projektowymi, ryzyko zastąpienia aktywności korzystnych pod względem rozwojowym, a także narażenie na szkodliwe treści oraz niewłaściwe kontakty w sieci. Pojawienie się nowych technologii potęguje te zagrożenia, co wymaga dokonania odważnych, choć przemyślanych wyborów pozwalających zwiększyć ochronę dzieci i nastolatków w internecie.

Powszechne korzystanie z mediów społecznościowych i innych usług cyfrowych sprawiło, że **decydenci i rodzice są bardzo zaniepokojeni zagrożeniami, na jakie narażone są dzieci i nastolatki w sieci**. Chociaż ograniczenia wiekowe w dostępie do mediów społecznościowych i innych usług cyfrowych spotkały się z krytyką, **mogą się one okazać niezbędnym działaniem zapobiegawczym** do czasu wykazania, że przestrzeń mediów społecznościowych+ jest bezpieczna dla dzieci i nastolatków, lub do czasu pojawienia się bezpiecznych alternatyw.

Ograniczenia wiekowe nie mają na celu obciążenia rodziców i opiekunów lub samych dzieci i nastolatków główną odpowiedzialnością za bezpieczeństwo małoletnich w internecie. Nie służą też zwolnieniu z tego obowiązku dostawców. **Dostawcy mediów społecznościowych i innych usług cyfrowych ponoszą główną odpowiedzialność za bezpieczeństwo opracowywanych i świadczonych przez siebie usług.**

Ciężar dowodu musi spoczywać na dostawcach, a nie na organach regulacyjnych, rodzicach i dzieciach. **Dopóki dostawcy mediów społecznościowych i innych usług cyfrowych nie wykażą, że ich usługi są zaprojektowane jako bezpieczne, powinni mieć ograniczoną możliwość oferowania takich usług dzieciom poniżej 13 roku życia w UE.** Oprócz ogólnounijnych ograniczeń państwa członkowskie mogą wprowadzić dalsze prewencyjne ograniczenia wiekowe w odniesieniu do nastolatków w wieku powyżej 13 lat.

Prewencyjne ograniczenia wiekowe to natychmiastowe środki służące osiągnięciu długoterminowego celu, jakim jest zapewnienie małoletnim bezpiecznej przestrzeni w mediach społecznościowych+ poprzez promowanie zmiany kulturowej. Wstępne doświadczenia krajów, które wprowadziły ogólny zakaz dostępu do mediów społecznościowych, pokazują, że większość małoletnich znajduje sposób na obejście tej polityki. Jednocześnie niektórzy małoletni przestali korzystać z ryzykownych mediów społecznościowych i usług cyfrowych, dzięki czemu mają teraz więcej czasu na aktywność offline (np. na uprawianie sportów czy bezpośrednie interakcje społeczne). Należy zatem uznać, że stopniowa zmiana w zakresie norm korzystania z mediów społecznościowych+ przez małoletnich jest możliwa.

Zmiana wymaga jednak czasu. Na przykład w niektórych krajach (m.in. w Niemczech i Szwecji) społeczna akceptacja ustawowego zakazu stosowania kar cielesnych w szkołach wymagała ponad jednego pokolenia. Za sprawą zakazu kar cielesnych doprecyzowano oczekiwania wobec rodziców, opiekunów, nauczycieli i wychowawców oraz zwiększono zaangażowanie osób postronnych, aby zapewnić wychowywanie dzieci bez użycia przemocy. O tym, że środek ten był dobrym rozwiązaniem, przekonują dające się zaobserwować korzystne tendencje. Potwierdza to również jego ocena, dokonywana w sposób ciągły od momentu jego wprowadzenia.

Zmiana postaw społecznych konieczna jest również w celu zapewnienia skuteczności ograniczeń wiekowych. Ciągła ocena i długoterminowe monitorowanie mogą pomóc decydentom upewnić się, czy nawyki małoletnich i ich rodziców, opiekunów i wychowawców z czasem się zmieniają.

Dorastając w świecie mediów społecznościowych+, dzieci i nastolatki muszą mieć możliwość prowadzenia zdrowego i satysfakcjonującego życia oraz korzystania z możliwości oferowanych przez media społecznościowe i inne usługi cyfrowe. **Prawa dziecka mają zastosowanie w internecie tak samo jak poza nim** – od prawa do bezpieczeństwa i prawa do ochrony przed wyzyskiem ekonomicznym i wszelkimi formami przestępczości (w szczególności przed przemocą seksualną) po prawo dostępu do informacji, edukacji i rekreacji.

„Od dziesięcioleci zwiększamy bezpieczeństwo dzieci w świecie rzeczywistym i teraz musimy zrobić to samo w świecie cyfrowym. Korzyści z technologii nie mogą powodować negatywnych skutków dla bezpieczeństwa, zdrowia i szczęścia dzieci.”

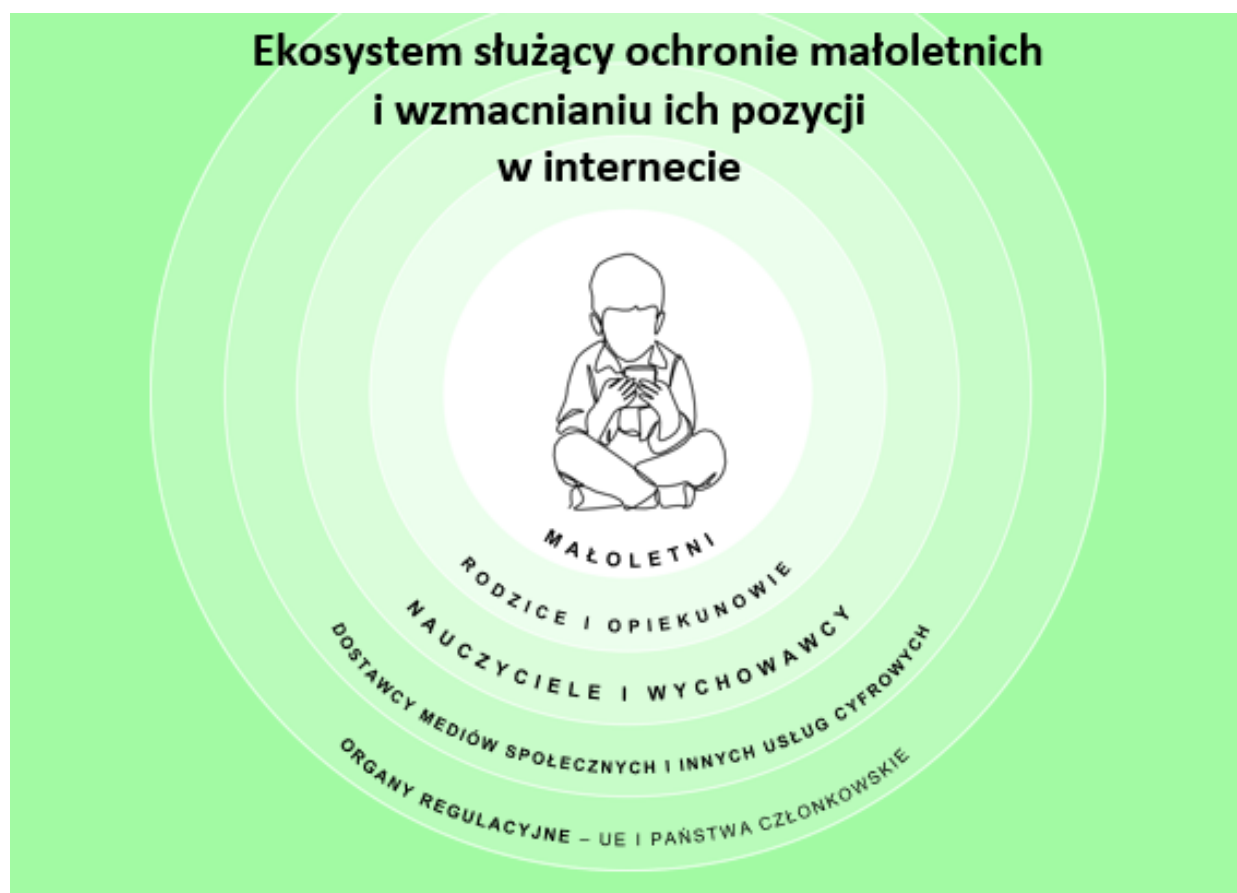
Przewodnicząca Komisji Ursula von der Leyen

Dzieci mają prawo dorastać w bezpiecznych warunkach, które sprzyjają ich rozwojowi, zarówno w internecie, jak i poza nim. Należy nadal wspierać małoletnich poza internetem, trzeba też jednak uznać, że środowisko cyfrowe staje się coraz ważniejszym elementem ich codziennego życia. Dlatego też wszystkie media społecznościowe oraz inne usługi cyfrowe powinny im zapewniać domyślną ochronę.

U podstaw środków na rzecz bezpieczeństwa dzieci w internecie muszą się znaleźć prawa dziecka. Ewentualne ograniczenia wiekowe muszą być w pełni zgodne z prawami dziecka oraz proporcjonalne i wyważone pod względem jego dobra. Środki stosowane w tym celu muszą nadążać za rozwojem technologicznym.

Nawet jeśli główną odpowiedzialność za bezpieczeństwo oferowanych usług ponoszą dostawcy mediów społecznościowych i innych usług cyfrowych, zwłaszcza w przypadku małoletnich, **aby chronić i wzmacniać pozycję dzieci i nastolatków w środowisku mediów społecznościowych+ potrzebny jest cały ekosystem podmiotów**. Od organów regulacyjnych, które muszą wprowadzić niezbędne środki, poprzez dostawców oferujących bezpieczne i dostosowane do wieku usługi, po rodziców, opiekunów, nauczycieli i wychowawców, którzy odgrywają zasadniczą rolę w nadzorowaniu i ukierunkowywaniu sposobu, w jaki osoby małoletnie korzystają z internetu. Małoletni szybko dorastają, a środowisko mediów społecznościowych+ szybko się zmienia, dlatego **powodzenie takiego ekosystemu zależy od wzajemnie powiązanych działań wszystkich podmiotów** podzielających tę samą wizję zapewnienia dzieciom i nastolatkom bezpiecznego dorastania w cyfrowym świecie.

Rys. 1: Ekosystem służący ochronie małoletnich i wzmacnianiu ich pozycji w internecie



Zapewnienie silniejszego impulsu politycznego na rzecz zwiększenia bezpieczeństwa dzieci w internecie

Ostatnie miesiące pokazały, że bezpieczeństwo dzieci w internecie staje się priorytetem politycznym na całym świecie. **Wprowadzenie i wdrożenie przez Australię rozwiązania polegającego na opóźnieniu możliwości korzystania z mediów społecznościowych przez dzieci, oraz ciągła jego ocena, pozwala reszcie świata wyciągnąć ważne wnioski.** Inne kraje, takie jak Zjednoczone Królestwo i Kanada, poszły za tym przykładem i zamierzają przedstawić wnioski ustawodawcze, Indonezja natomiast wprowadziła już zakaz.

Z niedawnego badania wynika, że zdaniem 92 proc. Europejczyków wzmocnienie ochrony dzieci i młodzieży w internecie powinno należeć do priorytetów UE. ⁱ

Przywódcy europejscy również zaczęli zajmować się tą kwestią. Deklaracja z Jutlandiiⁱⁱⁱ z września 2025 r. oraz rezolucja Parlamentu Europejskiego wzywająca do ustanowienia ogólnounijnego minimalnego wieku dojrzałości cyfrowejⁱⁱⁱ, powołanie przez przewodniczącą Ursulę von der Leyen specjalnego panelu ds. bezpieczeństwa dzieci w internecie oraz niedawne konkluzje Rady Europejskiej^{iv} wyraźnie wskazują na rosnącą dynamikę polityczną sprzyjającą podjęciu konkretnych działań w celu przeciwdziałania rosnącym zagrożeniom, na jakie narażone są dzieci w internecie.

W czerwcu 2026 r. grupa G-7 – w tym Kanada, Francja, Niemcy, Włochy, Japonia, Zjednoczone Królestwo, Stany Zjednoczone i Unia Europejska – po raz pierwszy uzgodniły na najwyższym szczeblu politycznym wspólne zasady ochrony małoletnich przed zagrożeniami związanymi z usługami cyfrowymi^v.

Ponadto kilka państw członkowskich UE prowadzi prace legislacyjne z zamiarem ustanowienia minimalnego wieku dostępu do mediów społecznościowych i innych usług cyfrowych, które mogą narażać dzieci i nastolatki na szkodliwe skutki. Na przykład Francja proponuje wprowadzenie ograniczenia dla osób poniżej 15 roku życia w oparciu o czarną listę zastrzeżonych usług. Grecja planuje wprowadzenie ograniczenia możliwości korzystania z serwisów społecznościowych online w stosunku do osób poniżej 15 roku życia. Dania rozważa wprowadzenie ograniczenia dla osób poniżej 16 roku życia, z możliwością obniżenia tej granicy za zgodą rodziców. Szwecja przewiduje wprowadzenie ograniczenia w oparciu o rok, w którym dziecko kończy 15 lat, przy czym niektóre rodzaje usług są wyłączone z tego ograniczenia. Przyjęcie przepisów w tej dziedzinie rozważa też wiele innych państw, od Portugalii i Hiszpanii po Niemcy i Polskę.

W tej sytuacji istnieje realne ryzyko, że dojdzie do rozdrobnienia europejskiego jednolitego rynku usług cyfrowych. W związku z tym wiele państw członkowskich opowiada się za tym, by kwestią tą zająć się na szczeblu UE. Należy przyjąć, że w poszczególnych państwach członkowskich występują różne uwarunkowania kulturowe i krajowe mające wpływ na edukację, umiejętności cyfrowe i ochronę

małoletnich. Rozdrobnienie mogłoby doprowadzić do sytuacji, w której małoletni korzystaliby z różnych poziomów ochrony w całej UE. Oznaczałoby to również, że organy regulacyjne mogłyby stanąć w obliczu praktycznych komplikacji związanych z egzekwowaniem przepisów, a dostawcy usług ponosiliby wyższe koszty przestrzegania przepisów. Mogłoby to mieć niekorzystne skutki uboczne dla rozwoju bezpieczniejszych mediów społecznościowych i innych usług cyfrowych oraz skuteczności przepisów dotyczących bezpieczeństwa w sieci.

UE podjęła już konkretne działania, aby chronić małoletnich. Niedawne decyzje przyjęte przez Komisję Europejską podkreślają jedynie konieczność zajęcia się zagrożeniami dla dzieci i nastolatków w sieci, na występowanie których to zagrożeń istnieją konkretne dowody. Do ewidentnych przykładów należą wstępne ustalenia dotyczące Meta i TikToka w związku z domniemaniem, że firmy te nie spełniają wysokich standardów ochrony małoletnich w sieci wymaganych na mocy aktu o usługach cyfrowych (DSA), oraz w związku z niezapewnieniem łatwo dostępnych mechanizmów sygnalizowania treści przedstawiających niegodziwe traktowanie dzieci w celach seksualnych. Punktem zwrotnym w debacie na temat odpowiedzialności platform były ponadto niedawne przełomowe decyzje sądów amerykańskich.

Krótką historia ochrony małoletnich w internecie

Wysiłki na rzecz ochrony dzieci i nastolatków w internecie podejmowano od początku jego istnienia, tj. już w okresie poprzedzającym media społecznościowe, smartfony i sztuczną inteligencję. Podstawy dzisiejszych zasad w zakresie ochrony małoletnich w sieci zostały ustanowione w latach 90. XX wieku i na początku XXI wieku, kiedy to przyjęto przepisy mające umożliwić usługodawcom i przedsiębiorstwom prowadzenie działalności i wymianę informacji ponad granicami. Chociaż przepisy te nie zostały opracowane wyłącznie w celu ochrony dzieci i nastolatków w sieci, obejmowały wiele zasad, które nadal stanowią podstawę obowiązujących przepisów w trzech obszarach.

Pierwszym z tych obszarów są regulacje dotyczące mediów i usług cyfrowych na rynku wewnętrznym, które wprowadziły wspólne zasady dotyczące usług telewizyjnych w całej Europie, w tym zabezpieczenia przed treściami, które mogą być szkodliwe dla małoletnich. Pierwsze zharmonizowane ramy dotyczące usług online lub „usług społeczeństwa informacyjnego” (ustanowione dyrektywą o handlu elektronicznym) wspierały również rozwój transgranicznych usług internetowych w UE.

Drugim obszarem są przepisy dotyczące ochrony danych i prywatności, które zapoczątkowała dyrektywa o ochronie danych z 1995 r. wprowadzająca wspólne normy dotyczące gromadzenia i wykorzystywania danych osobowych we wszystkich państwach członkowskich.

Trzecim obszarem jest ochrona konsumentów. Wspólne przepisy UE pozwalają zwalczać wprowadzające w błąd i agresywne praktyki handlowe. Zgodnie z tymi przepisami konsumenci podatni na zagrożenia potrzebują dodatkowej ochrony. Ta ważna zasada obowiązuje również w środowisku cyfrowym. Obejmuje ona sytuacje, w których dzieci i nastolatki są narażone na praktyki handlowe, które mogą mieć na nie inny wpływ niż na osoby dorosłe.

Ponieważ technologie cyfrowe stały się nieodłączną częścią naszej codzienności, UE stale aktualizuje obowiązujące ramy prawne, aby odpowiadały nowym wyzwaniom. Ogólnym rozporządzeniem o ochronie danych (RODO) wprowadzono szczególne środki ochrony w odniesieniu do danych osobowych dzieci w internecie i zgody na ich przetwarzanie. Rozszerzono przepisy dyrektywy o audiowizualnych usługach medialnych na nowe formy treści audiowizualnych i na platformy udostępniania plików wideo. Natomiast aktem o usługach cyfrowych ustanowiono przepisy dotyczące internetowych usług pośrednich, m.in. w konkretnym celu ochrony małoletnich.

Wprowadzone zmiany odzwierciedlają szerszą tendencję: technologie cyfrowe nie mieszczą się już ściśle w jednej kategorii regulacyjnej lub prawnej. Media społecznościowe i inne usługi cyfrowe łączą elementy mediów, komunikacji, handlu i przetwarzania danych, często w ramach tej samej platformy. W związku z tym skuteczne podejście do ochrony małoletnich w sieci musi być całościowe i opierać się na instrumentach w kilku obszarach prawa UE, m.in. na przepisach dotyczących platform, ochrony danych i ochrony konsumentów oraz na regulacjach w zakresie mediów audiowizualnych.

Wraz z szybkim rozwojem i wprowadzaniem sztucznej inteligencji zagrożenia dla małoletnich w internecie gwałtownie rosną. Towarzyszy temu ciągły rozwój mediów społecznościowych i innych usług cyfrowych, które w epoce „ekonomii uwagi” stawiają sobie za cel, by przyciągać jak najwięcej użytkowników i jak najdłużej ich angażować. Dziś bardziej niż kiedykolwiek potrzebne są działania organów regulacyjnych w celu wzmocnienia ochrony małoletnich i umożliwienia im bezpiecznego poruszania się po świecie mediów społecznościowych+.

Fakty dotyczące zagrożeń i korzyści dla małoletnich w sieci

Szybki rozwój technologiczny przyniósł dzieciom nadzwyczajne możliwości w zakresie interakcji z rówieśnikami, wyrażania własnej kreatywności oraz dostępu do wiedzy i wsparcia. Dzieci nie są jednak dorosłymi, a środowisko mediów społecznościowych+ naraża je na różne zagrożenia mające wpływ na ich zdrowie fizyczne i psychiczne oraz na poszczególne etapy dojrzewania. Ważny wpływ mają też czynniki społeczno-ekonomiczne i indywidualne, takie jak sytuacja rodzinna czy płeć, a także cechy projektowe mediów społecznościowych i innych usług cyfrowych.

Zasadnicze znaczenie dla podjęcia odpowiednich działań mających na celu ochronę i wzmocnienie pozycji małoletnich w internecie ma oparta na rzetelnych dowodach wiedza o sposobach, w jaki ryzyka i szkodliwe skutki

wiążą się z mediami społecznościowymi i innymi usługami cyfrowymi. Szczególne cechy, funkcje lub formaty stosowane w mediach społecznościowych+ mogą być szkodliwe w różnym stopniu, w zależności od sytuacji społecznej i osobistej dziecka lub nastolatka. Osoby małoletnie należące do mniejszości rasowych, etnicznych i religijnych, członkowie społeczności LGBTIQ+, osoby o specjalnych potrzebach edukacyjnych lub osoby z wcześniejszymi zaburzeniami psychicznymi mogą być szczególnie podatne na szkodliwe skutki aktywności w sieci. Podatność ta jest oczywiście potęgowana przez media społecznościowe i inne usługi cyfrowe wykorzystujące szkodliwe, manipulacyjne lub uzależniające cechy projektowe lub treści. Jako że te cechy i funkcje ciągle się zmieniają, należy stale kontynuować badania i gromadzenie dowodów.

Zagrożenia, jakie media społecznościowe stwarzają dla zdrowia fizycznego i psychicznego małoletnich, są dalekosiężne. Jeśli chodzi o zdrowie fizyczne, zbyt długi czas spędzany przed ekranem zastępuje zabawę na świeżym powietrzu i uprawianie sportu, co może mieć wpływ na zdrowie, sprawność fizyczną i sen dzieci. Korzystanie z mediów społecznościowych+ i z urządzeń od najmłodszych lat wypiera własnoręczne odkrywanie realnego świata i bezpośrednie interakcje społeczne. Może to wpływać na rozwój społeczno-emocjonalny i podatność na problemy ze zdrowiem psychicznym. Długotrwałe używanie urządzeń może również powodować problemy takie jak zaburzenia układu mięśniowo-szkieletowego i cyfrowe zmęczenie oczu.

Zagrożenia dla zdrowia psychicznego dzieci stwarzane przez korzystanie z mediów społecznościowych i innych usług cyfrowych są znaczne. Bezpośrednie zagrożenia dla zdrowia psychicznego dzieci stwarzane przez środowisko mediów społecznościowych+ są wzajemnie powiązane z możliwością pogłębiania przez media społecznościowe+ istniejących wcześniej problemów ze zdrowiem psychicznym, w tym depresji i stanów lękowych. Również w tym przypadku czynniki społeczne i indywidualne determinują stopień narażenia dzieci i nastolatków na ryzyko.

Ogólnie rzecz biorąc, intensywne korzystanie z mediów społecznościowych i innych usług cyfrowych przez dzieci i nastolatków wiąże się z problemami ze snem i koncentracją oraz częstszym występowaniem depresji i stanów lękowych. Uzależniające cechy projektowe wzmacniają te efekty, zachęcając do kompulsywnego sprawdzania, wywołując „lęk przed tym, że coś nas omija” (FOMO) i powodując częstsze porównywanie się z innymi. Może to osłabiać poczucie własnej wartości małoletnich i podnosić poziom stresu. Promowanie treści za pomocą algorytmów i systemy rekomendacji mogą wzmacniać dezinformację i nawoływanie do nienawiści. Poważne szkody wynikające z tego efektu odczuwają w internecie zwłaszcza słabsze grupy społeczne.

Ryzyko, że małoletni będą w internecie narażeni na kontakt z materiałami przestępczymi i nielegalnymi, jest znaczne. Zarówno dorośli, jak i małoletni celowo wykorzystują media społecznościowe i inne usługi cyfrowe, w tym platformy gier, do

kontaktów z dziećmi i nastolatkami. Zagrożenia obejmują narażenie na niegodziwe traktowanie dzieci w celach seksualnych (materiały), nagabywanie dzieci w celach seksualnych, cyberprzemoc, radykalizację postaw i podżeganie do popełniania czynów nielegalnych, aktów przemocy lub aktów terrorystycznych. Powszechne stosowanie narzędzi sztucznej inteligencji stanowi poważne zagrożenie dla dzieci i nastolatków w związku z produkcją syntetycznych materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych (np. deepfake). Nadużycia te mają drastyczny wpływ na rozwój małoletnich, ich zdrowie psychiczne i fizyczne, a w najpoważniejszych przypadkach – mogą kosztować ich życie.

Dostawcy mediów społecznościowych i innych usług cyfrowych ponoszą główną odpowiedzialność za zapewnienie małoletnim bezpieczeństwa w ramach swoich usług. Ponadto ważną rolę w nadzorowaniu czasu spędzanego przez dzieci i nastolatki w internecie oraz w pomaganiu małoletnim w radzeniu sobie z zagrożeniami, na jakie są oni narażeni w środowisku mediów społecznościowych+, odgrywają rodzice i opiekunowie. Zapewnienie odpowiednich aktywności offline i bezpośrednich interakcji z innymi ludźmi ma kluczowe znaczenie w każdym wieku.

Mimo że świat mediów społecznościowych+ może być szkodliwy, **oferuje on jednocześnie dzieciom i nastolatkom wiele możliwości.** Gdy małoletni mają mocną pozycję, by bezpiecznie komunikować się w internecie i posiadają solidne umiejętności cyfrowe, korzystanie z mediów społecznościowych i innych usług cyfrowych może korzystnie wpływać na dobrostan, relacje społeczne, zapewniać wspierające sieci rówieśników, możliwości samoekspresji, zaangażowania obywatelskiego i samodzielnego uczenia się. Ukierunkowane inicjatywy w zakresie umiejętności cyfrowych – takie jak europejska strategia na rzecz lepszego internetu dla dzieci, centra bezpieczniejszego internetu oraz włączenie umiejętności korzystania z mediów do krajowych programów kształcenia i szkolenia – wykazały, że można dzięki nim zachęcać do krytycznego myślenia, zwiększyć odporność na dezinformację oraz poprawić zdolności małoletnich do bezpiecznego poruszania się w internecie.

Media społecznościowe i inne usługi cyfrowe, które uwzględniają bezpieczeństwo już na etapie projektowania, mogłyby przyczynić się do wzmocnienia pozycji dzieci i nastolatków oraz wzmocnić ich uczestnictwo w internecie poprzez wspieranie nabywania przez nich umiejętności cyfrowych i umiejętności korzystania z mediów. Odpowiednia do wieku edukacja cyfrowa zapewniana w szkołach przy wsparciu rodziców i opiekunów mogłaby również przygotować małoletnich do korzystania z możliwości oferowanych przez cyfrowy świat oraz do mitygowania ewentualnych zagrożeń i szkód.

Potrzeba przeciwdziałania zagrożeniom typowym dla danego wieku

W miarę jak dzieci dorastają i stają się bardziej niezależne, zdolność rodziców do nadzorowania ich aktywności w internecie maleje. Rośnie natomiast wpływ rówieśników. W okresie dojrzewania, w drodze do osiągnięcia pełnoletności, małoletni

stają się coraz bardziej niezależni w korzystaniu z internetu, lepiej rozumieją zagrożenia, na które są narażeni w internecie, a także lepiej sobie z nimi radzą. Trzylatek i szesnastolatek mają w oczywisty sposób różne potrzeby. Podkreśla to, jak duże **znaczenie ma podejście do bezpieczeństwa dzieci w internecie z uwzględnieniem kwestii rozwojowych**. Takie podejście zastosowaliśmy w niniejszym sprawozdaniu, **poprzez rozróżnienie między różnymi grupami wiekowymi**:

Poniżej trzeciego roku życia dzieci są przede wszystkim narażone na problemy związane z relacjami i „technoferencję”¹ jako bierni użytkownicy internetu. Chodzi tu o sytuację, gdy opiekunowie zastępują bezpośrednie kontakty międzyludzkie czasem spędzonym przed ekranem, aby „uspokoić” małe dzieci lub odwrócić ich uwagę. Może to mieć wpływ na umiejętność skupienia się, naukę mówienia i rozwój społeczno-emocjonalny.

W przedziale wiekowym od 3 do 5 lat dzieci jako nowi niezależni użytkownicy korzystający z internetu pod nadzorem opiekunów są coraz bardziej narażone na zagrożenia występujące w środowisku internetowym i zagrożenia związane z dłuższym czasem ekranowym. Media społecznościowe i inne usługi cyfrowe, które są zoptymalizowane pod kątem natychmiastowej gratyfikacji, powtarzalnych nagród i ciągłej zewnętrznej stymulacji, są w zasadniczy sposób niedopasowane do rozwijających się zdolności dzieci i mogą zaszkodzić ich długoterminowemu rozwojowi.

W przedziale wiekowym od 6 do 9 lat dzieci znacznie częściej korzystają z mediów społecznościowych i innych usług cyfrowych. Zewnętrzne informacje zwrotne z internetu (np. polubienia, oceny i rankingi) nakładają się na rozwijającą się samoocenę opartą na nabywaniu kompetencji w świecie rzeczywistym. Może to potęgować niepokój o wyniki i porównywanie się z rówieśnikami, zwiększając podatność na nękanie w sieci, mowę nienawiści i prześladowanie przez rówieśników.

W przedziale wiekowym od 10 do 12 lat dostęp dzieci do mediów społecznościowych+ staje się głównym warunkiem wstępnym uczestnictwa w życiu społecznym. W tym wieku wyczulenie dzieci typowe dla tego okresu rozwoju w najdotkliwszy sposób zderza się ze wzmocnieniem tej wrażliwości napędzanym przez platformy. Algorytmiczne systemy rekomendacji potęgują porównywanie się z innymi, narażenie na szkodliwe lub nielegalne treści (w tym materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych, ekstremistyczną propagandę i dezinformację) oraz narażenie na uzależniające wzorce projektowe, które nasilają objawy depresji i stanów lękowych. Niedawne badania perspektywiczne sugerują, że zakup pierwszego smartfona w wieku 12 (a nie 13) może wiązać się z wyższym ryzykiem depresji i innych problemów ze

¹ Powodowane technologią zaburzenie interakcji rodzic–dziecko.

zdrowiem psychicznym po upływie jednego roku^{vi}. Przykład ten pokazuje, że ogólnie rzecz biorąc, dzieci poniżej 13 roku życia są szczególnie podatne na zagrożenia.

W przedziale wiekowym od 13 do 15 lat nastolatki przechodzą od nadzorowanego do coraz bardziej samodzielnego korzystania z mediów społecznościowych i innych usług cyfrowych. W tym wieku tradycyjne formy nadzoru ze strony opiekunów i nauczycieli w szkole stają się coraz mniej skuteczne. Zagrożenia są w coraz większym stopniu kształtowane przez strukturę mediów społecznościowych i innych usług cyfrowych, a nie przez indywidualne zachowania. Kluczowym wyzwaniem jest radzenie sobie z systemami algorytmicznymi, które kształtują ekspozycję na treści i wpływają na zachowanie, a których sposoby działania są mało przejrzyste.

Osiągnięcie samodzielności jest normalnym elementem dorastania w dzisiejszym świecie internetowym, podobnie jak w świecie offline. Nie chodzi zatem o to, jak ograniczać nastolatków w procesie uzyskiwania samodzielności, lecz jak ograniczyć ich narażenie na szkodliwe skutki w okresie największej podatności rozwojowej. Skuteczna ochrona wymaga rozwojowo uwarunkowanego, wielowarstwowego podejścia, łączącego objęcie mediów społecznościowych i innych usług cyfrowych regulacjami prawnymi, interwencje edukacyjne oraz wsparcie samodzielnego kontrolowania się i krytycznego korzystania z mediów.

W przedziale wiekowym od 16 do 18 lat nastolatki przechodzą etap coraz większej konsolidacji tożsamości i rosnącej samodzielności. Rozwijające się zdolności nastolatków lepiej przygotowują ich do zrozumienia zagrożeń, z którymi mierzą się w internecie, i do radzenia sobie z nimi. Jednak rozwój neurobiologiczny nadal trwa, a korzystanie z mediów społecznościowych i innych usług cyfrowych nasila ryzyko uzależnienia, zaburzeń lękowych oraz problemów ze zdrowiem psychicznym. Nastolatki w tym wieku muszą zdobyć niezbędne umiejętności (np. umiejętność krytycznego myślenia i oceny sytuacji), aby skutecznie i bezpiecznie poruszać się w świecie cyfrowym oraz w pełni wykorzystać jego potencjał.

Sześć podstawowych zasad służących ochronie małoletnich i wzmacnianiu ich pozycji w internecie

Środowisko mediów społecznościowych+ to dla dzieci i nastolatków zarówno zagrożenia, jak i możliwości, dlatego należy stworzyć kompleksowe ramy, które ochronią dzieci w internecie, wzmacniając jednocześnie ich pozycję.

Współprzewodniczący opracowali sześć podstawowych zasad, które nadały kierunek pracom specjalnego panelu i które odzwierciedlono w strukturze niniejszego sprawozdania. Środki powinny opierać się na solidnych dowodach i analizie wyzwań oraz możliwości, przed którymi stoją dzieci w internecie. Skuteczne wdrożenie i ocena mają kluczowe znaczenie dla zapewnienia rezultatów.

- **Zasada 1: Podejście uwzględniające rozwój (zob. rozdział 1)**

Zapewnienie odpowiednich do wieku regulacji i zróżnicowanych wytycznych.

Stopniowy rozwój dzieci i nastolatków wymaga opracowania i wdrożenia środków ochrony uwzględniających zagrożenia, na jakie są one narażone w poszczególnych okresach życia. W miarę możliwości środki te powinny uwzględniać osobistą i społeczną sytuację dzieci, która może zwiększać ich narażenie na zagrożenia.

- **Zasada 2: Równość i różnorodność (zob. rozdział 2)**

Uznanie faktu, że w zależności od grupy wiekowej i społeczno-ekonomicznej istnieją nierówności pod względem zagrożeń i narażenia na szkodliwe skutki w internecie. Płeć, orientacja seksualna, pochodzenie rasowe, etniczne i religijne, specjalne potrzeby edukacyjne oraz istniejące wcześniej problemy ze zdrowiem psychicznym wpływają na podatność osób małoletnich na zagrożenia w internecie. Czynniki te wpływają również na zasoby i zdolności rodziców i opiekunów do wspierania dzieci i nastolatków na drodze do samodzielności.

- **Zasada 3: Ochrona małoletnich (zob. rozdział 3)**

Dzieci i nastolatki muszą mieć możliwość korzystania z bezpiecznej przestrzeni mediów społecznościowych⁺. Przy projektowaniu mediów społecznościowych i innych usług cyfrowych należy zapewniać ochronę małoletnich przed szkodliwymi treściami, uzależniającymi funkcjami, zaniedbaniem cyfrowym² i przestępstwami w internecie (na przykład niegodziwym traktowaniem w celach seksualnych). Małoletni powinni mieć możliwość łatwego zgłaszania wszelkich szkodliwych treści lub funkcji. Takie zgłoszenia powinny być traktowane priorytetowo, a szkodliwe treści lub funkcje powinny być niezwłocznie usuwane przez dostawców.

- **Zasada 4: Rozliczalność usług cyfrowych i prawa konsumentów (zob. rozdział 3)**

Dostawcy mediów społecznościowych i innych usług cyfrowych muszą wziąć na siebie główną odpowiedzialność za zapewnienie małoletnim bezpiecznego dostępu do przestrzeni internetowej i bezpiecznego korzystania z niej. Należy zachęcać do stosowania środków pozwalających uwzględnić bezpieczeństwo już w fazie projektowania usług cyfrowych oraz szybko egzekwować przepisy związane z treściami. Ciężar dowodu powinien spoczywać na dostawcach mediów społecznościowych i innych usług cyfrowych, którzy powinni udowodnić, że ich usługi nie są szkodliwe, zanim uzyskają do nich dostęp dzieci i nastolatki.

- **Zasada 5: Wzmocnienie pozycji i edukacja medialna (zob. rozdział 4)**

Umożliwienie rodzicom i opiekunom, nauczycielom i wychowawcom wspierania dzieci i nastolatków w stopniowym przejściu do bezpiecznego i samodzielnego korzystania z internetu. Oferowanie wystarczających możliwości (np. szkoleń w zakresie

² Powtarzające się niezapewnienie przez opiekuna rozwojowo odpowiedniej uwagi, adekwatnego reagowania, nadzoru lub ochrony, ponieważ technologie cyfrowe zakłócają, zastępują lub podkopują podstawowe działania opiekuńcze.

umiejętności cyfrowych i umiejętności korzystania z mediów) oraz odpowiedniej infrastruktury, aby umożliwić rodzicom refleksję nad własną aktywnością w sieci i kierowanie interakcjami małoletnich w internecie. Środki muszą być dostosowane do zmieniających się ról, jakie pełnią opiekunowie i nauczyciele wraz z dojrzewaniem dzieci i nastolatków.

- **Zasada 6: Prawa i uczestnictwo dzieci (zob. rozdział 4)**

Ochrona prawa dzieci do bezpiecznego uczestnictwa, interakcji i współtworzenia, w internecie i poza nim. Prawa dziecka, rozumiane zgodnie z odpowiednimi ramami międzynarodowymi³, powinny zawsze leżeć u podstaw środków ochrony dzieci. Ograniczenia wiekowe muszą respektować prawa dziecka w internecie, być proporcjonalne, ograniczone w czasie i wyważone względem najlepszego interesu dziecka. Podkreśla to również potrzebę inwestowania w aktywności poza internetem i promowanie takiej aktywności - w odniesieniu do małoletnich w każdym wieku.

Specjalni doradcy przewodniczącej i współprzewodniczący specjalnego panelu ds. bezpieczeństwa dzieci w internecie

Prof. dr Jörg M. Fegert

Dr Maria Melchior



Prof. dr Jörg M. Fegert

Dyrektor ds. medycznych
Kliniki Psychiatrii Dziecięcej i
Młodzieżowej, Psychosomatyki
i Psychoterapii Dzieci i
Młodzieży w Szpitalu
Uniwersyteckim w Ulm



Dr Maria Melchior

Dyrektor ds. badań we
francuskim Narodowym
Instytucie Zdrowia i Badań
Medycznych (INSERM)

³ W szczególności chodzi o Konwencję ONZ o prawach dziecka i ogólne uwagi Komitetu Praw Dziecka, Kartę praw podstawowych Unii Europejskiej oraz strategię UE na rzecz praw dziecka.

SZEŚĆ PODSTAWOWYCH ZASAD

służących ochronie małoletnich i wzmocnieniu ich pozycji w internecie

BEZPIECZEŃSTWO DZIECI W INTERNECIE

ANALIZA SYTUACJI

PODEJŚCIE UWZGLĘDNIAJĄCE ROZWÓJ

Zapewnienie odpowiednich do wieku regulacji i zróżnicowanych wytycznych

RÓWNOŚĆ I RÓŻNORODNOŚĆ

Uznanie faktu, że we wszystkich grupach istnieją nierówności pod względem zagrożeń, narażenia i szkodliwych skutków w internecie

OCHRONA MAŁOLETNIICH

Ochrona przed szkodliwymi treściami, uzależniającymi cechami projektowymi, zaniedbaniem cyfrowym, przestępstwami (np. niegodziwym traktowaniem w celach seksualnych, nękaniami)

ROZLICZALNOŚĆ USŁUG CYFROWYCH I PRAWA KONSUMENTÓW

Egzekwowanie przepisów dotyczących bezpieczeństwa już na etapie projektowania oraz przepisów dotyczących treści

WZMOCNIENIE POZYCJI I EDUKACJA MEDIALNA

Umożliwienie rodzicom i opiekunom wspierania małoletnich w nabywaniu umiejętności cyfrowych i umiejętności korzystania z mediów w celu odpowiedzialnego użytkowania

PRAWA I UCZESTNICTWO DZIECI

Ochrona prawa dzieci do bezpiecznego uczestnictwa i współtworzenia w internecie

ŚRODKI

OCENA

Najważniejsze zalecenia dotyczące ochrony i wzmocnienia pozycji małoletnich w internecie

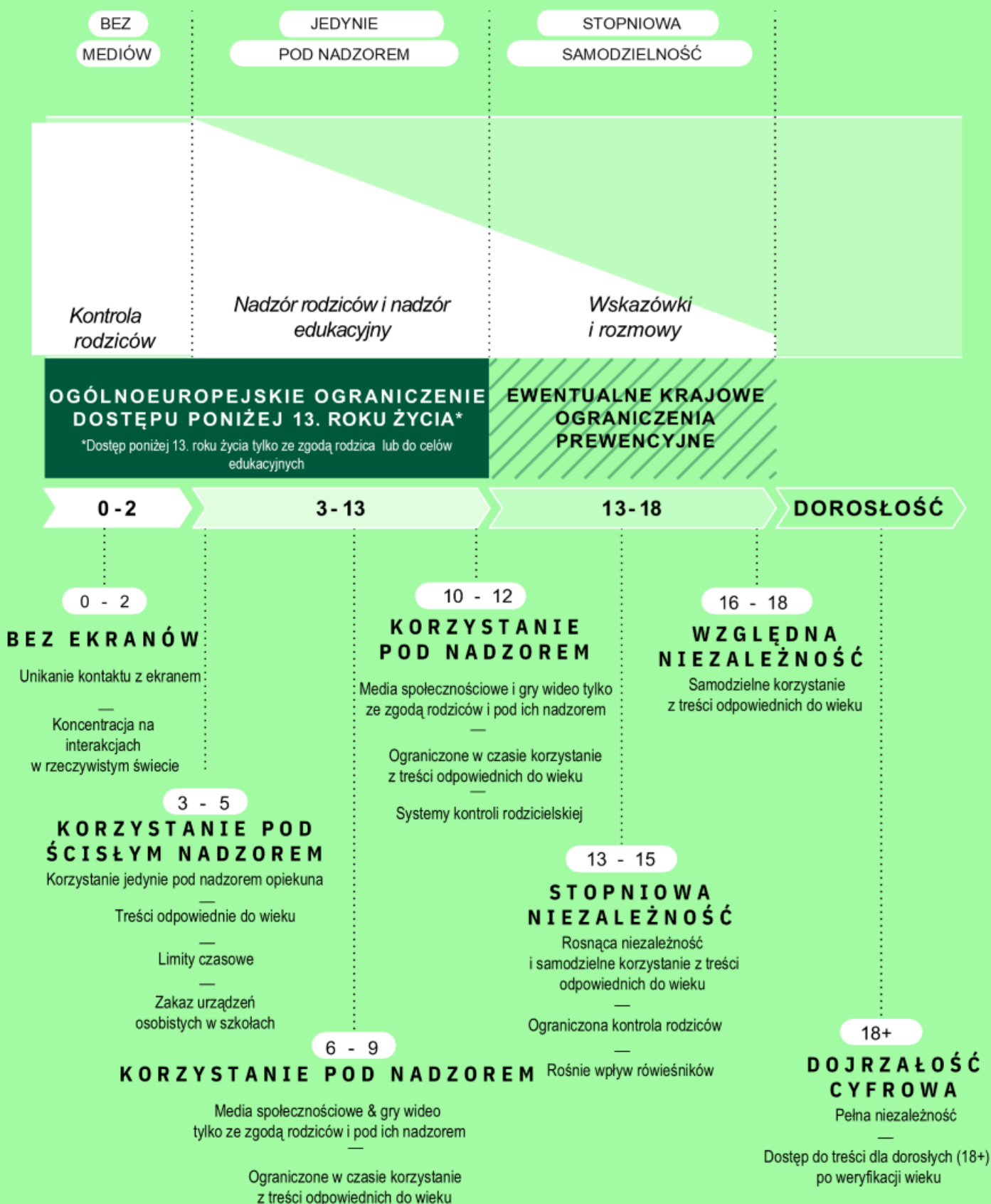
Nadrzędnym celem zaleceń zawartych w niniejszym sprawozdaniu, opartych na podejściu uwzględniającym rozwój dzieci i nastolatków oraz odzwierciedlających sześć podstawowych zasad, jest zrównoważenie konieczności ochrony dzieci i nastolatków w internecie z ich prawem do uczestnictwa w mediach społecznościowych+ i korzystania z oferowanych przez nie możliwości.

Zalecenia dotyczące odpowiedniego do wieku korzystania z mediów społecznościowych i innych usług cyfrowych

- 1. 0–2 lat: Unikanie ekranów i mediów społecznościowych+.** Unikanie intensywnego korzystania z ekranów we wczesnym dzieciństwie nie oznacza całkowitego zakazu. Podejście takie uznaje natomiast potrzeby rozwojowe dzieci w zakresie przywiązania, rozwoju sensorycznego i wczesnej nauki mówienia. Rodzice i opiekunowie powinni dawać pierwszeństwo bezpośrednim interakcjom i świadomie korzystać z urządzeń cyfrowych na własne potrzeby, aby oferować pozytywny wzór do naśladowania i uniknąć „technoferencji”. Podejście to jest zgodne z zaleceniami Światowej Organizacji Zdrowia dotyczącymi kształtowania się przywiązania emocjonalnego oraz zapobiegania zaburzeniom w rozwoju neurobiologicznym i poznawczym dzieci i problemom ze zdrowiem fizycznym (np. ze wzrokiem).
- 2. 3–12 lat: Korzystanie z odpowiednich do wieku mediów społecznościowych+ i urządzeń pod nadzorem.** Nie należy pozwalać dzieciom na korzystanie z urządzeń internetowych bez nadzoru. Szkoły powinny zapewnić infrastrukturę do nadzorowanego i ograniczonego korzystania z urządzeń do celów edukacyjnych, wspierając nabywanie umiejętności cyfrowych i umiejętności korzystania z mediów, rozwijanie odporności emocjonalnej i krytycznej refleksji nad zagrożeniami. Rodzice i opiekunowie powinni nadzorować i wspierać stopniowe nabywanie samodzielności cyfrowej poprzez media społecznościowe i inne usługi cyfrowe odpowiednie do wieku. Powinni oni również prowadzić regularne rozmowy z dziećmi na temat potencjalnych korzyści i zagrożeń związanych z interakcjami małoletnich w internecie. Zarówno opiekunowie, jak i nauczyciele powinni nadal zachęcać dzieci w tym wieku do udziału w aktywnościach poza internetem.
- 3. 13–18 lat: Coraz bardziej samodzielne korzystanie z mediów społecznościowych+ odpowiednich do wieku.** W wieku od 13 do 18 lat nastolatki powinny mieć dostęp wyłącznie do odpowiednich do ich wieku i „domyślnie bezpiecznych” mediów społecznościowych i innych usług cyfrowych, w których aktywnie wprowadzono kluczowe zabezpieczenia (np. ograniczenia dotyczące systemów niekończącego się przewijania treści i systemów rekomendacji). Do czasu opracowania tych „domyślnie bezpiecznych” mediów społecznościowych i innych usług cyfrowych podstawowe znaczenie ma

indywidualna, odpowiednia do wieku kontrola rodzicielska i nadzór. Można rozważyć dodatkowe środki zabezpieczające ze strony organów regulacyjnych. Ponieważ nastolatki powyżej 16 roku życia dążą do większej samodzielności cyfrowej, zagrożenia związane z narażeniem na szkodliwe treści w internecie są w ich przypadku nadal aktualne. W związku z tym rodzice i opiekunowie powinni kontynuować rozmowy z małoletnimi na temat ich doświadczeń w internecie. Nastolatki powinny mieć uprzywilejowany dostęp do usług wsparcia i systemów zgłaszania skarg, a jednocześnie powinny korzystać z sieci wzajemnego wsparcia promujących odpowiedzialne korzystanie z mediów społecznościowych i innych usług cyfrowych.

Korzystanie z mediów społecznościowych+ przez osoby małoletnie zgodnie z wiekiem



Zalecenia dotyczące ochrony dzieci i nastolatków w internecie

- **Zaproponowanie zharmonizowanego ogólnounijnego ograniczenia dostępu do mediów społecznościowych i innych usług cyfrowych dla dzieci poniżej 13 roku życia.**

Niezbędne jest zharmonizowane ogólnounijne ograniczenie dostępu do mediów społecznościowych i innych usług cyfrowych, w tym wirtualnych asystentów AI, dla dzieci poniżej 13 roku życia. Zharmonizowane ograniczenie dostępu ułatwiłoby wdrożenie obowiązku potwierdzania wieku, w sposób proporcjonalny i zgodny z przysługującymi prawami, oraz zachęciłoby dostawców mediów społecznościowych i innych usług cyfrowych do uwzględniania bezpieczeństwa już na etapie projektowania. Dzieci poniżej 13 roku życia powinny mieć ograniczony czasowo dostęp do odpowiednich dla danego wieku środowisk mediów społecznościowych+ wyłącznie za zgodą i pod nadzorem rodziców lub w kontekstach edukacyjnych. Od 13 roku życia nastolatki powinny móc coraz bardziej samodzielnie korzystać z odpowiednich do wieku i bezpiecznych mediów społecznościowych i innych usług cyfrowych.

Zharmonizowane przepisy dotyczące ogólnounijnego minimalnego wieku 13 lat przyczyniłyby się do właściwego funkcjonowania jednolitego rynku dzięki zapewnieniu jednolitych ram, do których musieliby zastosować się usługodawcy. Harmonizacja przepisów ułatwiłaby ich egzekwowanie i nadzór ze strony organów regulacyjnych zarówno na szczeblu krajowym, jak i unijnym. Zapewniłaby ona również wszystkim małoletnim w całej UE taki sam poziom ochrony w internecie, niezależnie od aspektów społeczno-gospodarczych, kulturowych i krajowych.

- **Wprowadzenie skutecznych systemów potwierdzania wieku w celu sprawdzania wieku oraz wspieranie podejścia uwzględniającego bezpieczeństwo już na etapie projektowania i odpowiedniego do wieku, aby chronić małoletnich w internecie i wzmacniać ich pozycję.**

Metody potwierdzania wieku – zarówno weryfikacja wieku, jak i szacowanie wieku – muszą być proporcjonalne i zgodne z minimalnymi wymogami, w szczególności w odniesieniu do praw podstawowych użytkowników, w tym praw dziecka i powiązanych gwarancji. Każda metoda stosowana do sprawdzania wieku powinna być zgodna z najwyższymi standardami prywatności i ochrony danych i nie powinna prowadzić do przetwarzania dokumentów tożsamości ani danych biometrycznych do celów szacowania wieku. Należy wdrożyć normy techniczne, takie jak „dowód z wiedzą zerową”, w celu zapewnienia, aby ani platforma, która powinna zweryfikować wiek, ani dostawca rozwiązania służącego do weryfikacji wieku nie otrzymywali żadnych informacji, które mogłyby umożliwić śledzenie lub identyfikację użytkownika.

Metody potwierdzania wieku powinny prawidłowo określać wiek lub grupę wiekową oraz powinny być łatwe i wiarygodne do stosowania w praktyce, w rzeczywistych warunkach. Metody te powinny być solidne, aby zapobiegać obchodzeniu przepisów i zagrożeniom w zakresie cyberbezpieczeństwa, inkluzywne (i niedyskryminujące) i dostępne w równym stopniu dla wszystkich, którzy muszą z nich korzystać. Dostawcy mediów społecznościowych i innych usług cyfrowych muszą wywiązać się z obowiązku zapobiegania narażeniu małoletnich na ryzykowne usługi lub podszywanie się użytkowników pod dzieci i nastolatki.

- **Rozszerzenie i harmonizacja przepisów dotyczących kluczowych zabezpieczeń przy projektowaniu mediów społecznościowych i innych usług cyfrowych.**

W mediach społecznościowych i innych usługach cyfrowych należy wprowadzić jasne zabezpieczenia uwzględniające bezpieczeństwo już na etapie projektowania i odpowiednie do wieku (np. potencjalne ograniczenia niekończącego się przewijania treści, automatycznego odtwarzania, powiadomień push i problematycznych spersonalizowanych systemów rekomendacji). Aby przeciwdziałać uzależniającym projektom, zwodniczym interfejsom, niechcianym kontaktom i szkodliwym bańkom z toksycznymi treściami (ang. rabbit holes), domyślne ustawienia ochronne powinny stanowić integralną część mediów społecznościowych i innych usług cyfrowych. Rozszerzenie i harmonizacja przepisów dotyczących kluczowych zabezpieczeń zapewniłyby pewność i jednolitość w całym środowisku mediów społecznościowych+. Ze względu na szybki rozwój technologii wszelkie przepisy dotyczące kluczowych zabezpieczeń powinny umożliwiać ich dostosowywanie, aby stale uwzględniać nowe szkodliwe cechy projektowe.

- **Przeniesienie ciężaru dowodu na dostawców mediów społecznościowych i innych usług cyfrowych w celu wykazania, że ich produkty i usługi są bezpieczne dla małoletnich.**

Szczególne ograniczenia wiekowe powinny mieć zastosowanie do czasu wprowadzenia przez media społecznościowe i innych dostawców usług cyfrowych kluczowych zabezpieczeń projektowych chroniących dzieci i nastolatki. Dopóki dostawcy nie wykażą istnienia tych bezpiecznych i odpowiednich do wieku funkcji, a tym samym nie zastosują się do środków unijnych i krajowych, nie powinni mieć możliwości oferowania swoich usług małoletnim. W przypadku gdy istnieje wersja „domyślnie bezpieczna”, funkcje nieodpowiednie dla danego wieku (funkcje dla dorosłych) powinny być aktywowane dopiero po skutecznym potwierdzeniu wieku.

- **Wzmocnienie zdolności w zakresie egzekwowania przepisów i oceny.**

Z uwagi na to, że obecnie w odniesieniu do bezpieczeństwa dzieci w internecie zastosowanie mają różne przepisy (akt o usługach cyfrowych, RODO, akt w sprawie AI itp.), organy odpowiedzialne za monitorowanie stosowania poszczególnych ram prawnych powinny zintensyfikować współpracę i wymianę informacji. Ma to kluczowe znaczenie dla wyeliminowania niespójności oraz dla zapewnienia spójnego, przewidywalnego i skutecznego otoczenia prawnego, którego fundament stanowi ochrona praw podstawowych. Komisja Europejska powinna przeanalizować, jakie mechanizmy umożliwiają sprawną współpracę między organami nadzorczymi, co pozwoli wykorzystać istniejące już struktury egzekwowania prawa. Ponadto należy ocenić, czy organy regulacyjne odpowiedzialne za egzekwowanie prawa i ocenę potrzebują dodatkowych zasobów lub czy powinny zostać poddane restrukturyzacji. Należy rozważyć działania mające na celu wzmocnienie roli społeczeństwa obywatelskiego w egzekwowaniu prawa oraz jego wkładu w zdolności w zakresie egzekwowania prawa, w tym za pośrednictwem istniejących struktur. Egzekwowanie przepisów powinno mieć charakter uzupełniający; należy unikać działań o sprzecznym charakterze.

- **Szybkie przyjęcie środków i zagwarantowanie, aby dostawcy mediów społecznościowych i innych usług cyfrowych mieli jasne obowiązki w zakresie zapobiegania niegodziwemu traktowaniu dzieci w celach seksualnych w internecie, w tym w ramach łączności interpersonalnej, wykrywania, zgłaszania i blokowania takiego traktowania.**

W związku z wygaśnięciem rozporządzenia tymczasowego ustanawiającego przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i zwalczanie takiego traktowania (rozporządzenie tymczasowe w sprawie niegodziwego traktowania dzieci w celach seksualnych) powstała luka, którą należy szybko wyeliminować. Współprawodawcy UE powinni szybko przyjąć proponowane rozporządzenie długoterminowe w celu zapobiegania niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczania. Ponad 80 proc. dochodzeń w sprawie niegodziwego traktowania dzieci w celach seksualnych wszczyna się na podstawie zgłoszeń przekazywanych przez dostawców mediów społecznościowych i innych usług cyfrowych. Same dzieci często są zbyt wystraszone, aby zgłaszać przypadki niegodziwego traktowania. Wykrywanie materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych, w tym w ramach łączności interpersonalnej, to często jedyny sposób na powstrzymywanie niegodziwego traktowania.

- **Państwa członkowskie mogą wprowadzać dodatkowe zapobiegawcze ograniczenia dostępu do mediów społecznościowych i innych usług cyfrowych od 13 roku życia.**

Dodatkowe zapobiegawcze ograniczenia dostępu powinny uzupełniać ogólnounijne ograniczenie dostępu do mediów społecznościowych i innych usług cyfrowych dla osób poniżej 13 roku życia. Nastolatki mogą mieć dostęp wyłącznie do takiego środowiska mediów społecznościowych+, które jest bezpieczne pod względem treści i cech projektowych, dostosowane do wieku i opracowane z myślą o ich prawach i potrzebach. Państwa członkowskie różnią się uwarunkowaniami historycznymi i krajowymi, niektóre państwa mogą więc preferować próg wiekowy wyższy niż 13 lat. Wszystkie dodatkowe krajowe ograniczenia dostępu o charakterze zapobiegawczym powinny podlegać ciągłej ocenie, a w miarę możliwości ponownym ocenom po tym, jak media społecznościowe i inne usługi cyfrowe staną się domyślnie bezpieczne dla dzieci i nastolatków.

- **Wzmocnienie egzekwowania przepisów dotyczących dostępu naukowców do danych oraz kontroli danych.**

Akt delegowany z lipca 2025 r., przyjęty na podstawie art. 40 aktu o usługach cyfrowych, stworzył, zasadniczo, zweryfikowanym badaczom nowe możliwości dostępu do danych z platform internetowych. Dane te można wykorzystywać do przeprowadzania badań przyczyniających się do wykrywania, identyfikowania i zrozumienia ryzyk systemowych, a także do dokonania oceny środków zmniejszających ryzyko, które promują bezpieczeństwo dzieci w internecie.

To, czy te nowe możliwości zaowocują konkretnymi wynikami, zależy od przestrzegania przepisów przez dostawców mediów społecznościowych i innych usług cyfrowych oraz od skutecznego egzekwowania przepisów przez organy regulacyjne. Jest to również uzależnione od tego, jak szeroki będzie zakres objętych usług, a także od jakości i ciągłości udostępnionych danych. Po zgromadzeniu przez badaczy wstępnych doświadczeń na podstawie aktu delegowanego Komisja powinna ocenić skuteczność operacyjną wymogów dotyczących dostępu do danych i kontroli danych, o których mowa w art. 40. Ma to kluczowe znaczenie dla zapewnienia, aby platformy internetowe podejmowały działania następcze w związku z wnioskami o dostęp do danych na potrzeby oceny zgodności, oceny ryzyka oraz na potrzeby badań.

Obowiązki w zakresie dostępu do danych są nie tylko kluczowym elementem określonego w akcie o usługach cyfrowych zestawu narzędzi na rzecz przejrzystości, lecz także elementem szeroko pojętego zakresu obowiązków dostawców mediów społecznościowych i innych usług cyfrowych w zakresie ograniczania ryzyka. Należy także zachęcać mniejsze platformy do umożliwiania naukowcom dostępu do danych, biorąc pod uwagę zagrożenia, jakie platformy takie stwarzają dla małoletnich, oraz rolę, jaką niezależna kontrola pełni w przeciwdziałaniu tym zagrożeniom. Normą podczas wdrażania art. 40 powinno

być stosowanie zasad FAIR⁴ w odniesieniu do zarządzania danymi naukowymi i opieki nad nimi.

Zalecenia służące wzmocnieniu pozycji dzieci i nastolatków w internecie

- **Rozszerzenie bezpiecznych możliwości aktywnego udziału małoletnich w kształtowaniu środowiska mediów społecznościowych+.**

Dzieci i nastolatki powinny dysponować faktycznymi możliwościami aktywnego kształtowania prawodawstwa, polityk i inicjatyw edukacyjnych promujących bezpieczeństwo dzieci w internecie i wzmocnienie ich pozycji w internecie. W pracach tych należy szerzej stosować narzędzia pozwalające na uczestnictwo dzieci i młodzieży. Mówiąc dokładniej, należy włączać dzieci w proces wspólnego opracowywania polityki bezpieczeństwa, programów szkoleniowych, ocen i wytycznych. Należy nieprzerwanie monitorować i analizować wprowadzone środki, aby móc ocenić ich wpływ na bezpieczeństwo i prawa dzieci.

Procesy przewidujące uczestnictwo powinny zapewnić, aby dzieci otrzymywały jasne informacje, rozumiały, jak wykorzystywane będzie ich wkład, oraz otrzymywały informacje zwrotne dotyczące rezultatów. Należy podjąć szczególne wysiłki i włączyć w te działania dzieci z grup defaworyzowanych, marginalizowanych i szczególnie wrażliwych. Wszystkim działaniom służącym uczestnictwu, w które zaangażowane zostaną dzieci, powinny towarzyszyć odpowiednie środki ochronne.

- **Wzmocnienie mechanizmów rozpatrywania skarg oraz praw konsumentów w odniesieniu do dzieci i nastolatków.**

Dostawcy mediów społecznościowych i innych usług cyfrowych powinni priorytetowo traktować w procedurach moderowania treści wszelkie zgłoszenia i skargi ze strony dzieci i nastolatków. Należy wzmocnić obowiązki dostawców wynikające z istniejących ram, aby móc odpowiednio finansować telefony zaufania i mechanizmy składania skarg. Mechanizmy te muszą być dostosowane do wieku, przyjazne dla użytkownika, dostępne i skuteczne, muszą ponadto chronić prywatność.

- **Upowszechnianie działań w zakresie edukacji cyfrowej i umiejętności cyfrowych skierowanych do małoletnich, rodziców i opiekunów, nauczycieli oraz wychowawców.**

⁴ Zasady FAIR dotyczące zarządzania danymi naukowymi i opieki nad nimi zaprezentowano w 2016 r. w publikacji w czasopiśmie „Scientific Data”. Celem wspomnianych zasad jest udoskonalenie infrastruktury wspierającej ponowne wykorzystywanie danych naukowych poprzez zwiększenie zdolności maszyn i osób fizycznych do wyszukiwania i wykorzystywania danych. Zob.: Wilkinson, M.D., et al. (2016). [Zasady FAIR dotyczące zarządzania danymi naukowymi i opieki nad nimi](#). Scientific Data, 3.

Edukacja cyfrowa i umiejętności cyfrowe powinny być uwzględniane na wszystkich poziomach edukacji i traktowane jako kluczowe umiejętności podstawowe małych, rodziców i nauczycieli. Powszechna edukacja cyfrowa powinna uwzględniać kwestie dobrostanu cyfrowego.

Odpowiednia edukacja powinna umożliwiać dzieciom i nastolatkom krytyczną ocenę informacji i źródeł internetowych, a także rozpoznawanie technik manipulacji, w tym dezinformacji, deepfejków oraz targetowania. Powinna też pozwalać małym, ich rodzicom i nauczycielom zrozumieć, w jaki sposób tworzy się i udostępnia treści cyfrowe oraz w jaki sposób algorytmy kształtują to, co użytkownicy widzą i czego doświadczają w świecie mediów społecznościowych+.

Ustrukturyzowana edukacja w zakresie bezpieczeństwa w internecie powinna prowadzić do nabywania praktycznych umiejętności w zakresie ochrony danych osobowych, zarządzania ustawieniami prywatności, utrzymania bezpiecznych tożsamości cyfrowych oraz identyfikowania zagrożeń, w szczególności w mediach społecznościowych, w komunikatorach i w środowisku gier. Umiejętności te należy rozwijać stopniowo, począwszy od podstawowych nawyków w zakresie bezpieczeństwa, a skończywszy na bardziej złożonych kwestiach takich jak zrozumienie śladu cyfrowego, zgody i ryzyka związanego z funkcjonowaniem platform. Należy promować higienę cyfrową za pomocą wytycznych dotyczących równowagi, zarządzania uwagą i rozpoznawania nadmiernych lub szkodliwych wzorców korzystania.

- **Rozszerzanie możliwości i odpowiedniej infrastruktury w celu promowania aktywności poza internetem.**

Państwa członkowskie i władze lokalne powinny nie tylko utrzymać, lecz także rozszerzać dostęp do przystępnych cenowo możliwości uprawiania sportu, sztuki, uczęszczania do klubów młodzieżowych, korzystania z bibliotek i przestrzeni społecznościowych, zachęcając w ten sposób do zdrowej aktywności poza internetem i tworząc atrakcyjne alternatywy wobec nadmiernego korzystania z ekranów przez małych. Powyższe powinno obejmować inwestycje w kreowanie bezpiecznego, integracyjnego i dostosowanego do wieku środowiska, w którym małe mogą nawiązywać kontakty, uczyć się, grać i budować pozytywne relacje w obrębie swoich społeczności.

- **Promowanie współdziałania przy tworzeniu wytycznych dla rodziców.**

UE i państwa członkowskie powinny – wspólnie ze stowarzyszeniami rodziców – promować opracowanie wytycznych dla rodziców. Wytyczne mogłyby zawierać

jasne i przystępne porady mające na celu wzmocnienie pozycji rodziców i opiekunów we wspieraniu bezpiecznego, odpowiedzialnego i pozytywnego zaangażowania małoletnich w środowisko mediów społecznościowych+. Wytyczne powinny zawierać praktyczne porady dotyczące kluczowych obszarów, w tym bezpieczeństwa i prywatności w internecie, dobrostanu cyfrowego, etycznego i odpowiedzialnego korzystania z mediów cyfrowych oraz dostępu do wsparcia.

- **Zapewnienie dostatecznego finansowania publicznego i wspólnych norm na potrzeby organizacji społeczeństwa obywatelskiego i wzajemnego doradztwa.**

UE i państwa członkowskie powinny zapewnić, aby centra bezpieczniejszego internetu i organizacje społeczeństwa obywatelskiego prowadzące porównywalną działalność w dalszym ciągu otrzymywały dostateczne środki finansowe oraz aby ich praca opierała się na wspólnych normach opracowanych przez ekspertów. Ma to zasadnicze znaczenie dla utrzymania i dalszego rozwoju ich działań, w tym informowania, szkolenia i oferowania usług wsparcia. Finansowanie publiczne ma decydujące znaczenie dla zagwarantowania niezależności i spójności.

Finansowanie powinno również wspierać dalszy rozwój wzajemnego doradztwa, telefonów zaufania, infolinii, zasobów edukacyjnych, kampanii informacyjnych oraz działań w zakresie budowania zdolności. Należy przeznaczyć dodatkowe inwestycje na zwiększenie widoczności, dostępności i zasięgu wspomnianych podmiotów, w tym z korzyścią dla małoletnich znajdujących się w trudnej sytuacji, a także na wspieranie inicjatyw promujących bezpieczniejsze środowisko mediów społecznościowych+.

- **Udostępnienie długoterminowego finansowania na rzecz prowadzonych na dużą skalę europejskich badań wzdłużnych oraz dalsze wspieranie badań randomizowanych z grupą kontrolną.**

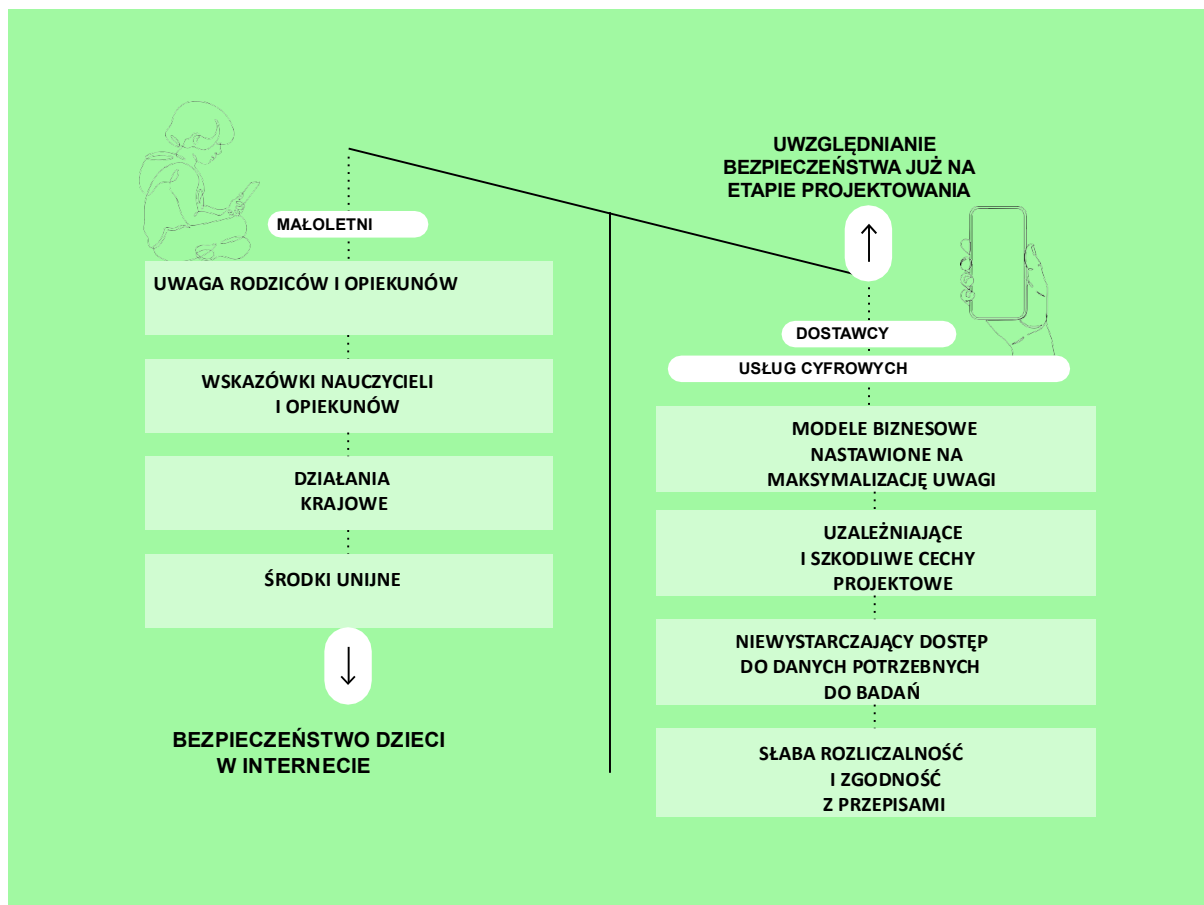
Inspiracją dla prowadzonych na dużą skalę europejskich badań wzdłużnych związanych z bezpieczeństwem dzieci w internecie mogłyby być badania takie jak północnoamerykańskie badanie dotyczące kognitywnego rozwoju mózgu osób młodocianych (ang. *Adolescent Brain Cognitive Development, ABCD*)⁵.

⁵ Badanie ABCD jest największym długoterminowym badaniem rozwoju mózgu i zdrowia dzieci w Stanach Zjednoczonych. W ramach badania obserwuje się rozwój behawioralny ponad 11 tys. dzieci w wieku od 9 do 10 lat poprzez okres dojrzewania, aż do wczesnej dorosłości. Zgromadzone dane umożliwią stworzenie podstawowych norm rozwoju mózgu nastolatków oraz zbadanie wpływu płci biologicznej, płci społeczno-kulturowej, snu, aktywności fizycznej i czasu spędzanego przed ekranem na ich rozwój. Wyniki badania pomogą również zrozumieć rozwój problemów zdrowia psychicznego w okresie dojrzewania oraz ich związek z nadużywaniem substancji psychoaktywnych.

Dostępność europejskich danych zgromadzonych w prowadzonych na dużą skalę badaniach wzdłużnych (obejmujących okres dziesięciu lat lub dłuższy) jest istotna z punktu widzenia wspierania rozwojowego i neurobiologicznego podejścia do bezpieczeństwa dzieci w internecie. Takie badania pomogłyby wyeliminować luki w ustaleniach w europejskim kontekście, które są w dużej mierze ustaleniami skorelowanymi, a które dotyczą wpływu korzystania z mediów społecznościowych i innych usług cyfrowych na rozwój małoletnich, ich zdrowie fizyczne i psychiczne oraz szkodliwych skutków, na jakie narażeni są małoletni w internecie.

Decydujące znaczenie dla wzmocnienia bazy dowodowej na potrzeby polityki mają badania randomizowane z grupą kontrolną. Finansowanie badań naukowych powinno wyraźnie wspierać podejścia rozwojowe i psychopatologiczne badające podatność małoletnich na zagrożenia w internecie, na którą wpływ mają czynniki społeczne i indywidualne w okresie dzieciństwa i dojrzewania.

Rysunek 2: Równowaga w ekosystemie: bezpieczeństwo na etapie projektowania w środowisku mediów społecznościowych+



Bezpieczeństwo w internecie

WSKAZÓWKI DLA DZIECI I NASTOLATKÓW



Poznaj swoje prawa – pamiętaj, że w internecie masz prawo do bezpieczeństwa i szacunku.



Bądź w internecie miły/miła dla innych – media społecznościowe i gry powinny być dla każdego pozytywnym doświadczeniem. Traktuj innych z szacunkiem, tak jak chcesz, aby traktowano Ciebie.



Zastanów się, zanim umieścisz coś w internecie – zdjęcia, wideo, komentarze mogą zostać w sieci na zawsze. Dziel się tylko tym, co nie sprawi, że w przyszłości będziesz się wstydzić.



Chroń swoje dane osobowe – nie udostępniaj prywatnych danych, takich jak Twoje pełne imię i nazwisko, adres, szkoła, numer telefonu, hasła czy miejsce, w którym aktualnie przebywasz.



Pamiętaj, że AI to narzędzie, nie żywy człowiek – AI może popełniać błędy, tworzyć nieprawdziwe informacje oraz fałszywe zdjęcia, nagrania wideo, głosy i wiadomości.



Zanim zaufasz lub coś udostępnisz: sprawdź – nie wszystko w internecie jest prawdziwe. Zawsze krytycznie przyjmuj informacje, zwłaszcza historie, filmy lub wiadomości, które są zaskakujące, a przed udostępnieniem sprawdź wiarygodne źródła.



Rozpoznawaj zagrożenia – wstrzymaj się i przemyśl dziwną prośbę „znajomego znajomych”, propozycję, która brzmi zbyt dobrze, by była prawdziwa, lub wiadomość, której autor próbuje wymusić na Tobie decyzję.



Nie przyjmuj zdjęć i zaproszeń do rozmowy od obcych – jeżeli masz wątpliwości co do wieku lub tożsamości danej osoby, poproś dorosłego o sprawdzenie, z kim masz do czynienia (lub powiedz tej osobie, że Twoja mama /Twój tata są z Tobą, i sprawdź reakcję).



Korzystaj z ustawień prywatności i bezpieczeństwa – Twoje konta powinny być prywatne, korzystaj z mocnych haseł i w miarę możliwości włączaj dodatkowe zabezpieczenia.



Nie udostępniaj prywatnych zdjęć – nigdy nie udostępniaj intymnych zdjęć ani nagrań, nawet jeżeli ktoś wywiera na Ciebie nacisk (szczególnie jeżeli nie masz jeszcze 18 lat). Jeżeli je udostępnisz, stracisz nad nimi kontrolę.



Blokuj, zgłaszaj i zapisuj dowody – jeżeli ktoś w internecie nęka Cię, oszukuje, grozi Ci lub sprawia, że czujesz się niekomfortowo, zgłoś i zablokuj tę osobę, zachowaj zrzuty ekranu lub wiadomości.



Jeżeli masz wrażenie, że coś jest nie tak, powiedz o tym dorosłej osobie, której ufasz – nie powinno być Ci głupio, prośba o pomoc nie sprawi, że będziesz mieć kłopoty.



Pomóż w tworzeniu bezpiecznego internetu – naucz się, jak funkcjonują aplikacje, gry, strony internetowe, algorytmy i AI; pomóż także innym zachować bezpieczeństwo.



Wykorzystaj swój głos – zaangażuj się i weź udział w kształtowaniu przyszłości cyfrowego świata.



Bezpieczeństwo w internecie

WSKAZÓWKI DLA RODZICÓW I OPIEKUNÓW



Pomóż swojemu dziecku w nabyciu zdrowych nawyków związanych z czasem spędzaniem przed ekranem: ograniczaj ten czas: dzieci w wieku od 0 do 2 nie powinny w ogóle korzystać z ekranu, dzieci w wieku do 10–12 lat powinny mieć ograniczenia i korzystać z ekranu pod Twoim nadzorem. W przypadku nastolatków w wieku od 13 do 18 lat należy przedyskutować ograniczenia w korzystaniu z ekranów, aby młodzi ludzie mieli dostatecznie dużo czasu na naukę i bezpośrednie kontakty z przyjaciółmi.



Sprawdź, czy aplikacje i gry są dostosowane do wieku Twojego dziecka.



W przypadku młodszych dzieci (do 12 roku życia), konsole i urządzenia powinny być używane wyłącznie w obecności osoby dorosłej.



Nie pozwalaj na korzystanie z urządzeń w łazience, w sypialni lub podczas posiłków.



Zwracaj uwagę na ton rozmów dzieci w internecie i podczas gier komputerowych. Bądź wyczulony/wyczulona na sygnały ostrzegawcze.



Spędzaj czas z dziećmi w internecie – poproś swoje dziecko, aby obejrzało z Tobą swoje ulubione treści.



Nie krytykuj tego, co ogląda Twoje dziecko – pomóż mu wypracować swój własny osąd (zorientujesz się przy tej okazji, co sugeruje jego algorytm).



Zachęcaj swoje dziecko do rozmowy z Tobą, gdy zaniepokoi je coś w internecie – zapewnij je, że pomożesz, że nie będziesz obwiniać ani karać i że nie zabierzesz urządzenia.



Kontynuuj rozmowy o bezpieczeństwie w internecie również wtedy, gdy Twoje dziecko rośnie, gdy ma 16, 18 lat, a nawet więcej.



Unikaj dzielenia się treściami dotyczącymi Twojego dziecka – przemyśl dokładnie, zanim umieścisz w internecie zdjęcia lub wideo, na których są Twoje dzieci. Obce osoby i sztuczna inteligencja mogą wykorzystywać takie materiały na wiele sposobów.



Dawaj dobry przykład – nie spędzaj nadmiernie dużo czasu przed swoim urządzeniem, gdy Twoje dzieci są w pobliżu. Poświęć im uwagę, na którą zasługują, i nie przeocz ważnych chwil i ważnych rozmów ze swoim dzieckiem.



Wszystkie zalecenia współprzewodniczących według rozdziałów

Rozdział 1: Rozwojowe podejście do bezpieczeństwa dzieci w internecie

1. Opracowanie i wdrożenie środków ochrony dzieci w internecie, które są dostosowane do wieku
2. Zapewnienie małoletnim bezpiecznej przestrzeni w internecie
3. Wzmocnienie pozycji małoletnich i osób je wspierających
4. (0–2 lata) – Zwiększenie wiedzy opiekunów na temat znaczenia, jakie dla rozwoju ma bezpośrednia interakcja międzyludzka, począwszy od wczesnego dzieciństwa
5. (0–2 lata) – Unikanie korzystania z mediów społecznościowych i innych usług cyfrowych oraz zapewnienie, aby ekspozycja na ekrany była minimalna, zwłaszcza w przypadku dzieci poniżej 3 roku życia
6. (0–2 lata) – Ograniczenie rozpowszechniania na profilach w mediach społecznościowych danych dotyczących dzieci
7. (3 do 12 lat) – Zapewnienie, by dzieci korzystały z internetu na określonych z góry zasadach i pod nadzorem dorosłego
8. (3 do 12 lat) – Oferowanie dzieciom i środowiskom je wspierającym wysokiej jakości edukacji cyfrowej i edukacji na temat dobrostanu cyfrowego
9. (13 do 18 lat) – Zapewnienie, by nastolatki zaczynały stopniowo samodzielnie korzystać z internetu

Rozdział 2: Dowody dotyczące zagrożeń, na jakie narażeni są małoletni w internecie

10. Opieranie się w obszarach niedostatecznie zbadanych na dowodach, aby wzmocnić proces kształtowania polityki opartej na dowodach
11. Media społecznościowe i inne usługi cyfrowe powinny aktywnie wykorzystywać niezależną wiedzę akademicką w opracowywaniu strategii oraz narzędzi ograniczających ryzyko
12. Udostępnienie długoterminowego finansowania na rzecz prowadzonych na dużą skalę europejskich badań wzdlużnych oraz dalsze wspieranie badań randomizowanych z grupą kontrolną

13. Inwestowanie w bezpieczną, wspólną europejską infrastrukturę badawczą, która pozwoli na bezpieczny dostęp do danych osób małoletnich
14. Wzmocnienie egzekwowania przepisów dotyczących dostępu naukowców do danych oraz kontroli danych

Rozdział 3: Ochrona małoletnich w szybko zmieniającym się środowisku mediów społecznościowych+

15. Zaproponowanie zharmonizowanego ogólnounijnego ograniczenia dostępu do mediów społecznościowych i innych usług cyfrowych dla osób małoletnich poniżej 13 roku życia
16. Wprowadzenie skutecznych systemów weryfikowania wieku oraz wzmocnienia tym samym podejścia uwzględniającego bezpieczeństwo na etapie projektowania i dostosowanego do wieku, co pozwoli chronić małoletnich w internecie i wzmocnić ich pozycję
17. Rozszerzenie i zharmonizowanie przepisów dotyczących kluczowych elementów bezpieczeństwa na etapie projektowania mediów społecznościowych i innych usług cyfrowych
18. Przeniesienie ciężaru dowodu na dostawców mediów społecznościowych i innych usług cyfrowych, tak aby musieli oni wykazywać, że ich produkty i usługi są bezpieczne dla małoletnich
19. Wzmocnienie zdolności w zakresie egzekwowania przepisów i oceny
20. Szybkie przyjęcie środków i zagwarantowanie, aby dostawcy mediów społecznościowych i innych usług cyfrowych mieli jasne obowiązki w zakresie zapobiegania niegodziwemu traktowaniu dzieci w celach seksualnych w internecie, w tym w ramach łączności interpersonalnej, wykrywania, zgłaszania i blokowania takiego traktowania
21. Państwa członkowskie mogą wprowadzać dodatkowe zapobiegawcze ograniczenia dostępu do mediów społecznościowych i innych usług cyfrowych od 13 roku życia
22. Wzmocnienie polityki ochrony konsumentów celem ochrony małoletnich w internecie
23. Nieprzerwane monitorowanie i analizowanie wpływu wdrażanych środków
24. Przetwarzając dane dzieci na podstawie RODO, dostawcy mediów społecznościowych i innych usług cyfrowych powinni przede wszystkim uwzględniać najlepszy interes dziecka
25. Zapewnienie skutecznego wdrożenia dyrektywy w sprawie odpowiedzialności za produkty

Rozdział 4: Wzmocnienie pozycji małoletnich, aby mogli bezpiecznie poruszać się w świecie cyfrowym

26. Rozszerzenie bezpiecznych możliwości aktywnego udziału małoletnich w kształtowaniu środowiska mediów społecznościowych+
27. Wzmocnienie mechanizmów rozpatrywania skarg oraz praw konsumentów w odniesieniu do dzieci i nastolatków
28. Finansowanie i promowanie tworzenia mediów społecznościowych i innych usług cyfrowych i korzystania z mediów społecznościowych i innych usług cyfrowych, które są oparte na wartościach UE, i w obrębie których małoletni mogą bezpiecznie nawiązywać wzajemne relacje
29. Upowszechnianie działań w zakresie edukacji cyfrowej i umiejętności cyfrowych skierowanych do małoletnich, rodziców i opiekunów, nauczycieli oraz wychowawców
30. Rozszerzanie możliwości i odpowiedniej infrastruktury w celu promowania aktywności poza internetem
31. Promowanie współdziałania przy tworzeniu wytycznych dla rodziców
32. Udzielanie rodzicom i opiekunom nieprzerwanego wsparcia za pomocą najnowocześniejszych i aktualnych narzędzi kontroli i nadzoru
33. Zapewnienie dostatecznego finansowania publicznego i wspólnych norm na potrzeby organizacji społeczeństwa obywatelskiego i wzajemnego doradztwa
34. Przygotowanie systemów opieki zdrowotnej do diagnozowania i leczenia uzależnień oraz innych zaburzeń zdrowia psychicznego związanych z korzystaniem z mediów społecznościowych i innych usług cyfrowych
35. Wspieranie szkolenia nauczycieli pod kątem umiejętności cyfrowych i umiejętności korzystania z mediów oraz angażowanie rodziców
36. Promowanie kompetencji w zakresie AI jako integralnej części edukacji cyfrowej
37. Szkoły powinny zapewniać ustrukturyzowane możliwości poprawy zdrowia psychicznego i dobrostanu cyfrowego
38. W działaniach edukacyjnych należy zwrócić szczególną uwagę na grupy szczególnie wrażliwe
39. Inwestowanie w edukacyjną infrastrukturę cyfrową, która jest bezpieczna, solidna i godna zaufania i która pełni funkcje prewencyjne

Przypisy końcowe – Przedmowa

ⁱ Komisja Europejska (2026). [Cyfrowa dekada – Sprawozdanie z badania Eurobarometr – Luty – Marzec 2026 r.](#)

ⁱⁱ Duńska prezydencja, Rada Unii Europejskiej (2026 r.). [Deklaracja z Jutlandii w sprawie kształtowania bezpiecznego świata online dla małoletnich.](#)

ⁱⁱⁱ Parlament Europejski (2025 r.). [Ochrona nieletnich w internecie – Rezolucja Parlamentu Europejskiego z dnia 26 listopada 2025 r. w sprawie ochrony małoletnich w internecie \(2025/2060\(INI\)\).](#)

^{iv} Rada Europejska (2026 r.). [Konkluzje Rady Europejskiej](#) z dnia 19 marca 2026 r.

^v G7 (2026 r.). [Przywódcy apelują o bezpieczniejszą przestrzeń cyfrową dla małoletnich.](#)

^{vi} Szpital Dziecięcy w Filadelfii (2026 r.). [Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study \[Badanie przeprowadzone przez Szpital Dziecięcy w Filadelfii sugeruje, że same ograniczenia wiekowe nie usuną zagrożeń związanych ze smartfonami\].](#)
Dostęp: 12 lipca 2026 r.