Projekt z dnia 20 listopada 2026 r.

U S T A W A

z dnia …

o minimalnym wieku dostępu do internetowych serwisów społecznościowych

Rozdział 1

Przepisy ogólne

Art. 1. Ustawa określa:

1) obowiązki dostawców internetowych serwisów społecznościowych w zakresie dostępu małoletnich do usług;
2) zasady stosowania narzędzi służących do potwierdzania wieku;
3) zakres działań edukacyjnych związanych z funkcjonowaniem małoletnich w przestrzeni cyfrowej;
4) tryb postępowania w sprawie naruszenia obowiązków wynikających z ustawy;
5) administracyjne kary pieniężne za naruszenie obowiązków wynikających z ustawy.

Art. 2. Użyte w ustawie określenia oznaczają:

1) internetowy serwis społecznościowy – internetowy serwis społecznościowy w rozumieniu art. 2 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz. Urz. UE L 265 z 12.10.2022, str. 1 oraz Dz. Urz. UE L 2025/90024 z 10.01.2025);
2) profilowanie – profilowanie w rozumieniu art. 4 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

Art. 3. Małoletni osiąga minimalny wiek dostępu do internetowych serwisów społecznościowych po ukończeniu lat piętnastu.

Rozdział 2

Obowiązki dostawców internetowych serwisów społecznościowych

Art. 4. 1. Dostawca internetowego serwisu społecznościowego uniemożliwia osobie, która nie osiągnęła minimalnego wieku dostępu do internetowych serwisów społecznościowych:

1) założenie konta użytkownika w tym serwisie lub
2) uzyskanie dostępu do tego serwisu za pośrednictwem konta użytkownika utworzonego dla tej osoby lub innego konta użytkownika, do którego osoba ta mogłaby uzyskać dostęp

– jeżeli internetowy serwis społecznościowy spełnia przynajmniej jedną z przesłanek ryzyka dla prywatności i bezpieczeństwa określonych w ust. 2.

2. Przesłankami ryzyka dla prywatności i bezpieczeństwa, związanymi z internetowym serwisem społecznościowym, są:

1) umożliwianie użytkownikowi, posiadającemu konto użytkownika w tym serwisie, udostępnianie lub przekazywanie treści, w czasie rzeczywistym, nieokreślonej liczbie innych użytkowników;
2) umożliwianie użytkownikowi, posiadającemu konto użytkownika w tym serwisie, kontaktowanie się, komunikowanie się lub wchodzenie w innego rodzaju interakcje z innymi użytkownikami tego serwisu, nieznanymi temu użytkownikowi;
3) wykorzystywanie systemu rekomendacji opartego na profilowaniu osób fizycznych;
4) stosowanie środków mających na celu zachęcenia użytkownika do długotrwałego i nieprzerwanego korzystania z usług tego serwisu.

Art. 5. 1. Dostawca internetowego serwisu społecznościowego, w celu wykonania obowiązku, o którym mowa w art. 4 ust. 1, potwierdza wiek użytkownika przy użyciu:

1) elektronicznego poświadczenia atrybutów, pozwalającego na potwierdzenie osiągnięcia minimalnego wieku dostępu do internetowych serwisów społecznościowych, udostępnianego za pomocą europejskiego portfela tożsamości cyfrowej, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014 r., Dz. Urz. UE L 333 z 27.12.2022, str. 80 oraz Dz. Urz. UE L 2024/1183 z 30.04.2024.), zwanym dalej „rozporządzeniem 910/2014”, lub
2) usługi, o której mowa w art. 7 ust. 1, lub
3) rozwiązania informatycznego wpisanego na listę, o której mowa w art. 8 ust. 1.

2. Dostawca internetowego serwisu społecznościowego nie dokonuje potwierdzenia wieku użytkownika w sposób, o którym mowa w ust. 1, jeżeli dokonał weryfikacji tożsamości użytkownika, która pozwala na jego jednoznaczną identyfikację i w jej ramach pozyskał informacje dotyczące imienia, nazwiska i wieku.

3. Weryfikacja tożsamości użytkownika, o której mowa w ust. 2, może nastąpić w szczególności przez:

1) zastosowanie rozwiązań w zakresie identyfikacji i weryfikacji tożsamości zgodnie z art. 34 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644 i 1669 oraz z 2026 r. poz. 875 i 1206);
2) użycie środków identyfikacji elektronicznej, które spełniają wymogi rozporządzenia 910/2014 dla średniego lub wysokiego poziomu bezpieczeństwa;
3) użycie kwalifikowanego certyfikatu podpisu elektronicznego lub kwalifikowanego elektronicznego poświadczenia atrybutów, o których mowa w rozporządzeniu 910/2014;
4) usługę online, która umożliwia przekazywanie dostawcy internetowego serwisu społecznościowego danych z rejestru publicznego lub systemu teleinformatycznego podmiotu publicznego.

Art. 6. 1. Dostawca internetowego serwisu społecznościowego niezwłocznie ponawia potwierdzenie wieku użytkownika, jeżeli na podstawie informacji posiadanych przez niego w związku ze świadczeniem usługi powziął uzasadnione wątpliwości dotyczące:

1) osiągnięcia przez użytkownika minimalnego wieku dostępu do internetowych serwisów społecznościowych lub
2) udostępnienia konta użytkownika osobie trzeciej, która nie osiągnęła minimalnego wieku dostępu do internetowych serwisów społecznościowych.

2. Informacje, o których mowa w ust. 1, mogą wynikać w szczególności z:

1) danych podanych dobrowolnie przez użytkownika;
2) ustawień konta użytkownika lub sposobu korzystania z funkcji internetowego serwisu społecznościowego;
3) zgłoszenia otrzymanego przez dostawcę internetowego serwisu społecznościowego, jeżeli jego wiarygodność została uprawdopodobniona.

3. W przypadku, o którym mowa w ust. 1, po upływie 14 dni od ponowienia potwierdzenia wieku użytkownika dostawca internetowego serwisu społecznościowego uniemożliwia dostęp

do internetowego serwisu społecznościowego za pośrednictwem konta użytkownika do czasu ponownego potwierdzenia wieku użytkownika.

Rozdział 3

Narzędzia służące do potwierdzania wieku

Art. 7. 1. Minister właściwy do spraw informatyzacji może udostępnić usługę umożliwiającą użytkownikowi aplikacji mObywatel przekazywanie informacji dotyczącej:

1) daty urodzenia, lub
2) posiadania określonego wieku, lub
3) ukończenia określonego roku życia, lub
4) znajdowania się w określonym przedziale wieku.

2. W przypadku korzystania z usługi, o której mowa w ust. 1, w warunkach wzajemnej fizycznej obecności stron, w aplikacji mObywatel prezentowana jest dodatkowo fotografia obejmująca wizerunek twarzy użytkownika aplikacji mObywatel w celu umożliwienia jej porównania z wizerunkiem twarzy osoby udostępniającej informację dotyczącą wieku.

Art. 8. 1. Minister właściwy do spraw informatyzacji prowadzi listę rozwiązań informatycznych umożliwiających potwierdzenie wieku.

2. Na listę, o której mowa w ust. 1, wpisuje się rozwiązania informatyczne, które umożliwiają selektywne przekazywanie przez osobę zainteresowaną, pod jej wyłączną kontrolą, rozumianą w sposób określony dla europejskiego portfela tożsamości cyfrowej w art. 5a ust. 14 rozporządzenia 910/2014, informacji dotyczącej:

1) daty urodzenia, lub
2) posiadania określonego wieku, lub
3) ukończenia określonego roku życia, lub
4) znajdowania się w określonym przedziale wieku,

– zwaną dalej „informacją dotyczącą wieku”.

3. Rozwiązania informatyczne, o których mowa w ust. 2:

1) pozwalają na jednoznaczną identyfikację i potwierdzenie tożsamości użytkownika;
2) opierają się na wiarygodnych źródłach;
3) wykorzystują mechanizmy zapewniające cykliczne potwierdzenie pozostawania narzędzia pod wyłączną kontrolą użytkownika oraz prawidłowości informacji dotyczącej wieku.

4. Dostawca rozwiązania informatycznego składa wniosek o wpis na listę, o której mowa w ust. 1, na piśmie w postaci elektronicznej, na adres do doręczeń elektronicznych ministra właściwego do spraw informatyzacji.

5. Wniosek, o którym mowa w ust. 4, zawiera:

1) nazwę (firmę) podmiotu odpowiedzialnego za rozwiązanie informatyczne;
2) adres siedziby podmiotu odpowiedzialnego za rozwiązanie informatyczne;
3) numer NIP podmiotu odpowiedzialnego za rozwiązanie informatyczne, jeżeli został nadany;
4) numer KRS podmiotu odpowiedzialnego za rozwiązanie informatyczne, jeżeli został nadany;
5) niepowtarzalny identyfikator nadany przez państwo członkowskie Unii Europejskiej dla celów transgranicznej identyfikacji, o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, str. 1, z późn. zm.), podmiotu odpowiedzialnego za rozwiązanie informatyczne - w przypadku braku numeru NIP lub numeru KRS;
6) adres poczty elektronicznej podmiotu odpowiedzialnego za rozwiązanie informatyczne;
7) adres doręczeń elektronicznych lub adres korespondencyjny podmiotu odpowiedzialnego za rozwiązanie informatyczne, jeżeli jest inny niż adres, o którym mowa w pkt 2;
8) informacje o rozwiązaniu informatycznym umożliwiającym weryfikację wieku objętym wnioskiem, w tym:
   a) wskazanie funkcjonalności rozwiązania informatycznego obejmujących przekazywanie informacji dotyczącej wieku,
   b) informację czy rozwiązanie informatyczne może być wykorzystywane do weryfikacji wieku w warunkach wzajemnej fizycznej obecności stron,
   c) źródła informacji dotyczącej wieku.
9) oświadczenie o spełnieniu wymogów, o których mowa w przepisach wydanych na podstawie art. 9 ust. 8.

6. Wniosek, o którym mowa w ust. 4, opatruje się kwalifikowanym podpisem elektronicznym, podpisem osobistym albo podpisem zaufanym.

7. Minister właściwy do spraw informatyzacji może określić wzór wniosku, o którym mowa w ust. 4, w formie dokumentu elektronicznego w rozumieniu ustawy z dnia 17 lutego

2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2026 r. poz. 1241).

Art. 9. 1. Minister właściwy do spraw informatyzacji dokonuje wpisu rozwiązania informatycznego na listę, o której mowa w art. 8 ust. 1, po stwierdzeniu spełnienia wymagań, o których mowa w przepisach wydanych na podstawie ust. 8.

2. Wpis rozwiązania informatycznego na listę, o której mowa w art. 8 ust. 1, stanowi czynność materialno-techniczną.

3. Odmowa wpisu rozwiązania informatycznego na listę, o której mowa w art. 8 ust. 1, następuje w drodze decyzji administracyjnej.

4. Minister właściwy do spraw informatyzacji udostępnia listę, o której mowa w art. 8 ust. 1, w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

5. Lista, o której mowa w art. 8 ust. 1, zawiera:

1) nazwę (firmę) podmiotu odpowiedzialnego za rozwiązanie informatyczne;
2) numery i identyfikatory podmiotu odpowiedzialnego za rozwiązanie informatyczne, o których mowa w art. 8 ust. 5 pkt 3-5;
3) nazwę rozwiązania informatycznego;
4) informacje o rozwiązaniu informatycznym umożliwiającym weryfikację wieku objętym wnioskiem, o których mowa w art. 8 ust. 5 pkt 8;
5) rodzaj informacji dotyczącej wieku udostępnianej w rozwiązaniu informatycznym.

6. Wykreślenie rozwiązania informatycznego, wpisanego na listę, o której mowa w art. 8 ust. 1, następuje:

1) na wniosek podmiotu odpowiedzialnego za rozwiązanie informatyczne;
2) z urzędu, przez ministra właściwego do spraw informatyzacji, w przypadku:
   a) gdy rozwiązanie informatyczne nie spełnia warunków, o których mowa w przepisach wydanych na podstawie ust. 8, lub
   b) wystąpienia ryzyka naruszenia bezpieczeństwa rozwiązania informatycznego mogącego skutkować brakiem prawidłowości w zakresie przekazywania informacji dotyczącej wieku.

7. Wykreślenie rozwiązania informatycznego, wpisanego na listę, o której mowa w art. 8 ust. 1, następuje w formie:

1) czynności materialno-technicznej – w przypadku, o którym mowa w ust. 6 pkt 1;
2) decyzji administracyjnej – w przypadku, o którym mowa w ust. 6 pkt 2.

8. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, warunki techniczne i organizacyjne, jakie musi spełnić rozwiązanie informatyczne wpisane na listę, o której mowa w art. 8 ust. 1, uwzględniając konieczność udostępnienia rozwiązań informatycznych w zakresie weryfikacji wieku zapewniających skuteczne, bezpieczne, chroniące prywatność i interoperacyjne korzystanie oraz konieczność minimalizacji danych, ograniczenia celu, bezpieczeństwa, neutralności technologicznej i proporcjonalności, w tym odpowiednio wymagania dotyczące pełnej kontroli użytkowników nad używaniem udostępnionego rozwiązania informatycznego, określone dla europejskiego portfela tożsamości cyfrowej w art. 5a ust. 14 rozporządzenia 910/2014.

Art. 10. 1. Jeżeli z przepisu prawa wynika obowiązek lub uprawnienie do weryfikacji wieku, obowiązek ten lub uprawnienie to uznaje się za zrealizowane w przypadku potwierdzenia wieku na podstawie:

1) elektronicznego poświadczenia atrybutów udostępnianego za pomocą europejskiego portfela tożsamości cyfrowej, o którym mowa w rozporządzeniu 910/2014,
2) usługi, o której mowa w art. 7 ust. 1,
3) rozwiązania informatycznego umożliwiającego weryfikację wieku, o którym mowa w art. 8 ust. 1.

2. W przypadku, gdy potwierdzenie wieku następuje w warunkach wzajemnej fizycznej obecności stron, narzędzia, o których mowa w ust. 1, zapewniają, że prezentowana jest dodatkowo fotografia obejmująca wizerunek twarzy osoby, której wiek jest potwierdzany.

Rozdział 4

Działania edukacyjne

Art. 11. 1. Podstawa programowa wychowania przedszkolnego oraz podstawy programowe kształcenia ogólnego dla poszczególnych typów szkół, o których mowa w przepisach wydanych na podstawie art. 47 ust. 1 pkt 1 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2026 r. poz. 820, z późn. zm.[1)]), zawierają treści nauczania z zakresu zasad higieny cyfrowej, w tym dotyczących wpływu nadużywania urządzeń ekranowych na zdrowie psychiczne i fizyczne, zasad cyberbezpieczeństwa, w tym ochrony prywatności i bezpieczeństwa w cyfrowym świecie oraz zagrożeń wynikających z niewłaściwego używania technologii informacyjno-komunikacyjnych, w szczególności

---

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2026 r. poz. 904, 982, 1036, 1123 i 1527.

odnoszących się do cyberprzemocy i mowy nienawiści, uzależnienia od Internetu i gier komputerowych oraz niebezpiecznych kontaktów w sieci, dostosowane do wieku dzieci objętych wychowaniem przedszkolnym oraz uczniów.

2. Minister właściwy do spraw oświaty i wychowania może realizować działania informacyjne i promocyjne, dotyczące obszarów, o których mowa w ust. 1, lub zlecać ich wykonanie jednostkom organizacyjnym podległym temu ministrowi lub przez niego nadzorowanym.

3. Minister właściwy do spraw oświaty i wychowania może zlecać w drodze konkursu realizację działań, o których mowa w ust. 2, również podmiotom, o których mowa w art. 3 ust. 1 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe.

Rozdział 5

Postępowanie w sprawach o naruszenie ustawy

Art. 12. 1. Prezes Urzędu Komunikacji Elektronicznej, zwany dalej „Prezesem UKE”, jest uprawniony do przeprowadzania kontroli i postępowania pokontrolnego w celu weryfikacji spełniania przez dostawcę internetowego serwisu społecznościowego obowiązku, o którym mowa w art. 4 ust. 1.

2. Prezes UKE przeprowadza z urzędu kontrolę i postępowanie pokontrolne, o których mowa w ust. 1.

3. Do kontroli i postępowania pokontrolnego, o których mowa w ust. 1, stosuje się przepisy art. 22zl-22zw ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513 oraz z 2026 r. poz. 1296).

Rozdział 6

Administracyjne kary pieniężne

Art. 13. 1. Dostawca internetowego serwisu społecznościowego, który nie wypełnia obowiązków, o których mowa w art. 4 lub 5, podlega administracyjnej karze pieniężnej.

2. Administracyjną karę pieniężną, o której mowa w ust. 1, nakłada Prezes UKE, w drodze decyzji, w wysokości nie większej niż 6 % rocznego światowego obrotu dostawcy internetowego serwisu społecznościowego w roku obrotowym poprzedzającym rok nałożenia kary.

3. Administracyjna kara pieniężna, o której mowa w ust. 1, może zostać nałożona także w przypadku, gdy dostawca internetowego serwisu społecznościowego zaprzestał naruszania

prawa lub naprawił wyrządzoną szkodę, jeżeli Prezes UKE uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

Art. 14. 1. Wysokość obrotu, o którym mowa w art. 13 ust. 2, oblicza się jako sumę:

1) przychodów wykazanych w rachunku zysków i strat – w przypadku dostawcy internetowego serwisu społecznościowego, który sporządza ten rachunek na podstawie przepisów o rachunkowości;
2) przychodów wykazanych w sprawozdaniu finansowym za rok obrotowy równoważnych przychodom prezentowanym w rachunku zysków i strat sporządzanym na podstawie przepisów o rachunkowości lub wykazanych w innym dokumencie podsumowującym przychody w roku obrotowym, w tym w sprawozdaniu z wykonania budżetu – w przypadku dostawcy internetowego serwisu społecznościowego, który nie sporządza rachunku zysków i strat na podstawie przepisów o rachunkowości;
3) udokumentowanych przychodów uzyskanych w roku obrotowym – w przypadku braku dokumentów, o których mowa w pkt 1 i 2.

2. W przypadku gdy dostawca internetowego serwisu społecznościowego powstał w wyniku połączenia lub przekształcenia innych podmiotów, przy obliczaniu wysokości jego obrotu, o którym mowa w art. 13 ust. 2, Prezes UKE uwzględnia obrót osiągnięty przez te podmioty w roku obrotowym poprzedzającym rok nałożenia kary.

3. W przypadku gdy dostawca internetowego serwisu społecznościowego w roku obrotowym poprzedzającym rok nałożenia kary nie osiągnął obrotu, Prezes UKE nakładając administracyjną karę pieniężną na podstawie art. 13 ust. 1, uwzględnia średni obrót osiągnięty przez dostawcę internetowego serwisu społecznościowego w trzech kolejnych latach obrotowych poprzedzających rok nałożenia kary.

4. W przypadku gdy dostawca internetowego serwisu społecznościowego nie osiągnął obrotu w okresie trzyletnim, o którym mowa w ust. 3, wysokość administracyjnej kary pieniężnej nałożonej przez Prezes UKE na podstawie art. 13 ust. 1, nie przekracza równowartości 6 000 euro.

5. W przypadku gdy dostawca internetowego serwisu społecznościowego przed wydaniem decyzji nakładającej administracyjną karę pieniężną nie dysponuje danymi finansowymi niezbędnymi do ustalenia obrotu za rok obrotowy poprzedzający rok nałożenia kary, Prezes UKE, nakładając karę pieniężną na podstawie art. 13 ust. 1, uwzględnia:

1) obrót osiągnięty przez dostawcę internetowego serwisu społecznościowego w roku obrotowym poprzedzającym ten rok;

2) w przypadku, o którym mowa w ust. 3 – średni obrót osiągnięty przez dostawcę internetowego serwisu społecznościowego w trzech kolejnych latach obrotowych poprzedzających ten rok; przepis ust. 4 stosuje się odpowiednio.

6. Przeliczenie wartości euro na złote jest dokonywane według kursu średniego walut obcych ogłoszonego przez Narodowy Bank Polski w ostatnim dniu roku kalendarzowego poprzedzającego rok nałożenia kary.

Art. 15. Wpływy z tytułu administracyjnych kar pieniężnych, o których mowa w art. 13 ust. 1, stanowią dochód budżetu państwa.

Art. 16. 1. Administracyjne kary pieniężne podlegają egzekucji w trybie ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji w zakresie egzekucji należności pieniężnych (Dz. U. z 2026 r. poz. 1311).

2. Administracyjną karę pieniężną uiszcza się w terminie 14 dni od dnia, w którym decyzja, o której mowa w art. 13 ust. 2, stała się ostateczna.

Art. 17. W zakresie nieuregulowanym w niniejszej ustawie oraz ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691) do kar pieniężnych stosuje się odpowiednio przepisy działu III ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2026 r. poz. 622, z późn. zm.[2)]), z tym że uprawnienia organów podatkowych określone w tych przepisach przysługują Prezesowi UKE nakładającemu administracyjną karę pieniężną, o której mowa w art. 13 ust. 1.

Rozdział 7

Zmiany w przepisach obowiązujących

Art. 18. W ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną w art. 3a w ust. 2 w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:

„7) obowiązków dostawców internetowych serwisów społecznościowych w zakresie dostępu małoletnich do usług, o których mowa w ustawie z dnia … o minimalnym wieku dostępu do internetowych serwisów społecznościowych.”.

---

2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2026 r. poz. 825, 846, 875, 1098, 1154 i 1206.

Art. 19. W ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z późn. zm.[3)]) w art. 419 w ust. 1 w pkt 24 kropkę zastępuje się średnikiem i dodaje się pkt 25 w brzmieniu:

„25) kontrola obowiązku dostawców internetowych serwisów społecznościowych w zakresie dostępu małoletnich do usług, o którym mowa w ustawie z dnia … o minimalnym wieku dostępu do internetowych serwisów społecznościowych.”.

Rozdział 8

Przepisy przejściowe i końcowe

Art. 20. 1. Dostawca internetowego serwisu społecznościowego po raz pierwszy potwierdza wiek osób posiadających konto użytkownika, które założyły konto użytkownika:

1) do 1 września 2026 r. – w terminie 18 miesięcy od dnia wejścia ustawy w życie;
2) po 1 września 2026 r. – w terminie 6 miesięcy od dnia wejścia ustawy w życie.

2. Potwierdzenia wieku, o którym mowa w ust. 1 nie przeprowadza się, jeżeli dostawca może wykazać z wysokim stopniem pewności, że użytkownik ukończył lat piętnaście, w szczególności, jeżeli konto użytkownika zostało założone co najmniej 10 lat przed wejściem ustawy w życie.

Art. 21. Ustawa wchodzi w życie z dniem 1 września 2027 r.

Za zgodność pod względem prawnym,
legislacyjnym i redakcyjnym

Magdalena Witkowska
Dyrektor Departamentu Prawnego
w Ministerstwie Cyfryzacji
/podpisano elektronicznie/

Za zgodność pod względem prawnym,
legislacyjnym i redakcyjnym

Andrzej Barański
Dyrektor Departamentu Prawnego
w Ministerstwie Edukacji Narodowej
/podpisano elektronicznie/

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 637 i 820 oraz z 2026 r. poz. 252, 815 i 1296.

Uzasadnienie

Współczesne dzieciństwo i dorastanie przebiegają w środowisku silnie zdominowanym przez nowoczesne technologie. Smartfony, media społecznościowe i stały dostęp do internetu nie tylko zmieniły sposoby uczenia się i budowania relacji, lecz także wprowadziły nowe formy zagrożeń psychospołecznych takich jak cyberprzemoc, naruszenia prywatności i danych osobowych, kontakt z niepożądanymi treściami, dezinformacja, uzależnienie od mediów społecznościowych oraz gier komputerowych. W kontekście ostatnich wydarzeń związanych z aktami przemocy fizycznej w szkołach, realnym zagrożeniem jest zjawisko radykalizacji, której przejawy są widoczne także w przestrzeni cyfrowej.

W Polsce duża część dzieci poniżej 15 roku życia korzysta z mediów społecznościowych. Obecnie środowisko internetowe nie jest projektowane z myślą o dzieciach i nie uwzględnia ich mentalności, poziomu rozwoju psychicznego i podatności na zagrożenia, które mogą mieć poważny wpływ na ich dobrostan, rozwój oraz zdrowie fizyczne i psychiczne.

Istniejące wymogi wiekowe na platformach internetowych zazwyczaj nie są opracowywane w oparciu o potrzeby dzieci i praktycznie nie są egzekwowane. Większość dostawców usług cyfrowych określa w swoich warunkach korzystania z usług minimalny wiek dostępu do swoich usług lub ich użytkowania. Jak zauważyła OECD (raport „Age Assurance Practices of 50 Online Services Used by Children" 2025), wybór wieku przez platformę wynika z przyczyn związanych z prywatnością i prawem konsumenckim, a nie z oceny bezpieczeństwa lub adekwatności pod względem rozwoju. OECD podkreśla ponadto, że „bardzo niewiele (usług, które określają minimalny wiek w warunkach korzystania z usług) wdraża systemowe potwierdzanie wieku" oraz że tylko 2 z 50 analizowanych usług online systematycznie wymagają potwierdzenia wieku do założenia konta. Jedyną formą kontroli wieku przed założeniem konta jest zazwyczaj oświadczenie własne. Powszechnie uznaje się, że samo oświadczenie własne nie jest skutecznym środkiem potwierdzania wieku, ponieważ wielu użytkowników nie ujawnia swojego rzeczywistego wieku. Szereg badań pokazuje, że małoletni rutynowo podają nieprawdziwy wiek w internecie. W praktyce niepełnoletni użytkownicy mogą zatem z łatwością uzyskać dostęp do wielu usług online ograniczonych wiekiem.

W zakresie egzekwowania Aktu o usługach cyfrowych postępowania stwierdzające niewypełnianie obowiązków przez platformy internetowe wymagają czasu. Art. 28 Aktu o usługach cyfrowych koncentruje się na ochronie prywatności i zakazie profilowania reklamowego. Nie zapobiega jednak stosowaniu funkcji, które psychologicznie uzależniają dzieci od ekranu. Mechanizmy takie jak nieskończone przewijanie (infinite scroll),

autoodtwarzanie filmów (autoplay), powiadomienia push czy algorytmy rekomendacji wpędzające w tzw. „królicze nory” (szkodliwe pętle tematyczne) formalnie nie łamały wprost art. 28, mimo że negatywnie wpływają na zdrowie psychiczne małoletnich. Ze względu na ograniczoną skuteczność stosowania art. 28 Aktu o usługach cyfrowych zasadne jest podjęcie inicjatywy legislacyjnej w omawianym obszarze.

Rozdział 1 – Przepisy ogólne

Projektowany art. 2 projektu wprowadza definicję internetowego serwisu społecznościowego w rozumieniu art. 2 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz. Urz. UE L 265 z 12.10.2022, str. 1 oraz Dz. Urz. UE L 2025/90024 z 10.01.2025): oznacza platformę umożliwiającą użytkownikom końcowym łączenie się i komunikowanie ze sobą, udostępnianie treści oraz zapoznawanie się z innymi użytkownikami i treściami z wykorzystaniem różnych urządzeń, w szczególności za pośrednictwem czatów, postów, filmów wideo i rekomendacji). W potocznym rozumieniu mówi się w tym wypadku o mediach społecznościowych. Serwisy te posiadają różne funkcje, takie jak czaty, posty, filmy wideo czy rekomendacje. Przykłady takich serwisów to m.in. TikTok, Facebook, Instagram.

Internetowy serwis społecznościowy to specyficzny rodzaj platformy online, na której użytkownicy budują relacje społeczne, nawiązują kontakty i dzielą się treściami. W założeniu służyć ma do wymiany informacji o wspólnych zainteresowaniach, kwestiach zawodowych, aktywnościach czy prywatnym życiu. Serwisy te różnią się pod względem formatu i liczby oferowanych funkcji, w tym narzędzi komunikacji i rodzajów udostępnianych treści. Typowymi funkcjami takich platform są możliwość publikacji zdjęć, filmów oraz udostępnianie treści (wpisów, postów). Serwisy społecznościowe umożliwiają użytkownikom tworzenie własnych profili oraz budowanie sieci kontaktów.

Do zakresu projektu nie wchodzą komunikatory internetowe, które są objęte definicją usług łączności interpersonalnej niewykorzystujących numerów.

Ze względu na małe prawdopodobieństwo wyrządzania szkody małoletnim wyłączone z zakresu projektu są encyklopedie internetowe, repozytoria, usługi i systemy edukacyjno-naukowe, platformy tworzenia otwartego oprogramowania i platformy wymiany otwartego oprogramowania, usługi i systemy opracowane i obsługiwane wyłącznie do celów badań

naukowych i rozwoju oraz usługi i systemy zaprojektowane, opracowane i obsługiwane przez organy publiczne i do wyłącznego użytku tych organów publicznych lub w ich imieniu.

W art. 3 ustalono ukończenie lat piętnastu jako minimalny wiek dostępu do internetowych serwisów społecznościowych. Wiek 15 lat w polskim systemie edukacji zbiega się zazwyczaj z ukończeniem szkoły podstawowej. Jest to naturalny moment osiągnięcia pewnego pułapu „dojrzałości cyfrowej". Starsza młodzież lepiej radzi sobie z weryfikacją fake newsów, manipulacją oraz potrafi stawiać wyraźniejsze granice w relacjach z obcymi osobami w sieci. Profile w mediach społecznościowych często prezentują wyidealizowany, nierealistyczny obraz życia i wyglądu. U dzieci poniżej 15. roku życia, które dopiero budują swoją tożsamość, rodzi to frustrację, kompleksy oraz drastycznie obniża samoocenę.

Rozdział 2 – Obowiązki dostawców internetowych serwisów społecznościowych

Zgodnie z art. 4 dostawca internetowego serwisu społecznościowego będzie obowiązany uniemożliwić osobie poniżej wspomnianego minimalnego wieku na założenie konta użytkownika lub na dostęp do internetowego serwisu społecznościowego za pośrednictwem konta utworzonego dla tej osoby lub przypisanego do niej. Zakaz ten będzie dotyczył internetowych serwisów spełniających przynajmniej jedną z przesłanek ryzyka dla prywatności i bezpieczeństwa określonych w tym przepisie. Przesłanki te sformułowane zostały w sposób analogiczny do art. 6 ust. 1 propozycji rozporządzenia EU KIDS ACT – „UE na straży odpowiedzialnych i godnych zaufania przestrzeni cyfrowych w internecie".

W art. 5 ust. 1 wskazane zostały metody, za pomocą których dostawca internetowego serwisu społecznościowego może dokonywać potwierdzenia wieku użytkownika, czyli narzędzia do potwierdzania wieku, o których mowa w rozdziale 3. Mamy tutaj do czynienia z katalogiem zamkniętym i w konsekwencji dostawca będzie mógł zrealizować obowiązek ustawowy tylko na podstawie metod wskazanych w tym przepisie, tj. elektronicznego poświadczenia atrybutów udostępnianego za pomocą europejskiego portfela tożsamości cyfrowej (chodzi o każde z poświadczeń, o których mowa w art. 3 ust. 44-46 rozporządzenia 910/2014), dedykowanej usługi w aplikacji mObywatel oraz rozwiązania informatycznego wpisanego na listę rozwiązań informatycznych umożliwiających weryfikację wieku.

W art. 5 ust. 2 przewidziany został wyjątek dla dostawców serwisów społecznościowych, kiedy nie muszą dokonywać weryfikacji wieku, o której mowa w art. 5 ust. 1. Dotyczy on sytuacji, gdy taki dostawca posiada już informację co do tożsamości użytkownika i w jej ramach potrafi go jednoznacznie zidentyfikować, w tym posiada informację o jego wieku.

W pewnych sytuacjach użytkownicy platform społecznościowych są zainteresowani, by ich aktywność była jednoznacznie przypisana do ich osoby (np. przedsiębiorcy, którym zależy na posiadaniu statusu potwierdzonego lub oficjalnego konta). Skoro użytkownik dobrowolnie przekazał takiemu dostawcy informacje pozwalające na jego jednoznaczną identyfikację obejmującą m. in. wiek, to niecelowe jest, by w stosunku do niego zachodziła konieczność ponownego potwierdzania tej informacji przy pomocy metod pozwalających na selektywne przekazywanie informacji wskazanych w art. 5 ust. 1. Przepis ten ma charakter wyjątku od reguły ustanowionej wcześniej i w związku z tym nie może być interpretowany jako nakaz potwierdzania tożsamości przez dostawców internetowych serwisów społecznościowych. Przedmiotowy przepis mówi o jednoznacznej identyfikacji, a więc musi to być identyfikacja wskazująca na konkretną, jedną osobę. Nie zawsze taka identyfikacja opierać się będzie tylko o dane dotyczące imienia, nazwiska i wieku. W efekcie tej jednoznacznej identyfikacji taki dostawca będzie musiał jednak zawsze posiadać przynajmniej te trzy dane.

W art. 5 ust. 3 określono katalog metod, na podstawie których dostawca internetowego serwisu społecznościowego może dokonać weryfikacji tożsamości pozwalającej na jego jednoznaczną identyfikację. Katalog ten ma charakter otwarty i stanowi wyliczenie zawierające najbardziej popularne metody pozwalające na jednoznaczną identyfikację danej osoby. Dostawcy internetowych serwisów społecznościowych, żeby móc skorzystać z wyjątku opisanego w art. 5 ust. 2, będą więc mogli korzystać również z innych metod, byleby finalnie pozwalały one na weryfikację tożsamości danego użytkownika i jego jednoznaczną identyfikację, na skutek której będą oni posiadać dane dotyczące imienia, nazwiska i wieku tego użytkownika.

Art. 6 ma na celu ograniczenie sytuacji, w których nastąpiło potwierdzenie wieku danego użytkownika, a następnie doszło do udostępnienia danej usługi (np. konta w serwisie społecznościowym) osobie, która nie osiągnęła minimalnego wieku dostępu do internetowych serwisów społecznościowych lub z innych powodów okazało się, że wątpliwe jest by z usługi korzystała osoba, która taki wiek osiągnęła. Przepis nakłada na dostawcę internetowego serwisu społecznościowego by musiał on w takiej sytuacji dokonać ponownej weryfikacji wieku użytkownika. Przepis nie nakłada jednak na dostawców internetowych serwisów społecznościowych obowiązku gromadzenia danych, o których mowa w art. 6 ust. 2. Nadal decyzja w tym zakresie będzie należeć do dostawcy, który sam określi zakres danych, jakie gromadzi o użytkowniku i zdecyduje, czy ten zakres jest zgodny z obowiązującymi go przepisami prawa. W art. 6 ust. 3 przewidziano swoisty okres wyczekiwania związany

z pojawieniem się takiej wątpliwości. W momencie powzięcia przez takiego dostawcę wątpliwości, udostępnia on możliwość ponownego zweryfikowania wieku, a po upływie 14 dni uniemożliwia dostęp do swojego serwisu, za pośrednictwem konta którego dotyczą wątpliwości, do czasu ponownego potwierdzenia wieku użytkownika w sposób, o którym mowa w art. 5 ust. 1 lub 2.

Rozdział 3 – Narzędzia służące do potwierdzania wieku

W rozdziale uregulowano zasady stosowania narzędzi do potwierdzania wieku.

W art. 7 uregulowano funkcjonowanie nowej usługi w aplikacji mObywatel w zakresie weryfikacji wieku. Przepis ten wskazuje, że usługa ta będzie umożliwiać użytkownikowi aplikacji mObywatel, pod jego wyłączną kontrolą, selektywne przekazywanie informacji dotyczącej: daty urodzenia, posiadania określonego wieku, osiągnięcia określonego progu wiekowego lub osiągnięcia wieku w określonym przedziale wiekowym. Przepis umożliwia więc, by w usłudze była prezentowana przynajmniej jedna tego typu informacja, niektóre z nich lub wszystkie. Zakłada się, że początkowo usługa będzie udostępniać tylko informację o posiadaniu określonego progu wieku, a następnie funkcjonalności w tym zakresie będą rozszerzane. W przypadku gdy użytkownik będzie korzystał z usługi w warunkach fizycznej obecności stron w aplikacji oprócz informacji o wieku prezentowana będzie też fotografia obejmująca wizerunek twarzy użytkownika celem umożliwienia porównania go z twarzą osoby udostępniającej informację.

W art. 8 zawarto nową kompetencję dla ministra właściwego do spraw informatyzacji – prowadzenie listy rozwiązań informatycznych umożliwiających weryfikację wieku. Na tej liście znajdą się tylko te rozwiązania, które umożliwią selektywne przekazywanie przez osobę zainteresowaną, pod jej wyłączną kontrolą (w rozumieniu art. 5a ust. 14 rozporządzenia 910/2014) informacji dotyczącej daty urodzenia, liczby ukończonych lat, ukończenia określonego roku życia lub znajdowania się w określonym przedziale wieku. Wpis na listę będzie następował na wniosek dostawcy rozwiązania informatycznego. Na listę będą mogły być wpisane podmioty mające swoje siedziby na terenie całej Unii Europejskiej. Procedura będzie w pełni elektroniczna.

W art. 9 określono dalsze szczegóły funkcjonowania przedmiotowej listy, w tym formę, w jakiej będzie następował wpis lub odmowa dokonania wpisu, miejsce publikacji listy, jej zawartość, sposób wykreślenia rozwiązań z listy oraz formę takiego wykreślenia. Art. 9 ust. 8 zawiera również upoważnienie dla ministra właściwego do spraw informatyzacji do określenia,

w drodze rozporządzenia, szczegółowych warunków technicznych i organizacyjnych, jakie musi spełnić rozwiązanie informatyczne wpisane na listę.

Zgodnie z projektowanym art. 10 wyżej opisane narzędzia znajdą zastosowanie wszędzie tam, gdzie z przepisu prawa wynika obowiązek lub uprawnienie do weryfikacji wieku. W związku z tym przepisem oprócz dotychczasowej (tradycyjnej) metody potwierdzania wieku w postaci okazania dokumentu tożsamości równie skuteczne będzie wykorzystanie: elektronicznego poświadczenia atrybutów udostępnianego za pomocą europejskiego portfela tożsamości cyfrowej, o którym mowa w rozporządzeniu 910/2014, usługi w aplikacji mObywatel, o której mowa w art. 7 ust. 1, czy rozwiązania informatycznego, , o którym mowa w art. 8 ust. 1. W przypadku wzajemnej obecności stron narzędzia te muszą zapewniać również przedstawienie fotografii obejmującej wizerunek twarzy osoby poddawanej weryfikacji.

Rozdział 4 – Działania edukacyjne

Edukacja cyfrowa musi zapewniać nabycie podstawowej wiedzy i umiejętności z zakresu bezpieczeństwa cyfrowego ze względu na szeroki dostęp obywateli, w tym dzieci i młodzieży, do cyberprzestrzeni oraz wzrost zagrożenia cyberprzestępstwami. Zagrożenia w internecie rosną, a dezinformacja została uznana za jeden z najbardziej destabilizujących czynników dla społeczeństw europejskich.

Wskazane jest więc, aby edukacja w zakresie szeroko pojętego cyberbezpieczeństwa była zapewniona na jak najwcześniejszym etapie dostępu dzieci i młodzieży do przestrzeni cyfrowej. Podstawa programowa wychowania przedszkolnego i podstawa programowa kształcenia ogólnego dla poszczególnych typów szkół powinny uwzględniać aktualną wiedzę oraz kłaść nacisk na rozwijanie wiedzy i umiejętności służących bezpieczeństwu cyfrowemu, w tym ochronie urządzeń elektronicznych i treści cyfrowych, świadomości i rozumienia ryzyka, zagrożeń w środowisku cyfrowym i środków bezpieczeństwa oraz ochronie wizerunku i prywatnych danych. Nie można także pominąć aspektu wpływu nowych technologii na zdrowie – zarówno psychiczne jak i fizyczne małoletnich użytkowników sieci. Zagadnienia dotyczące ochrony zdrowia i dbania o samopoczucie poprzez stosowanie zasad higieny cyfrowej, reagowanie na przemoc w środowisku cyfrowym, przeciwdziałanie uzależnieniom od nowych technologii oraz wpływ technologii i jej stosowania na zdrowie psychiczne i fizyczne – to obszary konieczne do uwzględniania na każdym etapie kształcenia w edukacji formalnej.

Szkoła powinna odpowiednio przygotowywać poszczególne roczniki uczniów do świadomego i odpowiedzialnego korzystania z technologii informacyjno-komunikacyjnych, wyposażyć ich w kompetencje potrzebne do korzystania z różnych cyfrowych zasobów informacyjnych, wyszukiwania i krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej, w tym nawiązywania i utrzymywania opartych na wzajemnym szacunku relacji z innymi użytkownikami sieci.

Z uwagi na powyższe proponuje się przepis art. 11 wzmacniający obecność w podstawie programowej wychowania przedszkolnego oraz podstawach programowych kształcenia ogólnego dla poszczególnych typów szkół treści nauczania obejmujących: zasady higieny cyfrowej, w tym dotyczące wpływu nadużywania urządzeń ekranowych na zdrowie psychiczne i fizyczne, zasady cyberbezpieczeństwa, w tym ochronę prywatności i bezpieczeństwo w cyfrowym świecie oraz zagrożenia wynikające z niewłaściwego używania technologii informacyjno-komunikacyjnych, w szczególności odnoszące się do cyberprzemocy i mowy nienawiści, uzależnienia od Internetu i gier komputerowych oraz niebezpiecznych kontaktów w sieci.

W projekcie umożliwia się także ministrowi właściwemu do spraw oświaty i wychowania realizację działań informacyjnych i promocyjnych, w obszarach, które obejmą zagadnienia związane z: zasadami higieny cyfrowej, zasadami cyberbezpieczeństwa, zagrożeniami wynikającymi z niewłaściwego używania technologii informacyjno-komunikacyjnych. Minister będzie mógł zlecać realizację tych zadań jednostkom organizacyjnym podległym lub przez siebie nadzorowanym.

Minister będzie mógł również zlecać realizację powyższych działań, w drodze konkursu, organizacjom pozarządowym, w tym organizacjom harcerskim, instytutom badawczym, instytucjom kultury czy podmiotom prowadzącym statutową działalność w zakresie oświaty i wychowania.

Realizacja działań informacyjnych i promocyjnych pozwoli na skuteczniejsze dotarcie do grup docelowych, co doprowadzi do zwiększenia świadomości dzieci objętych wychowaniem przedszkolnym i uczniów w zakresie bezpiecznego i odpowiedzialnego korzystania z technologii cyfrowych.

Rozdział 5 – Postępowanie w sprawach o naruszenie ustawy

Art. 12 projektu upoważnia Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE” do przeprowadzania z urzędu kontroli i postępowania pokontrolnego w celu

weryfikacji spełniania przez dostawcę internetowego serwisu społecznościowego obowiązku zgodnie z którym nie zezwala on małoletniemu poniżej lat piętnastu na założenie konta użytkownika lub na dostęp do internetowego serwisu społecznościowego za pośrednictwem konta utworzonego dla tej osoby lub przypisanego do niej. Kontrola i postępowanie pokontrolne przeprowadzane będą zgodnie z przepisami art. 22zl-22zw ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513, z późn. zm.).

Rozdział 6 – Administracyjne kary pieniężne

W art. 13 przewidziano możliwość nałożenia administracyjnej kary pieniężnej na dostawcę internetowego serwisu społecznościowego, który nie wypełnia obowiązków związanych z potwierdzeniem wieku użytkownika. Karę będzie mógł nałożyć Prezes UKE, w drodze decyzji, w wysokości nie większej niż 6 % rocznego światowego obrotu dostawcy internetowego serwisu społecznościowego w roku obrotowym poprzedzającym rok nałożenia kary.

W tym kontekście wskazać należy, iż pojęcie to jest wykorzystywane w unijnych rozporządzeniach, w tym w Akcie o usługach cyfrowych, oraz w ogólnym rozporządzeniu o ochronie danych, jak i w polskim prawodawstwie, w ustawie z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów. Wpływa to na potencjalny wymiar kary, różnicując ją w tym zakresie od kar przewidzianych dotychczasowymi przepisami właściwymi dla właściwych organów, a więc wykluczając możliwość powstania ewentualnej dysproporcji.

W art. 14 określono sposób obliczania wysokości obrotu – w sposób analogiczny do art. 22zzo ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

Administracyjne kary pieniężne będą stanowiły dochód budżetu państwa i podlegały będą egzekucji w trybie ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji w zakresie egzekucji należności pieniężnych (Dz. U. z 2026 r. poz. 1311). W odniesieniu do kar pieniężnych, w zakresie nieuregulowanym w niniejszej ustawie oraz w ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, stosuje się odpowiednio przepisy działu III ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2026 r. poz. 622, z późn. zm.), który dotyczy między innymi zobowiązań podatkowych, kwestii zaległości podatkowych, odsetek za zwłokę, wygaśnięcia zobowiązań podatkowych, ulg, przedawnień, nadpłaty, odpowiedzialności solidarnej i podatkowej osób trzecich, a także praw i obowiązki następców prawnych i podmiotów przekształconych.

Rozdział 7 – Zmiany w przepisach obowiązujących

Art. 18 wprowadza zmianę w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, określając obowiązki dostawców internetowych serwisów społecznościowych w zakresie dostępu małoletnich do usług jako wyjątek od zasady państwa pochodzenia, o której mowa w art. 3a ust. 1 tej ustawy.

W art. 19 dodano zmianę w ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z późn. zm.), poszerzając zakres działania Prezesa UKE o kontrolę obowiązku dostawców internetowych serwisów społecznościowych w zakresie dostępu małoletnich do usług.

Rozdział 8 – Przepisy przejściowe i końcowe

W art. 20 doprecyzowano terminy potwierdzenia po raz pierwszy przez dostawcę internetowego serwisu społecznościowego wieku osób posiadających konto użytkownika. W stosunku do osób, które założyły konto użytkownika do 1 września 2026 r. potwierdzenie będzie musiało nastąpić w ciągu 18 miesięcy od dnia wejścia ustawy w życie. Natomiast w stosunku do osób, które założyły konto po 1 września 2026 r., termin ten będzie wynosił 6 miesięcy od dnia wejścia ustawy w życie, a zatem potwierdzenie wieku użytkownika po raz pierwszy będzie musiało mieć miejsce przed dniem 1 marca 2028 r. Nie będzie konieczne przeprowadzenie takiego potwierdzenia wieku w stosunku do użytkowników, co do których dostawca może wykazać z wysokim stopniem pewności, że ukończyli lat piętnaście, w szczególności jeżeli konto użytkownika zostało założone co najmniej 10 lat przed wejściem ustawy w życie.

Ustawa wejdzie w życie z dniem 1 września 2027 r.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja zawiera przepisy techniczne w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), zatem podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2026 r. poz. 500).

Projekt ustawy nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2026 r. poz. 936) projekt ustawy został udostępniony w Biuletynie Informacji Publicznej. Ponadto, zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2026 r. poz. 404), projekt ustawy został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

OCENA SKUTKÓW REGULACJI

Nazwa projektu Projekt ustawy o minimalnym wieku dostępu do internetowych serwisów społecznościowych **Ministerstwa wiodące** Ministerstwo Cyfryzacji Ministerstwo Edukacji Narodowej **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Dariusz Standerski, Sekretarz Stanu w Ministerstwie Cyfryzacji Katarzyna Lubnauer, Sekretarz Stanu w Ministerstwie Edukacji Narodowej **Kontakt do opiekuna merytorycznego projektu** Mateusz Sztobryn, Zastępca Dyrektora Departamentu Projektów i Strategii w Ministerstwie Cyfryzacji, email: Mateusz.Sztobryn@cyfra.gov.pl Tomasz Kulasa – Dyrektor Departamentu Innowacji i Rozwoju w Ministerstwie Edukacji Narodowej, tel. 538 818 140, e-mail: tomasz.kulasa@men.gov.pl Justyna John, radca w Departamencie Innowacji i Rozwoju w Ministerstwie Edukacji Narodowej, tel. 22 3474 559, e-mail: justyna.john@men.gov.pl	**Data sporządzenia** 2026-11-20 **Źródło:** Inicjatywa własna **Nr w Wykazie prac legislacyjnych i programowych Rady Ministrów:** UD492

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Usługi społeczeństwa informacyjnego, w szczególności internetowe serwisy społecznościowe, stały się istotnym elementem codziennego życia dzieci i młodzieży. Mogą one sprzyjać rozwojowi osobowości, edukacji, aktywności obywatelskiej, nawiązywaniu relacji, komunikacji oraz kreatywności, jednak niosą również zagrożenie dla prywatności, bezpieczeństwa i ochrony małoletnich.

Jak wynika z przedstawionego przez Komisję Europejską w dniu 17 września 2026 r. wniosku legislacyjnego EU Kids Act[4], jedynie połowa dzieci w wieku 9–16 lat w Europie deklaruje, że czuje się bezpiecznie w Internecie. Zagrożenia, na jakie są narażeni małoletni w sieci, są realne i wymagają pilnej reakcji – wpływają bowiem na ich zdrowie, rozwój i dobrostan. Wśród skutków wymienia się między innymi spadek aktywności fizycznej, zwiększone ryzyko krótkowzroczności i zaburzeń snu, objawy depresyjne i lękowe, obniżone poczucie własnej wartości, negatywny wpływ na procesy uczenia się i rozwój poznawczy, zaburzenia odżywiania, osłabienie empatii, poczucie samotności oraz zachowania o charakterze uzależniającym. Nieletni są narażeni ponadto na cyberprzemoc, hejt, dezinformację i manipulację, a także na niegodziwe traktowanie w celach seksualnych i nagabywanie seksualne (grooming), co może prowadzić do poważnych konsekwencji emocjonalnych i społecznych.

Z badania Eurobarometr „Impact of excessive screen time and social media on young people's mental health", wynika, że wcześniejsze rozpoczęcie korzystania z mediów społecznościowych wiąże się z dłuższym czasem spędzanym online oraz większą ekspozycją na szkodliwe treści, w tym cyberprzemoc, mowę nienawiści czy niechciane treści seksualne. Jednocześnie intensywne korzystanie z mediów społecznościowych jest powiązane z częstszym występowaniem problemów ze snem, koncentracją, stresem i lękiem. Raport wskazuje, że wiek rozpoczęcia korzystania z mediów

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026PC0681

społecznościowych jest jednym z najsilniejszych czynników różnicujących późniejsze zachowania cyfrowe młodzieży. Osoby, które rozpoczęły korzystanie z mediów społecznościowych przed ukończeniem 10. roku życia, spędzają średnio 7,5 godziny dziennie przed ekranami w weekendy, podczas gdy osoby rozpoczynające korzystanie po 14. roku życia spędzają średnio 5,7 godziny. W świetle wyników badania, ponad połowa rodziców w UE wskazała dodatkowe ograniczenia wiekowe jako jedno z najskuteczniejszych działań służących ochronie zdrowia psychicznego młodych osób w środowisku cyfrowym[5].

Dzieci w okresie wczesnej i środkowej adolescencji (czyli między 11. a 15. rokiem życia), jak wskazuje Fundacja Dajemy Dzieciom Siłę, dopiero kształtują swoją tożsamość, a obecność w mediach społecznościowych może zakłócać ten proces. Obserwowanie wyidealizowanych obrazów innych osób może utrudniać budowanie realistycznego obrazu siebie[6]. Jak wynika z danych WHO[7], Polska znajduje się w pierwszej piątce państw europejskich o najwyższej liczbie sprawców i ofiar cyberprzemocy. Badania Rzecznika Praw Dziecka z 2025 r. pokazują, że w Polsce młodzi ludzie uważają hejt (84 %), stalking (77 %) i publikowanie treści bez zgody (74 %) za najbardziej szkodliwe zjawiska w sieci. Aż 97 % młodych ludzi zauważa szkodliwe zjawiska w Internecie, a tylko 1 % ankietowanych nie widzi żadnych zagrożeń online[8].

Serwisy społecznościowe mają własne regulaminy, które muszą być zaakceptowane przez użytkowników przed rozpoczęciem korzystania z platform. Regulaminy te często zawierają zapisy dotyczące minimalnego wieku użytkowników, zasad publikowania treści, ochrony prywatności oraz konsekwencji za naruszenie regulaminu. Minimalny wiek wymagany do samodzielnego założenia konta w serwisach społecznościowych to w większości 13 lat, jednak niektóre platformy wymagają ukończenia 16. lub 18. roku życia, w zależności od wyświetlanych treści.

Choć, jak wskazano powyżej, większość platform ustala w regulaminach minimalny wiek korzystania z usługi na poziomie 13 lat, w praktyce korzystają z nich także młodsze dzieci, w szczególności, że platformy te nie prowadzą (i nie mają mechanizmów) do realnej i rzetelnej weryfikacji wieku ich użytkowników. Raport Internet dzieci[9] pokazuje, że z aplikacji formalnie przeznaczonych dla osób w wieku 13 lat i więcej korzystają również użytkownicy w wieku 7–12 lat. Według ww. raportu, dzieci w wieku 7-12 lat przeznaczają aż 40% swojego czasu spędzanego w Internecie na korzystanie z platform społecznościowych. 1,2 mln dzieci w wieku 7-14 lat miało kontakt z reklamami piwa alkoholowego w aplikacjach mediów społecznościowych. Jednocześnie 69% dzieci w wieku 7-14 lat zagląda do serwisów edukacyjnych, ale spędza tam 6 minut dziennie podczas gdy całkowity czas ekranowy wynosi średnio dziennie 4 godziny i 25 minut. Część dzieci i młodzieży ma świadomość zagrożeń związanych z korzystaniem z Internetu, takich jak cyberprzemoc, oszustwa, nieodpowiednie treści i uzależnienie od Internetu, jednak wielu z nich nie wie, jak skutecznie chronić się przed tymi zagrożeniami.

Raport Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, dalej: „NASK-PIB", „Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców"[10] z 2025 r. wskazuje, że ponad połowa nastolatków (58 %) twierdzi, że ich rodzice nie ustalają żadnych zasad dotyczących korzystania z Internetu w zakresie czasu i dostępu do treści.

Dzieci i młodzież znajdują się w kluczowym etapie kształtowania swojej tożsamości, systemu wartości oraz zdolności do rozróżniania dobra od zła. W tym okresie są szczególnie podatni na wpływy zewnętrzne, w tym te pochodzące z Internetu. Osobom małoletnim brakuje narzędzi poznawczych, umożliwiających krytyczną analizę tego, co widzą, co może prowadzić do przyjmowania, chociażby podświadomie, takich zachowań za normę lub wzór do naśladowania.

[5] https://europa.eu/eurobarometer/surveys/detail/3686
[6] https://domowezasadyekranowe.fdds.pl/zasady/do-15-roku-zycia-bez-mediow-spolecznosciowych/
[7] https://iris.who.int/server/api/core/bitstreams/1d8d101a-e414-4635-a1dc-5cb50ed2b5da/content
[8] https://brpd.gov.pl/2025/02/12/spojrzmy-na-internet-oczami-dzieci-wyniki-badan-rpd/
[9] https://higienacyfrowa.pl/publikacje/internet-dzieci/
[10] https://www.nask.pl/nastolatki

Długotrwała ekspozycja na treści promujące negatywne wzorce objawia się u dzieci niskim poczuciem własnej wartości, depresją i wycofaniem społecznym.

Badania NASK-PIB wyraźnie pokazują, że zasady korzystania z Internetu w domu są inaczej postrzegane przez rodziców, a inaczej przez nastolatków. Tylko 21 % młodych ludzi twierdziło, że w ich rodzinach istnieją jasno określone reguły, aż 58% uważało, że takich zasad nie ma, a 21 % nie potrafiło jednoznacznie odpowiedzieć. Tymczasem rodzice w większości (57 %) byli przekonani, że w domu obowiązują określone zasady, choć 18 % z nich również nie miało co do tego pewności.

Rozbieżność ta może wynikać z różnic w rozumieniu przez obie grupy pojęcia „zasady". Podczas gdy rodzice mogą uznawać za zasady nieformalne ustalenia, ograniczenia czasowe czy okazjonalne zakazy, młodzież może postrzegać je jako niesystematyczne, arbitralne działania, które nie spełniają kryteriów stabilnego systemu normatywnego. Wskazuje to na potencjalny deficyt w zakresie komunikacji oraz brak wspólnego, jednoznacznego uzgodnienia oczekiwań i granic związanych z aktywnością online.

Interesujące jest to, że na przestrzeni lat niewiele się zmieniło. Porównanie wyników z 2022 r. i 2024 r. pokazało, że z perspektywy nastolatków coraz rzadziej obowiązywały ich zasady korzystania z Internetu (24 % vs. 21 %), a jednocześnie rosła liczba tych, którzy korzystali z sieci bez ograniczeń (54% vs. 58%). Rodzice natomiast w większości nadal deklarowali ustalanie reguł (59 % vs. 57 %), choć coraz częściej nie potrafili jednoznacznie określić swojego stanowiska („Trudno powiedzieć" wzrosło z 10 % do 18 %).

W świecie, w którym nastolatki są narażone na kontakt z nieodpowiednimi treściami, cyberprzemocą czy uzależnieniem od Internetu, brak jasnych zasad i wsparcia ze strony dorosłych może negatywnie wpływać na ich rozwój i bezpieczeństwo.

Dotychczasowe rozwiązania opierały się przede wszystkim na mechanizmach kontroli rodzicielskiej. Jak wynika zaś z przywoływanych wcześniej danych, rozwiązania te nie są odpowiednio skuteczne. Środki o charakterze wyłącznie edukacyjnym lub samoregulacyjnym, chociaż pożądane i istotne, nie gwarantują należytego poziomu ochrony małoletnim. Odpowiedzialność rodziców za wychowanie dziecka nie zwalnia zaś państwa z obowiązku podejmowania działań systemowych w sytuacji, gdy zagrożenie przyjęło tak masowy charakter.

Współczesne dzieciństwo i dorastanie przebiegają w środowisku silnie zdominowanym przez nowoczesne technologie. Smartfony, media społecznościowe i stały dostęp do Internetu nie tylko zmieniły sposoby uczenia się i budowania relacji, lecz także wprowadziły nowe formy zagrożeń psychospołecznych takich jak cyberprzemoc, naruszenia prywatności i danych osobowych, kontakt z niepożądanymi treściami, dezinformacja czy uzależnienie od Internetu.

Jak wynika z raportu z pierwszego Ogólnopolskiego Badania Higieny Cyfrowej i Aktywności Fizycznej Młodzieży (Instytut Cyfrowego Obywatelstwa, 2026)[11] 61 % nastolatków uważa, że spędza przed ekranami zbyt dużo czasu, a 62,7 % nastolatków słyszało o higienie cyfrowej, a głównym źródłem wiedzy jest szkoła.

Z kolei wyniki badania PISA 2025[12] wskazują, że na tle rówieśników z innych krajów, polskich piętnastolatków szczególnie wyróżnia duża częstotliwość codziennego wykorzystania urządzeń cyfrowych do spędzania czasu wolnego w szkole. Tylko 16 % polskich uczniów wskazało, że „wcale" nie korzysta z nich w tym celu, co stanowiło jeden z najniższych odsetków wśród krajów uczestniczących w badaniu (UE – 34 %, OECD – 36%).

Jednocześnie uczniowie wskazywali, że rozpraszają się korzystając z urządzeń cyfrowych w czasie lekcji (Polska – 74 %, UE – 59 %, OECD – 61 %). Na potrzebę bycia online i odpowiadania na wiadomości w czasie lekcji wskazywało aż 62% polskich piętnastolatków (UE 49 %, OECD 44 %). Dziewczęta częściej niż chłopcy zgłaszały niepokój z powodu braku telefonu oraz potrzebę bycia online.

[11] https://higienacyfrowa.pl/publikacje/raport-higiena-cyfrowa-mlodziezy/
[12] https://pisa.ibe.edu.pl/zasoby/#science

Edukacja cyfrowa musi więc zapewniać nabycie podstawowej wiedzy i umiejętności z zakresu odpowiedzialnego wykorzystywania zasobów cyfrowych i cyfrowego bezpieczeństwa, także ze względu na szeroki dostęp obywateli, w tym dzieci i młodzieży, do przestrzeni cyfrowej oraz wzrost zagrożenia cyberprzestępstwami. Zagrożenia w Internecie są coraz bardziej powszechne, a dezinformacja została uznana za jeden z najbardziej destabilizujących czynników dla społeczeństw europejskich. Wskazane jest, by edukacja w zakresie bezpieczeństwa cyfrowego była dostępna na jak najwcześniejszym etapie dostępu dzieci i młodzieży do przestrzeni cyfrowej, w sposób dostosowany do wieku odbiorcy. Według raportu „Nastolatki" (NASK-PIB, 2025) 28 %, czyli więcej niż co czwarty nastolatek, miał styczność z co najmniej jedną formą przemocy w przestrzeni cyfrowej motywowaną cechami osobistymi, tożsamością lub przekonaniami. W świetle ostatnich wydarzeń związanych z aktami przemocy fizycznej w szkołach, poważnym zagrożeniem jest zjawisko radykalizacji, której przejawy są widoczne także w przestrzeni cyfrowej. Ma ono realne skutki w prawdziwym życiu, dlatego tak ważne jest, aby dzieci i młodzież potrafiła zauważyć pierwsze symptomy niepokojących zachowań, i wiedziała, jak na nie zareagować.

Nie bez znaczenia pozostaje wpływ korzystania z Internetu na zdrowie psychiczne dzieci i młodzieży. Uzależnienie od mediów społecznościowych czy gier komputerowych jest zjawiskiem powszechnym. Raport „Nastolatki" (NASK-PIB, 2025) wskazuje, że współcześni nastolatkowie spędzają w Internecie średnio 4 godziny i 59 minut w dni powszednie. Średni czas korzystania z mediów społecznościowych wynosi natomiast 3 godziny i 49 minut wśród dziewcząt i 2 godziny 59 minut wśród chłopców. Warto zwrócić uwagę na różnicę w wykorzystywaniu Internetu ze względu na płeć. Dziewczęta częściej niż chłopcy korzystają z platform społecznościowych w celach związanych z socjalizacją, zarówno do kontaktów, jak i do wyrażania ekspresji. Chłopcy natomiast wybierają rozrywkę w postaci gier i konsumpcję treści, co może wiązać się z użytkowaniem serwisów związanych w dużym stopniu ze światem gier komputerowych (Discord i Twitch) oraz oglądaniem filmów poświęconych różnym obszarom tematycznym w serwisie YouTube.

Celem wychowania przedszkolnego i edukacji szkolnej w zakresie szeroko pojętego bezpieczeństwa cyfrowego jest więc przygotowanie najmłodszych do dokonywania świadomych i odpowiedzialnych wyborów w trakcie korzystania z zasobów dostępnych w Internecie, krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej, w tym nawiązywania i utrzymywania opartych na wzajemnym szacunku relacji z innymi użytkownikami sieci.

Zadania szkoły oraz obowiązkowe cele kształcenia i treści nauczania dotyczące bezpieczeństwa, w tym priorytety wychowawcze, określa podstawa programowa kształcenia ogólnego.

W podstawie programowej kształcenia ogólnego wskazuje się, że zadaniem szkoły jest zapewnienie uczniom bezpiecznych warunków oraz przyjaznej atmosfery do nauki. Najważniejszym celem kształcenia w szkole podstawowej jest dbałość o integralny rozwój biologiczny, poznawczy, emocjonalny, społeczny i moralny ucznia. Proces kształcenia i wychowania powinien wprowadzić uczniów w świat wartości, wskazać wzorce postępowania i budowania relacji społecznych sprzyjających bezpiecznemu rozwojowi ucznia (rodzina, przyjaciele), zbudować poczucie godności własnej osoby i szacunku dla godności innych osób, wyposażyć w zasób wiadomości oraz umiejętności, który pozwoli w sposób bardziej dojrzały i uporządkowany zrozumieć świat. Podstawa programowa podkreśla potrzebę rozwijania u uczniów postaw otwartości wobec świata i innych ludzi, aktywności w życiu społecznym oraz odpowiedzialności za zbiorowość.

Szkoła powinna przygotować uczniów do świadomego i odpowiedzialnego korzystania z technologii informacyjno-komunikacyjnych, wyposażyć ich w kompetencje potrzebne do korzystania z różnych cyfrowych zasobów informacyjnych, wyszukiwania i krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej, w tym nawiązywania i utrzymywania opartych na wzajemnym szacunku relacji z innymi użytkownikami sieci.

Cele kształcenia informatycznego – wymagania ogólne – są takie same dla wszystkich etapów edukacyjnych i dla wszystkich typów szkół. Ich uszczegółowienie następuje w ramach treści nauczania – wymagań szczegółowych. Treści podstawy programowej z informatyki mają charakter

przyrostowy, sugerując w ten sposób spiralny rozwój wiedzy, umiejętności i kompetencji uczniów przez wszystkie lata nauki szkolnej.

Cele kształcenia informatyki zdefiniowane w podstawie programowej obejmują m.in. przestrzeganie prawa i zasad bezpieczeństwa, respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocenę zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Przyjęte cele mają swoje odzwierciedlenie w treściach nauczania – wymaganiach szczegółowych określonych dla uczniów szkoły podstawowej i dla uczniów szkół ponadpodstawowych. W porównaniu ze szkołą podstawową, w liceum ogólnokształcącym i technikum wymagania z zakresu informatyki mają odpowiednio wyższy stopień trudności i są bardziej sproblematyzowane.

Na etapie edukacji wczesnoszkolnej (klasy I–III szkoły podstawowej) uczniowie rozwijają umiejętności w zakresie rozumienia, analizowania i rozwiązywania problemów, programowania i rozwiązywania problemów z wykorzystaniem komputera i innych urządzeń cyfrowych, posługiwania się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, rozwijania kompetencji społecznych, przestrzegania prawa i zasad bezpieczeństwa.

W klasach IV–VIII szkoły podstawowej uczniowie zapoznają się m.in. z:
• przyjętymi zasadami i prawem, w tym prawem do prywatności danych i informacji oraz prawem do własności intelektualnej,
• zagrożeniami związanymi z powszechnym dostępem do technologii oraz do informacji, metodami wystrzegania się ich,
• profilaktyką antywirusową, zabezpieczeniami przed zagrożeniem komputera wraz z zawartymi w nim informacjami,
• kwestiami etycznymi związanymi z wykorzystaniem komputerów i sieci, takimi jak: szacunek i kultura wypowiedzi (walka z wulgaryzmami, hejtem, mową nienawiści, trollingiem), ochrona prywatności i danych osobowych, przestrzeganie praw autorskich, piractwo, walka z dezinformacją, reagowanie na nękanie i szantaż, etyczne korzystanie ze sztucznej inteligencji.

Do katalogu najważniejszych umiejętności rozwijanych w szkołach ponadpodstawowych wpisano m.in. dbałość o poszanowanie praw autorskich i bezpieczne poruszanie się w cyberprzestrzeni.

Szkoła ma również przygotowywać uczniów do dokonywania świadomych i odpowiedzialnych wyborów w trakcie korzystania z zasobów dostępnych w Internecie, krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej, w tym nawiązywania i utrzymywania opartych na wzajemnym szacunku relacji z innymi użytkownikami sieci.

Podstawa programowa informatyki w szkole ponadpodstawowej – analogicznie jak w szkole podstawowej – wskazuje cel kształcenia jakim jest przestrzeganie prawa i zasad bezpieczeństwa, respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią.

Zgodnie z powyższym, wymagania szczegółowe wskazują, że uczeń:
• postępuje zgodnie z zasadami netykiety oraz regulacjami prawnymi dotyczącymi: ochrony danych osobowych, ochrony informacji oraz prawa autorskiego i ochrony własności intelektualnej w dostępie do informacji; jest świadomy konsekwencji łamania tych zasad;
• respektuje obowiązujące prawo i normy etyczne dotyczące korzystania i rozpowszechniania oprogramowania komputerowego, aplikacji cudzych i własnych oraz dokumentów elektronicznych;
• stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji;
• opisuje szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa.

W nauczaniu informatyki zostały zaakcentowane kompetencje społeczne. Wskazano np. bezpieczne budowanie swojego wizerunku w przestrzeni medialnej.

Zachowaniom bezpiecznym i odpowiedzialnym podczas korzystania z portali i mediów społecznościowych sprzyja ponadto realizacja treści nauczania zawartych w innych przedmiotach, takich jak: język polski, język obcy nowożytny, wiedza o społeczeństwie, etyka.

W ramach realizowanego od 1 września 2025 r. w szkołach ponadpodstawowych nowego przedmiotu pn. edukacja obywatelska, uczniowie w ramach wymagań szczegółowych wyjaśniają wpływ mediów tradycyjnych i społecznościowych na przekonania i postawy opinii publicznej oraz funkcjonowanie społeczeństwa, państwa i demokracji oraz wyjaśniają zagrożenia związane z upowszechnianiem niesprawdzonych informacji.

Nowy przedmiot – edukacja zdrowotna, realizowany w szkołach podstawowych i ponadpodstawowych od 1 września 2025 r. jako przedmiot nieobowiązkowy, a od 1 września 2026 r. jako obowiązkowy, umożliwia uczniom uzyskanie i rozwijanie wiedzy, umiejętności i kompetencji społecznych pozwalających na trafne rozpoznanie potrzeb zdrowotnych własnych i otoczenia oraz podejmowanie odpowiednich działań profilaktycznych czy naprawczych.

Treści zawarte w podstawie programowej kształcenia ogólnego w zakresie nowego przedmiotu edukacja zdrowotna mają pełnić rolę prewencyjną, szczególnie w przypadku przewidywanego możliwego pojawienia się u dzieci i młodzieży zachowań ryzykownych. Dział X dla szkół podstawowych oraz dział IX dla szkół ponadpodstawowych w całości poświęcony jest Internetowi i profilaktyce uzależnień. Uczy m.in.: przestrzegania zasad higieny cyfrowej; omawia: zagrożenia wynikające z niewłaściwego używania technologii informacyjno-komunikacyjnych, w tym, cyberprzemoc, hejt, mowę nienawiści, patostreaming, uzależnienie od gier i Internetu, niebezpieczne kontakty w sieci np.: uwodzenie w sieci; korzyści i zagrożenia związane z AI; zagrożenia związane z zażywaniem substancji psychoaktywnych oraz sposoby reagowania w sytuacjach występowania zagrożeń z korzystaniem z Internetu i substancji psychoaktywnych i ochronę prywatności, dezinformację, uzależnienia.

Obecnie w Instytucie Badań Edukacyjnych – Państwowym Instytucie Badawczym trwają prace eksperckie nad przygotowaniem projektu nowej podstawy programowej dla szkół ponadpodstawowych.

Także Polityka Cyfrowej Transformacji Edukacji (PCTE), przyjęta uchwałą nr 98 Rady Ministrów z dnia 12 września 2024 r., w sprawie przyjęcia polityki publicznej pod nazwą „Polityka Cyfrowej Transformacji Edukacji” (M.P. poz. 812), wskazuje na niezbędne działania, które powinny zostać podjęte dla pełnego urzeczywistnienia wizji nakreślonej w podstawie programowej kształcenia ogólnego, w dokumentach unijnych i innych dokumentach, w celu przygotowania kolejnych pokoleń obywateli do wyzwań społeczeństwa cyfrowego związanych z rozwojem informatyki i technologii cyfrowej. PCTE ma charakter programu i dokumentu strategicznego, wyznaczającego ramy polityki państwa i działań podejmowanych w obszarze cyfryzacji edukacji w perspektywie krótko, średnio oraz długoterminowej. Opisuje działania niezbędne do przeprowadzenia cyfrowej transformacji edukacji w obliczu rewolucji cyfrowej i wskazuje, że realizacją tych działań powinny zająć się przedszkola, szkoły, uczelnie i instytucje edukacyjne oraz administracja systemu oświaty w ramach cyfrowej transformacji edukacji, jako podstawowych działań cyfrowej transformacji społeczeństwa.

Najważniejsza część PCTE składa się z dziesięciu krótkich rozdziałów, w których w jednolitym układzie poruszono kwestie najbardziej istotne dla rozwoju cyfrowej edukacji i fundamentalne dla cyfrowej transformacji szkoły oraz całego systemu edukacji. PCTE wskazuje, iż w transformacji cyfrowej szkół bardzo ważną rolę pełnią inicjatywy skoncentrowane na zapewnieniu odpowiedniej higieny cyfrowej oraz bezpiecznym korzystaniu z komputera i Internetu.

Zagadnieniu cyberbezpieczeństwa poświęcono osobny rozdział w dokumencie – Cyfrowe bezpieczeństwo, w którym wskazano, że celem działań w obszarze edukacji jest sprawienie, aby użytkownik Internetu rozumiał i krytycznie oceniał różne aspekty mediów i kontekstów medialnych oraz tworzenia komunikacji w różnych kontekstach, świadomie korzystał np. z komunikatorów, platform elektronicznych, portali społecznościowych oraz miał świadomość zagrożeń związanych z dostępem do określonych treści, a także istnienia narzędzi ograniczających ich dostępność. PCTE wskazuje także, że jednym z celów działań ma być świadomość użytkowników o konieczności

zachowania higieny korzystania z urządzeń cyfrowych, w tym smartfonów. Wśród wskazanych w PCTE działań do zrealizowania w obszarze cyfrowego bezpieczeństwa można wymienić:
1.Wspieranie nauczania o edukacji medialnej, higienie cyfrowej i cyberbezpieczeństwie;
2.Opracowanie wytycznych dla nauczycieli i ram kompetencji uczniów w zakresie cyberbezpieczeństwa i higieny cyfrowej;
3.Opracowanie zasad systematycznego przeprowadzenia szkoleń dla nauczycieli i rodziców w zakresie cyberbezpieczeństwa.

W odniesieniu do technicznego aspektu zapewnienia bezpieczeństwa cyfrowego, art. 27 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2026 r. poz. 820, z późn. zm.) wskazuje wprost, że szkoły i placówki zapewniające uczniom dostęp do Internetu są obowiązane podejmować działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju, w szczególności zainstalować i aktualizować oprogramowanie zabezpieczające. W celu wspierania szkół w tym zadaniu, Ogólnopolska Sieć Edukacyjna zawiera usługę ochrony użytkownika OSE, która automatycznie monitoruje, wykrywa i blokuje dostęp do treści nielegalnych oraz szkodliwych dla uczniów w szkolnej sieci internetowej. Jest ona uruchamiana na wniosek dyrektora szkoły.

Promowanie higieny cyfrowej i bezpiecznego korzystania z Internetu jest stałym elementem priorytetowych kierunków realizacji polityki oświatowej państwa. Obejmuje m.in. rozwijanie krytycznego myślenia, odpowiedzialnego korzystania z technologii oraz przeciwdziałanie negatywnym skutkom nadmiernego używania urządzeń cyfrowych. W szkołach wykorzystywane są materiały edukacyjne dotyczące higieny cyfrowej opracowane przez NASK m.in. w ramach Ogólnopolskiej Sieci Edukacyjnej (OSE), w tym kursy, scenariusze lekcji oraz materiały dla nauczycieli, uczniów i rodziców. Realizowane są także szkolenia dla nauczycieli z zakresu umiejętności cyfrowych. Dodatkowo, na stronach MEN udostępniane są materiały informacyjne dotyczące edukacji medialnej (medialna.edu.pl) i higieny cyfrowej pn. „Informator dla rodziców i nauczycieli – zagrożenia ekranowe i w sieci". Ministerstwo Edukacji Narodowej uczestniczy także w europejskich inicjatywach dotyczących przeciwdziałania radykalizacji, dezinformacji i wzmacniania odporności społecznej, m.in. w ramach EU Knowledge Hub on Prevention of Radicalisation.

Ponadto, od 1 września 2026 r. obowiązują przepisy, wprowadzone ustawą z dnia 3 lipca 2026 r. o zmianie ustawy – Prawo oświatowe (Dz. U. poz. 1036), która reguluje korzystanie przez dzieci w przedszkolach, oddziałach przedszkolnych w szkołach podstawowych i innych formach wychowania przedszkolnego oraz uczniów w szkołach z telefonów komórkowych i innych urządzeń umożliwiających komunikację na odległość lub rejestrowanie obrazu lub dźwięku. Jednym z przewidzianych tam rozwiązań jest zakaz korzystania przez dzieci w przedszkolach, oddziałach przedszkolnych w szkołach podstawowych i innych formach wychowania przedszkolnego oraz uczniów w szkołach podstawowych dla dzieci i młodzieży z ww. telefonów komórkowych i urządzeń. W szkołach ponadpodstawowych oraz szkołach podstawowych dla dorosłych przewidziano natomiast możliwość wprowadzenia zakazu albo określenia innych warunków korzystania z ww. telefonów komórkowych i urządzeń w statutach tych szkół, z uwzględnieniem ustawowych wyjątków.

Projektowana ustawa jest komplementarna do ustawy z dnia 3 lipca 2026 r. o zmianie ustawy – Prawo oświatowe. Obie te interwencje legislacyjne służą bowiem wzmocnieniu higieny cyfrowej wśród dzieci i młodzieży.

Mając na uwadze powyższe, należy zapewnić, aby podstawa programowa wychowania przedszkolnego i podstawa programowa kształcenia ogólnego dla poszczególnych typów szkół uwzględniała aktualną wiedzę naukową oraz kładła nacisk na rozwijanie wiedzy i umiejętności dzieci i uczniów służących bezpieczeństwu cyfrowemu, w tym:
– ochronie urządzeń elektronicznych i treści cyfrowych,
– rozwijaniu świadomości cyfrowej,
– rozwijaniu wiedzy o zagrożeniach w środowisku cyfrowym i środkach bezpieczeństwa,
– ochronie prywatnych danych i prywatności,

– ochronie zdrowia i dbania o samopoczucie (higiena cyfrowa),
– rozwijaniu umiejętności reagowania na cyberprzemoc i przejawy radykalizacji,
– rozwijaniu wiedzy o wpływie nowoczesnych technologii i ich stosowania na środowisko.
Niezbędna jest także skuteczna realizacja przekazu skierowanego do uczniów, nauczycieli i rodziców w zakresie szeroko pojętego bezpiecznego korzystania z nowych technologii.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji i oczekiwany efekt

Konieczne jest wprowadzenie rozwiązań prawnych niezbędnych dla zapewnienia rzeczywistej ochrony zdrowia i praw dzieci. Projekt ustawy zakłada, że dostęp do internetowych serwisów społecznościowych będzie możliwy po ukończeniu 15. roku życia.

Internetowe serwisy społecznościowe mogą stwarzać ryzyko dla prywatności, bezpieczeństwa i ochrony małoletnich w wieku poniżej 15 lat. Przesłankami ryzyka dla prywatności i bezpieczeństwa są w szczególności wykorzystywanie systemu rekomendacji opartego na profilowaniu, czy udostępnianie funkcji lub rozwiązań informatycznych w celu zachęcenia użytkownika do długotrwałego i nieprzerwanego korzystania z usług internetowego serwisu społecznościowego.

Wiek 15 lat jest o tyle szczególny, że w świetle polskiego prawa stanowi granicę ochrony przed niektórymi czynami (np. art. 200 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2026 r. poz. 1342) odnoszący się do seksualnego wykorzystania małoletniego poniżej 15 roku życia)).

Wiek 15 lat w polskim systemie edukacji zbiega się zazwyczaj z ukończeniem szkoły podstawowej. Jest to naturalny moment osiągnięcia pewnego pułapu „dojrzałości cyfrowej". Starsza młodzież lepiej radzi sobie z weryfikacją fake newsów, manipulacją oraz potrafi stawiać wyraźniejsze granice w relacjach z obcymi osobami w sieci. Profile w mediach społecznościowych często prezentują wyidealizowany, nierealistyczny obraz życia i wyglądu. U dzieci poniżej 15. roku życia, które dopiero budują swoją tożsamość, rodzi to frustrację, kompleksy oraz drastycznie obniża samoocenę.

Dodatkowo, w wieku 15 lat dzieci są bardziej dojrzałe poznawczo i emocjonalnie, co pozwala im lepiej zrozumieć i ocenić ryzyko związane z korzystaniem z mediów społecznościowych i pozwala skuteczniej weryfikować treści. Są też bardziej świadome zagrożeń związanych z korzystaniem z mediów społecznościowych, takich jak cyberprzemoc, oszustwa, nieodpowiednie treści czy uzależnienia. Mają też większą zdolność do podejmowania świadomych decyzji i zarządzania swoją prywatnością online. Granica 15 lat znajduje uzasadnienie w podstawie programowej kształcenia ogólnego, biorąc też pod uwagę względy praktyczne: co do zasady w wieku 15 lat dzieci kończą szkołę podstawową i rozpoczynają kształcenie w szkole ponadpodstawowej. Ustalenie tego progu wiekowego na innym poziomie (np. 13 albo 16 lat) powodowałoby to, że w danej szkole część uczniów byłaby uprawniona do korzystania z mediów społecznościowych, a część nie. Takie rozróżnienie negatywnie wpłynęłoby na skuteczność proponowanych rozwiązań. Do tego, dzięki działaniom realizowanym w szkołach podstawowych, w wieku 15 lat uczniowie powinni już posiadać podstawowe kompetencje niezbędne do bezpiecznego i odpowiedzialnego funkcjonowania w środowisku cyfrowym, umiejętności krytycznej analizy informacji, logicznego myślenia, oceny wiarygodności źródeł oraz świadomego korzystania z technologii cyfrowych.

Wiele krajów na świecie przyjęło lub planuje przyjąć podobne granice wiekowe w dostępie do internetowych serwisów społecznościowych. Przepisy zakazujące korzystania z mediów społecznościowych poniżej 15. roku życia procedowane są m.in. we Francji, Danii, Szwecji. W niektórych krajach granica wieku podniesiona jest do 16. roku życia (przykład obowiązujących przepisów w Australii oraz procedowanych przepisów o zakazie mediów społecznościowych w Wielkiej Brytanii, Irlandii czy Hiszpanii). Kierunek zmian obserwowany w wielu państwach wskazuje na rosnące przekonanie, że granica 15-16 lat odpowiada poziomowi dojrzałości pozwalającemu na bardziej świadome i bezpieczne korzystanie z mediów społecznościowych.

Analiza rozwiązań legislacyjnych rozważanych obecnie w państwach europejskich pokazuje, że propozycje dotyczące ustanowienia minimalnego wieku dostępu do internetowych serwisów społecznościowych różnią się pod względem zakresu regulacji, przyjętych limitów wiekowych oraz rodzaju stosowanych ograniczeń.

W zakresie przedmiotowym część państw, takich jak Grecja i Francja, koncentruje się na platformach internetowych kwalifikowanych jako serwisy społecznościowe w rozumieniu unijnych aktów cyfrowych. Inne kraje przyjmują szersze lub bardziej złożone podejście. Przykładowo Norwegia proponuje objęcie regulacją usług, które ze względu na swoją konstrukcję, funkcjonalności lub prezentowane treści mogą negatywnie oddziaływać na rozwój emocjonalny, poznawczy, zdrowotny lub bezpieczeństwo dzieci. Belgia również przewiduje szeroki zakres podmiotowy, obejmujący usługi pośrednie, przy jednoczesnym uwzględnieniu kryterium potencjalnego negatywnego wpływu na rozwój małoletnich. Z kolei Austria odwołuje się do definicji platform udostępniania wideo, które oferują funkcjonalności uznawane za szkodliwe dla dzieci, natomiast we Włoszech proponuje się objęcie ograniczeniami zarówno serwisów społecznościowych, jak i platform udostępniania materiałów wideo.

Różnice dotyczą również proponowanego minimalnego wieku użytkowników. Projekty ustaw przygotowane we Francji i Grecji przewidują zakaz korzystania z określonych usług przez osoby poniżej 15. roku życia. W Norwegii rozważane jest ustanowienie granicy wieku na poziomie 16 lat, podczas gdy w innych państwach pojawiają się propozycje wprowadzenia limitów 13 lub 14 lat. Dyskutowane są również rozwiązania umożliwiające korzystanie z usług przez młodsze osoby za zgodą rodziców lub opiekunów prawnych. W niektórych systemach prawnych limit wieku odnosi się do faktycznego wieku użytkownika, natomiast w innych do roku kalendarzowego, w którym dana osoba osiąga określony wiek.

Poszczególne państwa odmiennie definiują także zakres ograniczeń. W większości projektów mowa jest o ograniczeniu „dostępu" do usług, jednak nie zawsze jest jasne, czy chodzi wyłącznie o możliwość utworzenia konta użytkownika, czy też o całkowity dostęp do danej platformy. Rozróżnienie to ma istotne znaczenie, ponieważ ograniczenie możliwości założenia konta nie musi uniemożliwiać korzystania z części funkcji lub treści dostępnych bez logowania.

W wielu państwach propozycje legislacyjne wykraczają poza samo ustanowienie minimalnego wieku użytkowników i obejmują dodatkowe obowiązki związane z weryfikacją wieku oraz projektowaniem usług z uwzględnieniem bezpieczeństwa dzieci. Przykładowo Grecja planuje nałożyć na dostawców usług obowiązek stosowania odpowiednich, proporcjonalnych i wiarygodnych metod weryfikacji wieku, które mogą być uzupełniane metodami jego szacowania. Austria z kolei przewiduje szczegółowe wymagania dotyczące systemów weryfikacji wieku, obejmujące m.in. zasadę minimalizacji danych, funkcjonalne oddzielenie dostawcy usługi od podmiotu weryfikującego wiek, brak możliwości śledzenia użytkownika na podstawie danych uwierzytelniających wiek oraz interoperacyjność stosowanych rozwiązań.

Doświadczenia państw europejskich wskazują zatem, że mimo wspólnego celu, jakim jest zwiększenie poziomu ochrony dzieci i młodzieży w środowisku cyfrowym, nie wykształcił się jeszcze jednolity model regulacyjny dotyczący minimalnego wieku dostępu do mediów społecznościowych. Przedmiotem dalszych dyskusji pozostają zarówno zakres usług objętych regulacją, właściwy próg wiekowy, jak i sposób skutecznego oraz proporcjonalnego egzekwowania nowych obowiązków. Nie jest więc możliwe przyjęcie jako wzoru, modelu już funkcjonującego w innym kraju europejskim, którego skuteczność została potwierdzona. Dlatego Polska wypracowała własne propozycje regulacji przedmiotowego obszaru.

Zgodnie z definicją przyjętą w art. 2 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 z dna 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych), internetowy serwis społecznościowy oznacza platformę umożliwiającą użytkownikom końcowym łączenie się i komunikowanie ze sobą, udostępnianie treści oraz zapoznawanie się z innymi użytkownikami i treściami z wykorzystaniem różnych urządzeń, w szczególności za pośrednictwem czatów, postów, filmów wideo i rekomendacji).

W potocznym rozumieniu mówi się w tym przypadku o mediach społecznościowych. Serwisy te posiadają różne funkcje, takie jak czaty, posty, filmy wideo czy rekomendacje. Przykłady takich serwisów to m.in. TikTok, Facebook, Instagram. Internetowy serwis społecznościowy to specyficzny rodzaj platformy online, na której użytkownicy budują relacje społeczne, nawiązują kontakty i dzielą się treściami. W założeniu służyć ma do wymiany informacji o wspólnych zainteresowaniach,

kwestiach zawodowych, aktywnościach czy prywatnym życiu. Serwisy te różnią się pod względem formatu i liczby oferowanych funkcji, w tym narzędzi komunikacji i rodzajów udostępnianych treści. Typowymi funkcjami takich platform są możliwość publikacji zdjęć, filmów oraz udostępnianie treści (wpisów, postów). Serwisy społecznościowe umożliwiają użytkownikom tworzenie własnych profili oraz budowanie sieci kontaktów[13].

Ze względu na małe prawdopodobieństwo wyrządzania szkody małoletnim wyłączone z zakresu projektu są encyklopedie internetowe, repozytoria, usługi i systemy edukacyjno-naukowe, platformy tworzenia otwartego oprogramowania i platformy wymiany otwartego oprogramowania, usługi i systemy opracowane i obsługiwane wyłącznie do celów badań naukowych i rozwoju oraz usługi i systemy zaprojektowane, opracowane i obsługiwane przez organy publiczne i do wyłącznego użytku tych organów publicznych lub w ich imieniu.

W projekcie ustawy zakłada się, że weryfikacja wieku przez internetowe serwisy społecznościowe będzie mogła następować za pomocą:
1) elektronicznego poświadczenia atrybutów potwierdzającego osiągnięcie określonego progu wieku, udostępnianego w ramach europejskiego portfela tożsamości cyfrowej, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE, zmienionym rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 1183 z późn. zm.), zwanym dalej „rozporządzeniem eIDAS”;
2) usługi w aplikacji mObywatel, która będzie oparta o mechanizm selektywnego przekazywania informacji dotyczącej wieku;
3) narzędzia informatycznego wpisanego na listę, prowadzoną przez ministra właściwego do spraw informatyzacji, pozwalającego na selektywne przekazywanie informacji dotyczącej wieku.

Każde z tych rozwiązań będzie oparte o zasadę selektywnego przekazywania informacji o użytkowniku. Będzie ono potwierdzać tylko fakt posiadania określonego wieku, osiągnięcia określonego progu wiekowego lub znajdowania się w określonym przedziale wiekowym, bez dodatkowego przekazywania innych informacji, takich jak np. imię i nazwisko. Rozwiązania te zapewnią tym samym prywatność użytkownikom, równocześnie realizując podstawowy cel projektu, czyli ograniczenie dostępu do mediów społecznościowych osobom poniżej ustawowego progu wieku. Rozwiązania te znajdą zastosowanie nie tylko w przypadku weryfikacji wieku w internetowych serwisach społecznościowych.

W związku z powyższym celowym jest sięgnięcie po funkcje, jakie oferować będzie europejski portfel tożsamości cyfrowej. Zgodnie z rozporządzeniem eIDAS pozwalać będzie on użytkownikom m. in. na bezpieczne żądanie, otrzymywanie, wybieranie, łączenie, przechowywanie, usuwanie, udostępnianie i prezentację – pod wyłączną kontrolą użytkownika – danych identyfikujących osobę oraz, w stosownych przypadkach, w połączeniu z elektronicznymi poświadczeniami atrybutów, uwierzytelnianie wobec stron ufających (usługodawców) w trybie online oraz, w stosownych przypadkach, w trybie offline, w celu uzyskania dostępu do usług publicznych i prywatnych, przy jednoczesnym zapewnieniu możliwości selektywnego ujawniania danych (art. 5a ust. 4 lit. a rozporządzenia eIDAS).

Założeniem rozporządzenia eIDAS jest, aby europejskie portfele tożsamości cyfrowej działały na terenie całej Unii Europejskiej. Pozwolą one na selektywne przekazywanie tylko określonych atrybutów (np. informacja o wieku czy informacja o przekroczeniu określonego progu wiekowego), które mogą być wykorzystywane w usługach online podmiotów publicznych i niepublicznych. Tym

[13] *K. Drążewski, M. Grochowski, G. Materna, J. Mazur, K. M. Szreder, M. Wilczyńska, B. Wołodkiewicz* [w:] *M. Grochowski* (red.), Akt o rynkach cyfrowych – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828. Komentarz [w:] Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-busines, Nb 11–12.

samym pozwolą one, aby dostawca określonej usługi online (np. podmiot odpowiedzialny za internetowy serwis społecznościowy) otrzymał jedynie informację o tym, że dany użytkownik posiada więcej niż np. 15 lat bez przekazywania innych danych tego użytkownika jak np. jego imię i nazwisko.

Zasadnym jest w tym zakresie sięgnięcie także po aplikację mObywatel, która posiada już ponad 13 milionów użytkowników – zostanie stworzona dedykowana usługa, pozwalająca na potwierdzanie wieku.

Biorąc pod uwagę, że europejski portfel tożsamości cyfrowej i aplikacja mObywatel są narzędziami dobrowolnymi oraz ciągły rozwój rozwiązań cyfrowych i pojawianie się nowych technologii zasadnym jest umożliwienie selektywnego potwierdzania wieku także w oparciu o inne zaufane rozwiązania. Będą one wpisywane na listę zaufanych rozwiązań w zakresie weryfikacji wieku, prowadzoną przez ministra właściwego do spraw informatyzacji. Lista obejmie podmioty krajowe oraz z Unii Europejskiej, które spełniają wymagania określone w rozporządzeniu wydanym przez ministra właściwego do spraw informatyzacji. Rozwiązanie nie może umożliwiać identyfikacji użytkownika ani jego lokalizowania, śledzenia, targetowania, profilowania lub wysyłania reklam do użytkownika.

Potwierdzenie wieku użytkownika polegać będzie na ustaleniu czy osoba zakładająca konto użytkownika lub posiadająca konto użytkownika ukończyła lat piętnaście. Dodatkowo dostawca internetowego serwisu społecznościowego będzie obowiązany ponawiać potwierdzenie wieku użytkownika, jeżeli na podstawie posiadanych przez niego informacji poweźmie wątpliwości dotyczące osiągnięcia minimalnego wieku dostępu do internetowych serwisów społecznościowych lub udostępnienia konta użytkownika osobie trzeciej, która takiego wieku nie osiągnęła.

Weryfikacja wieku nie będzie dokonywana każdorazowo. Założeniem projektu jest, że dostawca internetowego serwisu społecznościowego nie będzie mógł zezwolić małoletniemu poniżej minimalnego wieku dostępu do internetowych serwisów społecznościowych:

- na założenie konta użytkownika lub
- na dostęp do internetowego serwisu społecznościowego za pośrednictwem konta utworzonego dla tej osoby lub przypisanego do niej.

Projekt będzie dotyczył również kont już istniejących.

Organem odpowiedzialnym za nadzór nad przestrzeganiem przepisów projektowanej ustawy będzie Prezes Urzędu Komunikacji Elektronicznej, wykorzystując uprawnienia, które posiada jako koordynator do spraw usług cyfrowych w stosunku do dostawców usług pośrednich na podstawie ustawy o świadczeniu usług drogą elektroniczną, w zakresie umożliwiającym stosowanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (Akt o usługach cyfrowych).

Prezes UKE będzie ponadto dysponował uprawnieniami kontrolnymi wynikającymi z ustawy o świadczeniu usług drogą elektroniczną.

Projekt będzie wykorzystywał system nadzoru nad dostawcami usług pośrednich, który wynika z polskiego wdrożenia Aktu o usługach cyfrowych. Obejmuje to przepisy dot. kontroli i kar administracyjnych w wysokości do 6% globalnych obrotów dostawcy internetowego serwisu społecznościowego.

Ponadto, proponuje się dodanie przepisu wzmacniającego obecność w podstawie programowej wychowania przedszkolnego i podstawie programowej kształcenia ogólnego treści nauczania z zakresu: zasad higieny cyfrowej, w tym dotyczących wpływu nadużywania urządzeń ekranowych na zdrowie psychiczne i fizyczne, zasad cyberbezpieczeństwa, w tym ochrony prywatności i bezpieczeństwa w cyfrowym świecie oraz zagrożeń wynikających z niewłaściwego używania technologii informacyjno-komunikacyjnych, w szczególności odnoszących się do cyberprzemocy i mowy nienawiści, uzależnienia od Internetu i gier komputerowych oraz niebezpiecznych kontaktów w sieci, dostosowane

do wieku dzieci objętych wychowaniem przedszkolnym oraz uczniów. Zapewni to szerszą realizację w przedszkolach i szkołach zagadnień, które są kluczowe z punktu widzenia cyfrowego rozwoju społeczeństwa.

Projektowana ustawa stanowi o obowiązku zawarcia w podstawie programowej wychowania przedszkolnego oraz podstawach programowych kształcenia ogólnego w każdym typie szkoły obowiązkowych do realizacji treści nauczania z powyższego zakresu.

Jednocześnie projektowana zmiana nie łączy się z obligatoryjnym zwiększeniem w szkołach liczby godzin zajęć edukacyjnych. Treści te będą realizowane m. in. podczas zajęć edukacji zdrowotnej, informatyki i cyberbezpieczeństwa, edukacji obywatelskiej, historii, wychowania fizycznego oraz zajęć z wychowawcą.

Korzystanie z nowych technologii przez uczniów, jak wskazano w części 1 OSR, jest powszechne, a brak odpowiedniej edukacji może nieść za sobą poważne konsekwencje w takich obszarach jak:
1. Ochrona zdrowia psychicznego i fizycznego (Higiena cyfrowa)
• Zapobieganie przebodźcowaniu i uzależnieniom: Szkoła ucząca higieny cyfrowej pomaga uczniom zrozumieć mechanizmy uzależniające (np. algorytmy social mediów) i uczy, jak świadomie kontrolować czas spędzany przed ekranem.
• Zdrowy rozwój i sen: Edukacja w tym zakresie zwraca uwagę na negatywny wpływ niebieskiego światła na jakość snu oraz na konieczność zachowania równowagi między światem online a aktywnością fizyczną i relacjami w świecie realnym.
2. Bezpieczeństwo osobiste i przeciwdziałanie zagrożeniom
• Rozpoznawanie niebezpieczeństw: Młodzi ludzie często nie są świadomi ryzyka, takiego jak cyberprzemoc (hejting, nękanie), zjawiska radykalizacji przejawiającego się także w przestrzeni cyfrowej, grooming (manipulacja przez dorosłych w sieci) czy kontakt z patotreściami.
• Budowanie odporności na manipulację: Znajomość zagrożeń pozwala uczniom szybciej reagować na próby oszustwa, wyłudzenia czy dezinformację (fake newsy).
3. Świadome zarządzanie własną prywatnością
• Cyfrowy ślad (Digital Footprint): Edukacja uświadamia młodym ludziom, że raz zamieszczone w internecie zdjęcie, film czy komentarz mogą pozostać tam na zawsze i wpłynąć na ich przyszłą karierę lub relacje.
• Ochrona danych osobowych: Uczniowie dowiadują się, jak tworzyć silne hasła, dlaczego nie należy podawać obcym adresu czy numeru telefonu oraz jak działają uprawnienia aplikacji, które instalują na telefonach.
4. Wyrównywanie szans społecznych
• Różny poziom wiedzy w domach: Nie każdy rodzic posiada wystarczające kompetencje cyfrowe, by nauczyć dziecko bezpiecznego poruszania się w przestrzeni cyfrowej. Szkoła staje się miejscem, które gwarantuje każdemu uczniowi – bez względu na pochodzenie – dostęp do wiedzy na równym poziomie.
Minister właściwy do spraw oświaty i wychowania będzie mógł realizować działania informacyjne i promocyjne w powyższym zakresie, a także zlecać ich realizację podległym mu jednostkom lub przez niego nadzorowanych. Będzie mógł także, w drodze konkursu, zlecać realizację działań informacyjnych i promocyjnych organizacjom pozarządowym, w tym organizacjom harcerskim, instytutom badawczym, instytucjom kultury czy podmiotom prowadzącym statutową działalność w zakresie oświaty i wychowania. Rozwiązanie to umożliwi również prowadzenie działań edukacyjnych i profilaktycznych na poziomie ogólnokrajowym i lokalnym, zwiększając ich zasięg, skuteczność oraz oddziaływanie społeczne.

Obecnie działania z zakresu bezpieczeństwa cyfrowego, realizowane przez podległy ministrowi właściwemu do spraw oświaty i wychowania Ośrodek Rozwoju Edukacji (ORE), mają głównie formę pojedynczych, fakultatywnych kursów e-learningowych oraz publikacji materiałów pomocniczych dla nauczycieli na Zintegrowanej Platformie Edukacyjnej. Działania te mają charakter rozproszony i trafiają głównie do nauczycieli informatyki oraz wybranej kadry pedagogicznej w ramach standardowej oferty szkoleniowej. Wejście w życie ustawy wpłynie na objęcie wsparciem szkoleniowym ogółu kadry pedagogicznej. Działania ORE będą ilościowo i jakościowo rozszerzone o zwiększenie grupy docelowej, materiały i narzędzia dydaktyczne, zasięg i skalę.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

W październiku 2025 r. w deklaracji jutlandzkiej, podpisanej przez 25 państw członkowskich UE, wezwano do wprowadzenia weryfikacji wieku oraz stworzenia bezpieczniejszego środowiska internetowego dla małoletnich. Znaczenie ochrony małoletnich w internecie, w tym w kontekście cyfrowej pełnoletności, podkreśliła również Rada Europejska w konkluzjach z marca 2026 r. oraz października 2025 r. Z kolei Parlament Europejski w sprawozdaniu z listopada 2025 r. w sprawie ochrony małoletnich w internecie wezwał do ustanowienia zharmonizowanego europejskiego limitu wieku cyfrowego na poziomie 16 lat w odniesieniu do dostępu do mediów społecznościowych, platform udostępniania plików wideo oraz towarzyszy opartych na sztucznej inteligencji — chyba że rodzice lub opiekunowie zezwolą dziecku na korzystanie z tych usług wcześniej. Postulował ponadto ustanowienie bezwzględnego limitu wieku wynoszącego 13 lat, poniżej którego żaden małoletni nie mógłby uzyskać dostępu do platform mediów społecznościowych, niezależnie od zgody rodziców. Parlament wskazał również na potrzebę wprowadzenia dodatkowych przepisów dotyczących projektowania dostosowanego do wieku oraz uwzględniania bezpieczeństwa już na etapie projektowania usług, a także wezwał do przyjęcia jednolitego europejskiego podejścia do weryfikacji wieku, które zapewniłoby pewność prawa.

Komisja Europejska od lat aktywnie wspiera inicjatywy na rzecz poprawy bezpieczeństwa dzieci w internecie. Jednym z kluczowych projektów w tym obszarze jest Better Internet for Kids, którego celem jest podnoszenie świadomości na temat zagrożeń w sieci oraz dostarczanie dzieciom, rodzicom, nauczycielom i opiekunom narzędzi i zasobów służących bezpiecznemu korzystaniu z Internetu. W ramach inicjatywy organizowane są kampanie edukacyjne, prowadzone są analizy zagrożeń online oraz promowane są dobre praktyki w zakresie bezpieczeństwa w sieci. Projekt wspiera także współpracę międzynarodową, angażując organizacje zajmujące się ochroną dzieci w internecie na poziomie globalnym.

W całej Unii Europejskiej państwa członkowskie prowadzą prace nad przepisami krajowymi mającymi na celu zwiększenie bezpieczeństwa dzieci w internecie. W latach 2025–2026 w ramach procedury TRIS zgłoszono kilka projektów dotyczących ograniczeń wiekowych w odniesieniu do wybranych rodzajów usług cyfrowych (Włochy, Francja, Norwegia, Grecja, Austria, Belgia). W niemal wszystkich pozostałych państwach członkowskich trwają natomiast konsultacje, prace parlamentarne lub zapowiedziano odpowiednie inicjatywy rządowe. Przepisy krajowe różnią się między sobą zakresem, przyjętymi granicami wiekowymi oraz rodzajem wprowadzanych ograniczeń. Państwa proponują odmienne definicje i kryteria kwalifikowania usług cyfrowych objętych ograniczeniami, a także różne progi wiekowe — od 13 do 16 lat — zależne ostatecznie od zgody rodziców. Część projektowanych przepisów krajowych przewiduje ponadto dodatkowe obowiązki w zakresie bezpieczeństwa już na etapie projektowania usług.

W Australii od grudnia 2025 r. osoby poniżej 16. roku życia mają zakaz korzystania z głównych serwisów społecznościowych, w tym Tiktok, X, Facebook, Instagram, YouTube, Snapchat i Threads. Nie mogą zakładać nowych kont, a istniejące profile są dezaktywowane. Zakaz nie obejmuje jednak komunikatorów internetowych, które dostępne są, zgodnie z regulaminem korzystania z większości tego rodzaju usług, dla osób które ukończyły 13 lat.

Do zadań rządowego organu w Australii, eSafety Commissionera, należy m.in. monitorowanie skuteczności wprowadzonych rozwiązań w zakresie dostępu dzieci do mediów społecznościowych. W ramach tej działalności zespół tego organu wydał w 2026 r. dwa raporty omawiające skuteczność obowiązujących regulacji – jeden skupiający się bardziej na platformach cyfrowych[14], a drugi poświęcony perspektywie dzieci i ich rodziców[15]. Z tych raportów wynika, że w grupie wiekowej 10-15 lat dostrzeżono statystycznie istotną różnicę w posiadaniu co najmniej jednego konta w mediach

[14] https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf?v=1792995800730

[15] https://www.esafety.gov.au/sites/default/files/2026-08/Early-days-Early-Insights-SMMA-Evaluation-Understanding-experiences-of-social-media-age-restrictions-August2026.pdf?v=1792995831654

społecznościowych. Na początku obowiązywania zakazu takie konto posiadało 52,4% dzieci w tej grupie wiekowej, podczas gdy trzy miesiące później takie konto posiadało 42,1% dzieci. Zdaniem eSafety Commissioner, powodem tego, że stosunkowo duża grupa dzieci wciąż korzysta z kont w mediach społecznościowych jest nieefektywna implementacja metod weryfikacji wieku przez platformy cyfrowe (raport z przypisu nr 10, s. 7). To ryzyko jest w przypadku Polski zmniejszone dzięki unijnym oraz krajowym mechanizmom weryfikowania wieku, które zostały opisane w pkt 2 OSR-u, a które w przypadku Australii nie są tak silnie przygotowane.

W związku z tym, we wrześniu 2026 r. australijski parlament przyjął ustawę, która wzmacnia egzekwowanie zakazu m.in. poprzez poszerzenie kompetencji eSafety Commissioner oraz dwukrotne podwyższenie maksymalnych wysokości kar, które można nałożyć na platformy cyfrowe za niewywiązywanie się z postanowień dotyczących dostępu dzieci do mediów społecznościowych - *Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Bill 2026*.

W przypadku Francji, w sierpniu 2026 r. francuski parlament uchwalił ustawę, która wprowadzała podobne jak w Australii zakazy korzystania przez dzieci poniżej 15. roku życia z mediów społecznościowych, z wyjątkami m.in. w zakresie internetowych encyklopedii oraz platform i repertoriów edukacyjnych i naukowych (*LOI n° 2026-813 du 24 août 2026 visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux*). Jej zasadnicza część została jednak uznana przez Radę Konstytucyjną za niezgodną z francuską ustawą zasadniczą. Nowy projekt ustawy, utrzymujący główne założenia i uwzględniający orzeczenie Rady Konstytucyjnej, został przez francuski rząd przedstawiony w połowie września 2026 r. Komisji Europejskiej i niebawem zostanie wniesiony pod obrady francuskiego parlamentu.

W przypadku pozostałych państw unijnych, które zgłosiły swoje projekty w opisywanym wymiarze w ramach procedury TRIS, szczegóły zaproponowanych rozwiązań dopiero będą ustalane przez poszczególne państwa członkowskie Unii Europejskiej, na razie pozostając na wysokim poziomie ogólności.

Z przykładów Australii i Francji można wyciągnąć istotne wnioski, gdy idzie m.in. o konieczność wprowadzenia realnych mechanizmów weryfikowania wieku użytkowników, opartych o rozwiązania unijne i krajowe (opisane w pkt 2 OSR-u i znacznie silniejsze niż w przypadku Australii). Brak takich mechanizmów albo przygotowanie ich w sposób mało skuteczny silnie oddziałuje również na skuteczność samych wprowadzanych zasad korzystania z mediów społecznościowych przez dzieci i młodzież.

Obecnie toczą się prace nad projektem tzw. EU Kids Act, ujednolicającego podejście do weryfikacji wieku w platformach społecznościowych w całej Unii Europejskiej. Projekt EU Kids Act jest zbieżny z założeniami przedmiotowego projektu ustawy. Z chwilą wejścia opracowywanych przepisów unijnych przepisy krajowe zostaną dostosowane do przepisów europejskich w tym zakresie.

Ramy strategiczne i rekomendacje organizacji międzynarodowych (UNESCO, OECD, Unia Europejska)

Powszechny dostęp dzieci i młodzieży do przestrzeni cyfrowej oraz rosnące zagrożenia wymusiły wypracowanie spójnych ram przeciwdziałania tym zjawiskom na poziomie globalnym. Problem braku higieny cyfrowej oraz negatywnego wpływu niekontrolowanego korzystania z urządzeń cyfrowych na uczniów jest przedmiotem różnego typu dokumentów i wytycznych organizacji międzynarodowych i ponadnarodowych.

1. Wytyczne UNESCO

Raport UNESCO Global Education Monitoring Report 2023 („Technology in education: A tool on whose terms?") zarekomendował państwom wprowadzanie regulacji i ograniczeń w stosowaniu smartfonów na terenie placówek oświatowych. W raporcie wykazano, że sama obecność urządzenia mobilnego w pobliżu ucznia wywołuje mikrorozproszenia, które obniżają koncentrację i pogarszają wyniki w nauce, zwłaszcza u uczniów osiągających najsłabsze rezultaty edukacyjne. UNESCO wskazało również, że nadmierny czas ekranowy jest powiązany ze zmniejszeniem ciekawości poznawczej i samokontroli, chwiejnością emocjonalną oraz wyższym ryzykiem stanów lękowych i depresyjnych. Ponadto, zwrócono uwagę na potrzebę ochrony danych osobowych najmłodszych,

wskazując, że znaczna część aplikacji edukacyjnych stosowanych powszechnie podczas pandemii gromadziła dane dzieci z naruszeniem ich prawa do prywatności. Jednocześnie UNESCO zarekomendowało państwom ustanowienie ram kompetencji cyfrowych niezwiązanych z konkretną technologią (technology-neutral). Zalecono również wzmocnienie w szkołach działań profilaktycznych dla uczniów dotyczących rozpoznawania zagrożeń związanych z hasłami, uprawnieniami aplikacji i konsekwencjami pozostawiania cyfrowego śladu w internecie. Wskazano ponadto na potrzebę przyjęcia i wdrożenia przepisów chroniących prawa człowieka, dobrostan i bezpieczeństwo online uczniów i nauczycieli. Raport uzupełniający przygotowany z udziałem młodzieży w 2024 r. („Technology in education: a tool on our terms!") zawiera rekomendację, aby moduły dotyczące bezpieczeństwa online były integrowane do programów nauczania.

2. Wyniki badań i wnioski analityczne OECD (PISA)

Cykliczne badanie umiejętności uczniów PISA prowadzone przez OECD, stanowi jeden z punktów odniesienia w debacie publicznej i decyzjach dotyczących polityki edukacyjnej w państwach członkowskich. Analizy PISA wskazują na związek między sposobem korzystania przez uczniów z urządzeń cyfrowych a ich osiągnięciami edukacyjnymi. W badaniu PISA 2025 odsetek piętnastolatków wskazujących, że uczniowie rozpraszają się podczas lekcji korzystając z urządzeń cyfrowych, wyniósł w Polsce 74%, wobec średnio 59% w krajach UE i 61% w krajach OECD. Potrzebę ciągłego bycia online i natychmiastowego odpowiadania na wiadomości w czasie lekcji odczuwa 62% nastolatków w Polsce (przy średniej UE na poziomie 49% i OECD – 44%). Badania PISA wskazują, że rekreacyjne korzystanie z technologii w szkole przekraczające jedną godzinę dziennie może prowadzić do spadku wyników nauczania, m.in. z matematyki i czytania ze zrozumieniem. Wyniki te pokazują, że szkoła powinna nie tylko ograniczać sytuacje, w których urządzenia cyfrowe zakłócają przebieg lekcji, lecz także przygotowywać uczniów do świadomego, bezpiecznego i odpowiedzialnego korzystania z technologii. Obejmuje to w szczególności rozwijanie umiejętności samoregulacji czasu i sposobu korzystania z urządzeń, rozpoznawanie zagrożeń związanych z nternetem i mediami społecznościowymi, ochronę prywatności i danych osobowych, przeciwdziałanie cyberprzemocy oraz kształtowanie zasad bezpieczeństwa i odpowiedzialności w środowisku cyfrowym.

3. Ramy prawne i kierunki działań Unii Europejskiej

Instytucje europejskie uznają dezinformację oraz brak bezpieczeństwa cyfrowego za jeden z destabilizujących czynników społecznych.

a) Plan Działania w dziedzinie Edukacji Cyfrowej (Digital Education Action Plan 2021–2027): Plan wyznacza kierunki i wspiera państwa członkowskie w rozwijaniu umiejętności cyfrowych i uświadamianiu uczniów w zakresie higieny cyfrowej, ochrony zdrowia w sieci, etyki komunikacji oraz odporności na dezinformację. Uzupełnieniem tego planu jest Zalecenie Rady UE z 23 listopada 2023 r. w sprawie kluczowych czynników sprzyjających skutecznej edukacji cyfrowej, które wzywa państwa członkowskie do włączenia bezpiecznego korzystania z technologii i dobrostanu cyfrowego do obowiązkowych programów szkolnych od najwcześniejszych lat oraz do systemowego doskonalenia nauczycieli.

b) Europejskie Ramy Kompetencji Cyfrowych (DigComp 2.2): W obszarze 4 („Bezpieczeństwo") standard ten stanowi ramę odniesienia dla rozwijania kompetencji w zakresie ochrony urządzeń i treści, ochrony danych osobowych oraz dbania o dobrostan psychofizyczny, ze szczególnym uwzględnieniem podkompetencji 4.2 („Ochrona danych osobowych i prywatności") oraz 4.3 („Ochrona zdrowia i dobrostanu" – w tym unikanie zagrożeń dla zdrowia psychicznego i rozpoznawanie cyberprzemocy).

c) Europejska Strategia na rzecz Lepszego Internetu dla Dzieci (Better Internet for Kids, BIK+ 2022): Dokument ma na celu zapewnienie dzieciom ochrony, poszanowania i wzmocnienia ich pozycji w świecie cyfrowym. Opiera się na filarach bezpiecznego doświadczenia cyfrowego, wzmocnienia kompetencji cyfrowych (higiena cyfrowa w programach szkolnych) oraz aktywnego uczestnictwa młodzieży.

Parlament Europejski w rezolucji z 5 października 2023 r. w sprawie strategii BIK+ (2023/2670(RSP)) wezwał, by kompetencje cyfrowe, w tym umiejętności medialne, zostały uznane za obowiązkowy element programów szkolnych w całej UE, podkreślając, że powinny stanowić one nieodłączną część edukacji i uczenia się przez całe życie.

d) Regulacje rynkowe i ochrona małoletnich (DSA i EU Kids Act): Art. 28 DSA (Aktu o usługach cyfrowych) zobowiązuje platformy do zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w sieci. Ponadto, 17 września 2026 r. KE przedstawiła projekt rozporządzenia tzw. EU Kids Act, wprowadzającego m.in. rozwiązanie z zakresu weryfikacji wieku oraz ograniczenia dostępu do mediów społecznościowych dla dzieci poniżej 15. roku życia.

W systemach edukacyjnych wielu państw zagadnienia związane z higieną cyfrową, ochroną prywatności, bezpieczeństwem w sieci, cyberprzemocą, dobrostanem cyfrowym i odpowiedzialnym korzystaniem z technologii zostały włączone do krajowych ram kształcenia. Państwa stosują różne instrumenty prawne i programowe: od przepisów ustawowych, przez wiążące podstawy programowe i akty wykonawcze, po wytyczne ministerialne, strategie oraz programy wspierające.

Państwa, w których obowiązek wynika z przepisów ustawowych

Francja

Wiedza o higienie cyfrowej, bezpieczeństwie cyfrowym oraz bezpiecznym korzystaniu z sieci jest wpisana bezpośrednio do francuskiego Kodeksu edukacyjnego (Code de l'éducation). Artykuł L312-9 określa obowiązek kształcenia w zakresie korzystania z narzędzi i zasobów cyfrowych w placówkach oświatowych. Kształcenie to obejmuje między innymi podnoszenie świadomości na temat praw i obowiązków związanych z korzystaniem z Internetu i sieci, w tym ochrony prywatności i poszanowania własności intelektualnej, a także zagrożeń związanych z korzystaniem z tych narzędzi, w szczególności cyberprzemocy. Edukacja medialna i informacyjna jest realizowana obowiązkowo, a kompetencje cyfrowe uczniów są wspierane przez krajowy system Pix, służący do diagnozy i certyfikacji. Model ten uzupełnia ustawa nr 2018-698 z dnia 3 sierpnia 2018 r. dotycząca uregulowania korzystania z telefonów komórkowych w szkołach (Loi n° 2018-698 du 3 août 2018 relative à l'encadrement de l'utilisation du téléphone portable dans les établissements d'enseignement scolaire).

Włochy

Włoski ustawodawca wprowadził obowiązek kształcenia umiejętności cyfrowych na mocy ustawy z dnia 20 sierpnia 2019 r. nr 92 o wprowadzeniu nauczania edukacji obywatelskiej (Legge 20 agosto 2019, n. 92), tworząc wyodrębniony moduł „Edukacji Obywatelstwa Cyfrowego" (Educazione alla cittadinanza digitale). Zgodnie z regulacją, edukacja w zakresie obywatelstwa cyfrowego obejmuje między innymi znajomość zasad zachowania podczas korzystania z technologii cyfrowych i interakcji w środowiskach cyfrowych, świadomość tego, jak technologie cyfrowe mogą wpływać na dobrostan psychofizyczny i społeczny oraz znajomość polityk prywatności i ochrony danych osobowych. Rozwiązanie to stanowi bezpośredni, ustawowy odpowiednik konstrukcji projektowanej w Polsce. Dodatkowo ustawa nr 71/2017 nakłada na każdą szkołę obowiązek wyznaczenia nauczyciela koordynującego działania na rzecz zapobiegania i przeciwdziałania bullyingowi i cyberprzemocy. Z kolei akty ministerialne Ministerstwa Edukacji (MIN) z lat 2024–2025 stopniowo rozszerzyły zakaz korzystania przez uczniów z telefonów komórkowych - początkowo w pierwszym cyklu kształcenia, od roku szkolnego 2024/2025, a następnie także w drugim cyklu kształcenia, od roku szkolnego 2025/2026. W przypadku uczniów drugiego cyklu zakaz obejmuje korzystanie z telefonu podczas zajęć dydaktycznych oraz, co do zasady, w godzinach szkolnych.

Rumunia

W 2023 r. uchwalono nową Ustawę o Edukacji Przeduniwersyteckiej (Legea învățământului preuniversitar nr. 198/2023), która wpisała umiejętności cyfrowe (literația digitală) jako obowiązkową kompetencję kluczową na wszystkich etapach kształcenia. W szczególności ustawa nakłada na szkoły prawny obowiązek prowadzenia edukacji cyfrowej oraz obejmuje bezpośrednie

wymogi z zakresu higieny cyfrowej, w tym ochrony zdrowia psychicznego uczniów, profilaktyki uzależnień od technologii oraz przeciwdziałania cyberprzemocy.

Brazylia

W 2023 r. dokonano nowelizacji Głównej Ustawy Oświatowej (Lei de Diretrizes e Bases da Educação Nacional - LDB) poprzez uchwalenie ustawy o Narodowej Polityce Edukacji Cyfrowej (Lei nº 14.533, de 11 de janeiro de 2023). W ramach tej regulacji do art. 26 ustawy LDB dodano § 11, który ustanawia ustawowy obowiązek prowadzenia edukacji cyfrowej na wszystkich etapach szkolnictwa podstawowego i średniego (ensino fundamental e médio). Przepis ten nakłada na szkoły obowiązek realizowania programu obejmującego bezpieczne, krytyczne, etyczne i odpowiedzialne korzystanie z technologii informacyjno-komunikacyjnych, ze szczególnym uwzględnieniem ochrony prywatności, higieny cyfrowej oraz przeciwdziałania zagrożeniom psychospołecznym w sieci.

Stany Zjednoczone (USA)

Floryda (USA)

Amerykański stan Floryda wprowadził ustawowy obowiązek kształcenia w zakresie higieny cyfrowej na mocy ustawy House Bill 379 z 2023 r. (Chapter 2023-36, Laws of Florida), nowelizującej § 1003.42(2) Kodeksu Statutów Florydy (Florida Statutes). Zgodnie z wytycznymi wykonawczymi Departamentu Edukacji Florydy, uczniowie klas 6-12 uczestniczą w zajęciach edukacyjnych poświęconych negatywnym skutkom nadmiernego korzystania z technologii cyfrowych dla zdrowia psychicznego, w tym uczą się rozpoznawać mechanizmy prowadzące do uzależnienia. Zajęcia obejmują także zasady bezpieczeństwa osobistego w środowisku cyfrowym.

Karolina Północna (USA)

Stan Karolina Północna uchwalił ustawę House Bill 959 z 2025 r. pod tytułem „Protecting Students in a Digital Age", wprowadzającą nowy § 115C-81.26 do Ogólnych Statutów Karoliny Północnej (General Statutes, Chapter 115C). Od roku szkolnego 2026–2027 każdy uczeń musi zostać objęty tym tematem co najmniej jeden raz w toku szkoły podstawowej, jeden raz w toku gimnazjum oraz dwa razy w toku szkoły średniej, przy czym ustawa nie precyzuje, w którym konkretnie roku nauki ani w ramach jakiego przedmiotu ma to nastąpić - decyzję tę podejmuje lokalny okręg szkolny. Program uczy rozpoznawania negatywnego wpływu mediów społecznościowych i technologii cyfrowych na zdrowie psychiczne, w tym mechanizmów prowadzących do uzależnienia, a także sposobów, w jakie platformy manipulują zachowaniem użytkownika.

<u>Państwa, w których obowiązek wynika z podstaw programowych lub wiążących wytycznych</u>

Nie wszystkie państwa wprowadzają obowiązek edukacji cyfrowej bezpośrednio do ustawy. W części systemów odpowiednie treści są zagwarantowane przez krajowe podstawy programowe, wiążące wytyczne ministerialne albo obowiązkowe, przekrojowe moduły programowe. Rozwiązania te nie są równoważne regulacji ustawowej, ale stanowią istotny punkt odniesienia dla oceny różnych modeli wdrażania polityki publicznej.

Wielka Brytania - Anglia

Departament Edukacji (Department for Education – DfE) określił wymagania dotyczące edukacji cyfrowej za pośrednictwem podstaw programowych oraz ustawowych wytycznych dotyczących Relationships Education, Relationships and Sex Education (RSE) and Health Education, określanych skrótem RSHE. Kluczowe umiejętności dotyczące higieny cyfrowej znajdują się w National Curriculum in England: Computing oraz w ramach ustawowych wytycznych dla obowiązkowego przedmiotu Relationships, Sex and Health Education (RSHE) w dziale „Internet safety and harms" (obejmującym m.in. wpływ czasu ekranowego na zdrowie psychiczne, cyberprzemoc, ochronę prywatności oraz mechanizmy uzależniające). Od września 2026 r. obowiązują zaktualizowane wytyczne RSHE rozszerzone o zagrożenia związane ze sztuczną inteligencją, deepfake'ami i dezinformacją.

Irlandia

Rada ds. Programu Nauczania i Oceniania (National Council for Curriculum and Assessment – NCCA) oraz Departament Edukacji nakładają na szkoły obowiązek wdrażania modułów z zakresu bezpieczeństwa cyfrowego w ramowym programie obowiązkowego przedmiotu SPHE (Social, Personal and Health Education) oraz krajowej strategii Digital Strategy for Schools 2027. Edukacja w zakresie higieny cyfrowej, ochrony danych osobowych oraz dobrostanu psychofizycznego w sieci stanowi stały i weryfikowalny element kształcenia na wszystkich etapach edukacyjnych. Digital Strategy for Schools to 2027 stanowi dokument polityki publicznej wspierający rozwój kompetencji i bezpieczne korzystanie z technologii w szkołach, nie jest natomiast ustawą ustanawiającą samodzielny obowiązek edukacyjny.

Szwajcaria

Szwajcarski model edukacyjny jest zdecentralizowany i opiera się na porozumieniach międzykantonalnych. Wiążący krajowy plan nauczania Lehrplan 21 zawiera wyodrębniony i obowiązkowy moduł Medien und Informatik (MI). Program ten obliguje szkoły do prowadzenia zajęć z zakresu bezpiecznego korzystania z mediów, ochrony prywatności, rozpoznawania zagrożeń w sieci oraz analizy wpływu technologii na zdrowie i relacje społeczne uczniów.

Australia

System oświatowy w Australii nakłada obowiązek kształcenia z zakresu higieny cyfrowej poprzez ogólnokrajową podstawę programową (Australian Curriculum Version 9.0), opracowywaną na podstawie federalnych i stanowych regulacji prawnych. W ramowym dokumencie Digital Literacy General Capability zapisano takie umiejętności jak zarządzanie bezpieczeństwem w sieci, prywatnością i tożsamością cyfrową oraz cyfrowym dobrostanem, rozpoznanie zagrożenia związanego z treściami, ochrona danych osobowych, stosowanie praktyki cyberbezpieczeństwa i rozumienie wpływu technologii na zdrowie i bezpieczeństwo. Australia realizuje pełny model łączony: obok krajowej ramy programowej działa rządowy organ eSafety Commissioner, dostarczający szkołom akredytowane programy edukacyjne, a na mocy ustawy Online Safety Amendment (Social Media Minimum Age) Act 2024 wprowadzono ustawowy zakaz posiadania kont w mediach społecznościowych dla osób poniżej 16. roku życia.

Singapur

Ministerstwo Edukacji Singapuru (Ministry of Education - MOE) realizuje obowiązek kształcenia w zakresie higieny cyfrowej w strukturze programu Character and Citizenship Education (CCE), wprowadzając dedykowany moduł Cyber Wellness (CW). Program Cyber Wellness w ramach CCE skupia się na dobrostanie uczniów poruszających się w cyberprzestrzeni. Wyposaża ich w wiedzę i umiejętności pozwalające utrzymać pozytywną obecność w sieci, chronić prywatność, rozpoznawać zagrożenia i stosować dobrą higienę cyfrową oraz kształtować samoregulację czasu spędzanego przed ekranami (screen time balance).

Korea Południowa

Korea Południowa realizuje zasady higieny cyfrowej na podstawie Znowelizowanej Podstawy Programowej z 2022 r. (2022 Revised National Curriculum), w szczególności programu nauczania przedmiotu Informatyka. Rozwiązania programowe są uzupełniane regulacjami dotyczącymi ochrony młodzieży oraz programami profilaktyki uzależnień od Internetu i gier wideo. W ramach tych działań prowadzone są między innymi programy diagnostyczne, profilaktyczne i edukacyjne dotyczące nadmiernego korzystania z technologii cyfrowych. Od marca 2026 r. obowiązują również przepisy wynikające z nowelizacji Elementary and Secondary Education Act, ograniczające używanie smartfonów i innych urządzeń elektronicznych podczas zajęć lekcyjnych w szkołach podstawowych i średnich.

Przegląd rozwiązań przyjętych w analizowanych państwach wskazuje, że przeciwdziałanie zagrożeniom cyfrowym oraz ochrona dobrostanu psychofizycznego uczniów zajmują istotne miejsce w politykach edukacyjnych na świecie. Edukacja dotycząca bezpieczeństwa online, prywatności, dobrostanu cyfrowego i odpowiedzialnego korzystania z technologii jest coraz częściej traktowana jako stały element kształcenia, a nie jako inicjatywa fakultatywna. Zagadnienia związane z bezpiecznym korzystaniem z technologii, ochroną danych osobowych, higieną cyfrową oraz

przeciwdziałaniem uzależnieniom są włączane do obowiązujących programów nauczania i krajowych ram kształcenia - w ramach edukacji obywatelskiej, zdrowotnej, informatycznej lub ogólnych ram kompetencji cyfrowych. Zakres tych działań pozostaje zgodny z kierunkami wyznaczanymi przez unijne ramy kompetencji cyfrowych, w szczególności DigComp 2.2, oraz przez Digital Education Action Plan 2021–2027, który wspiera rozwój wysokiej jakości, włączającej i dostępnej edukacji cyfrowej w państwach członkowskich. Doświadczenia międzynarodowe pokazują, że skuteczność tych rozwiązań zależy od zachowania spójności między regulacjami prawno-programowymi, zapewnieniem systemowego wsparcia i doskonalenia zawodowego nauczycieli a budowaniem umiejętności samoregulacji u samych uczniów.

Działania podejmowane w wybranych państwach

Austria

W marcu 2026 r. rząd federalny zapowiedział ustanowienie minimalnego wieku 14 lat dla korzystania z wybranych platform społecznościowych, wskazując na zagrożenia związane z uzależniającymi mechanizmami projektowania usług cyfrowych, cyberprzemocą, dezinformacją oraz negatywnym wpływem mediów społecznościowych na zdrowie psychiczne dzieci i młodzieży.

W lipcu 2026 r. austriacki rząd skierował do konsultacji publicznych projekt przepisów przewidujący ograniczenie dostępu do platform wykorzystujących mechanizmy sprzyjające nadmiernemu korzystaniu z usług cyfrowych, takie jak algorytmy rekomendacyjne oparte głównie na treściach pochodzących od nieznajomych użytkowników, nieskończone przewijanie treści (infinite scroll), automatyczne odtwarzanie materiałów, systemy nagród za aktywność czy powiadomienia zachęcające do ponownego korzystania z platformy. Wśród usług objętych projektowanymi regulacjami wskazywane są m.in. TikTok, Instagram, YouTube i Snapchat.

Projekt zakłada obowiązek stosowania mechanizmów weryfikacji wieku przy zachowaniu zasad ochrony prywatności. Rozważane rozwiązania opierają się na modelu, w którym platforma otrzymuje jedynie informację o spełnieniu wymogu wiekowego przez użytkownika, bez dostępu do jego pełnych danych identyfikacyjnych. Jedną z możliwych metod weryfikacji ma być wykorzystanie krajowego systemu identyfikacji elektronicznej ID Austria.

Jednocześnie Austria deklaruje poparcie dla wypracowania wspólnych rozwiązań na poziomie Unii Europejskiej, wskazując jednak, że ze względu na czas potrzebny na przyjęcie regulacji unijnych konieczne jest równoległe prowadzenie prac legislacyjnych na poziomie krajowym.

Holandia

Holandia nie przyjęła dotychczas wiążących regulacji krajowych ustanawiających minimalny wiek korzystania z mediów społecznościowych. Jednocześnie kwestia ta została uwzględniona w umowie koalicyjnej rządu, która zakłada dążenie do ustanowienia na poziomie europejskim minimalnego wieku 15 lat dla samodzielnego korzystania z mediów społecznościowych, przy jednoczesnym zapewnieniu rozwiązań służących weryfikacji wieku z poszanowaniem prywatności użytkowników. W tym celu zlecono analizę mającą określić możliwości prawne wdrożenia takich rozwiązań w świetle obowiązującego prawa unijnego i krajowego.

Holandia analizuje możliwe modele weryfikacji wieku użytkowników mediów społecznościowych. W prowadzonych pracach szczególny nacisk kładzie się na skuteczność proponowanych rozwiązań oraz ich zgodność z zasadami ochrony prywatności, proporcjonalności, przejrzystości i dostępności.

Portugalia

W lutym 2026 r. portugalski parlament przyjął w pierwszym czytaniu projekt przepisów ograniczających dostęp dzieci i młodzieży do mediów społecznościowych. Projekt został przedstawiony przez rządzącą partię Social Democratic Party (PSD) i uzyskał szerokie poparcie parlamentarne. Przepisy są nadal przedmiotem dalszych prac legislacyjnych dotyczących szczegółów wdrożenia.

Przyjęty kierunek zakłada ustanowienie minimalnego wieku 16 lat dla samodzielnego korzystania z mediów społecznościowych, obowiązkową weryfikację wieku, zweryfikowaną zgodę rodzicielską

dla użytkowników w wieku 13-16 lat oraz dodatkowe obowiązki platform w zakresie ochrony małoletnich przed szkodliwymi treściami i uzależniającymi mechanizmami działania usług cyfrowych.

Słowenia

W Słowenii nie obowiązują obecnie szczególne regulacje określające minimalny wiek korzystania z mediów społecznościowych. Kwestie związane z wiekiem użytkowników regulowane są pośrednio przez przepisy dotyczące ochrony danych osobowych. Zgodnie z Zakon o varstvu osebnih podatkov (ZVOP-2) dziecko może samodzielnie wyrazić zgodę na przetwarzanie danych osobowych w związku z korzystaniem z usług społeczeństwa informacyjnego po ukończeniu 15. roku życia. W przypadku młodszych użytkowników wymagana jest zgoda rodzica lub opiekuna.

Istotnym elementem słoweńskiego podejścia są również działania edukacyjne realizowane przez szkoły oraz krajowy punkt ds. bezpieczeństwa w internecie Safe.si, obejmujące edukację medialną, bezpieczeństwo cyfrowe oraz wsparcie dla rodziców i nauczycieli.

W lutym 2026 r. rząd Słowenii rozpoczął prace nad regulacjami mającymi ograniczyć dostęp do mediów społecznościowych dla dzieci poniżej 15. roku życia. Planowane przepisy miałyby objąć przede wszystkim platformy oparte na treściach generowanych przez użytkowników, takie jak TikTok, Instagram czy Snapchat. Celem projektowanych rozwiązań jest ograniczenie ryzyk związanych z uzależniającymi mechanizmami wykorzystywanymi przez platformy cyfrowe, ochrona zdrowia psychicznego małoletnich oraz zwiększenie bezpieczeństwa dzieci w środowisku online.

Słowenia znajduje się obecnie na etapie przechodzenia od modelu opartego głównie na ochronie danych osobowych i edukacji cyfrowej do bardziej restrykcyjnego podejścia, przewidującego ustawowe ograniczenie dostępu do mediów społecznościowych dla osób poniżej 15. roku życia.

Doświadczenia innych państw wskazują na potrzebę trwałego i powszechnego uregulowania edukacji dotyczącej funkcjonowania w środowisku cyfrowym. W polskich warunkach regulacja ustawowa zapewniłaby jednolite stosowanie obowiązku we wszystkich szkołach i jednoznacznie potwierdziłaby, że edukacja w zakresie higieny cyfrowej, zagrożeń online, ochrony prywatności i bezpieczeństwa cyfrowego jest obowiązkowym elementem kształcenia, a nie jedynie zalecanym kierunkiem działań.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Prezes UKE	1	Dane własne	Prezes UKE jest organem regulacyjnym rynku usług komunikacji elektronicznej. Rozszerza się kompetencje Prezesa UKE.
Dostawcy internetowych serwisów społecznościowych	Wielkość trudna do oszacowania	Dokładne oszacowanie jest bardzo utrudnione ze względu na niską dostępność danych finansowych i brak obowiązków raportowych dla międzynarodowych firm w Polsce.	Obowiązek wdrożenia mechanizmu weryfikacji wieku.
Osoby poniżej 15 roku życia	5,3 mln (stan na dzień 31 grudnia 2025 r.)	Dane Głównego Urzędu Statystycznego	Ograniczenie dostępu do internetowych serwisów społecznościowych.
Osoby od 15 roku życia	32 mln (stan na dzień 31 grudnia 2025 r.)	Dane Głównego Urzędu Statystycznego	Objęcie obowiązkowym mechanizmem weryfikacji wieku.

Minister właściwy do spraw oświaty i wychowania	1	Informacja powszechnie dostępna	Możliwość realizacji kampanii informacyjnych i promocyjnych.
Minister właściwy do spraw informatyzacji	1	Informacja powszechnie dostępna	Nałożenie nowych obowiązków w postaci konieczności dostosowania aplikacji mObywatel i udostępnienia w niej nowej usługi oraz prowadzenia listy zaufanych rozwiązań w zakresie weryfikacji wieku.
Sądy administracyjne	17 (16 sądów wojewódzkich oraz Naczelny Sąd Administracyjny)	Informacja powszechnie dostępna	Rozpatrywanie odwołań od decyzji Prezesa UKE.
Użytkownicy aplikacji mObywatel	Ponad 13 mln	Dane własne	Uzyskanie dostępu do nowej usługi umożliwiającej selektywną weryfikację wieku w usługach online.
Użytkownicy europejskiego portfela tożsamości cyfrowej zapewnianego bezpośrednio przez Polskę	Niemożliwe do oszacowania	Brak	Możliwość selektywnej weryfikacji wieku w usługach online.
Przedsiębiorcy posiadający zasoby do świadczenia usług w zakresie weryfikacji wieku	Niemożliwe do oszacowania	Brak	Możliwość oferowania nowego rodzaju usług.
Szkoły publiczne i niepubliczne, przedszkola	ok. 37,5 tys.	System informacji oświatowej – stan na 30 września 2026 r.	Dostosowanie programów nauczania przedszkolnego i szkolnego do zapisów podstawy programowej wychowania przedszkolnego i podstawy programowej kształcenia ogólnego dla poszczególnych typów szkół wzmacniającej treści dotyczące higieny cyfrowej, zagrożeń wynikających z korzystania z internetu, zasad ochrony prywatności i bezpieczeństwa w cyfrowym świecie.
Uczniowie szkół publicznych i niepublicznych oraz przedszkoli (w tym dzieci uczęszczające do oddziałów	Ok. 6,6 mln (w tym ok 4,95 mln uczniów i dzieci poniżej 15 roku życia)	System informacji oświatowej – stan na 30 września 2026 r.	Nabywanie wiedzy z zakresu higieny cyfrowej, zagrożeń wynikających z korzystania z Internetu, zasad ochrony prywatności i

przedszkolnych zorganizowanych w szkołach podstawowych)			bezpieczeństwa przestrzeni cyfrowej.
Nauczyciele szkół publicznych i niepublicznych oraz przedszkoli	ok. 0,7 mln	System informacji oświatowej – stan na 30 września 2026 r.	Realizacja zapisów podstawy programowej wychowania przedszkolnego i podstawy programowej kształcenia ogólnego dla poszczególnych typów szkół, uwzględniających informacje dotyczące higieny cyfrowej, zagrożeń wynikających z korzystania z internetu, zasad ochrony prywatności i bezpieczeństwa w cyfrowym świecie.
Jednostki podległe i nadzorowane przez ministra właściwego do spraw oświaty i wychowania	7	Informacja powszechnie dostępna	Możliwość realizacji kampanii informacyjnych i promocyjnych, zleconych przez ministra właściwego do spraw oświaty i wychowania.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2026 r. poz. 936) projekt ustawy został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.

Projekt ustawy zostanie poddany 30-dniowym konsultacjom publicznym z następującymi podmiotami:

1) Polską Izbą Informatyki i Telekomunikacji;
2) Krajową Izbą Gospodarczej Elektroniki i Telekomunikacji;
3) Polską Izbą Komunikacji Elektronicznej;
4) Krajową Izbą Gospodarczą;
5) Krajową Izbą Komunikacji Ethernetowej;
6) Polską Izbą Radiodyfuzji Cyfrowej;
7) Polską Izbą Handlu;
8) Izbą Gospodarki Elektronicznej;
9) Krajową Izbą Gospodarki Cyfrowej;
10) Polskim Towarzystwem Informatycznym;
11) Stowarzyszeniem Inżynierów Telekomunikacji;
12) Fundacją Panoptykon;
13) Związkiem Pracodawców Mediów Publicznych;
14) Związkiem Pracodawców Mediów Elektronicznych Mediakom;
15) Związkiem Pracodawców Branży Internetowej IAB Polska;
16) Związkiem Telewizji Kablowych w Polsce Izba Gospodarcza;
17) Związkiem Cyfrowa Polska;
18) Sektorową Radą ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
19) Polską Radą Biznesu;
20) Naczelną Organizacją Techniczną;
21) Stowarzyszeniem Twoja Sprawa;

22) Towarzystwem Przyjaciół Dzieci;
23) Centrum Edukacji Obywatelskiej;
24) Krajową Izbą Gospodarczą Rozwiązań Podwójnego Zastosowania i Obronności „Polska Izba Dual Use”;
25) Polskim Towarzystwem Terapii Poznawczej i Behawioralnej;
26) Polską Akademią Nauk;
27) Instytutem Spraw Publicznych;
28) Krajowym Forum Oświaty Niepublicznej;
29) Federacją Inicjatyw Oświatowych;
30) Ogólnopolskim Stowarzyszeniem Kadry Kierowniczej Oświaty;
31) Polskim Stowarzyszeniem na Rzecz Osób z Niepełnosprawnością Intelektualną;
32) Ogólnopolskim Stowarzyszeniem Dyrektorów Centrów Kształcenia Ustawicznego;
33) Stowarzyszeniem Dyrektorów Szkół Średnich;
34) Stowarzyszeniem Cyfrowy Dialog;
35) Społecznym Towarzystwem Oświatowym;
36) Radą Szkół Katolickich;
37) Sekretariatem Konferencji Episkopatu Polski;
38) Aliansem Ewangelicznym w RP;
39) Polską Radą Ekumeniczną;
40) Fundacją Dajemy Dzieciom Siłę;
41) Fundacją Digital University;
42) Fundacją EdTech Poland;
43) Fundacją Fabian Digital;
44) Fundacją Polskiego Funduszu Rozwoju;
45) Fundacją Rodzice Szkole;
46) Fundacją Rozwoju Demokracji Lokalnej;
47) Fundacją Rozwoju Systemu Edukacji;
48) Fundacją Szkoła z Klasą;
49) Fundacją Save the Children International Poland;
50) Fundacją Centrum Cyfrowe.

Projekt ustawy zostanie poddany 30-dniowemu opiniowaniu z następującymi podmiotami:
1) Krajową Radą Radiofonii i Telewizji;
2) Prezesem Urzędu Ochrony Konkurencji i Konsumentów;
3) Prezesem Urzędu Komunikacji Elektronicznej;
4) Prezesem Urzędu Ochrony Danych Osobowych;
5) Rzecznikiem Małych i Średnich Przedsiębiorców;
6) Komisją Nadzoru Finansowego;
7) Rzecznikiem Praw Dziecka;
8) Rzecznikiem Praw Obywatelskich;
9) Prezesem Głównego Urzędu Statystycznego;
10) Naukową i Akademicką Siecią Komputerową - Państwowym Instytutem Badawczym;
11) Przewodniczącym Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15;
12) Unią Metropolii Polskich;
13) Unią Miasteczek Polskich;
14) Związkiem Gmin Wiejskich RP;
15) Związkiem Miast Polskich;
16) Związkiem Powiatów Polskich.

Projekt ustawy zostanie przekazany do zaopiniowania, z terminem przedstawienia opinii w ciągu 30 dni, zgodnie art. 16 ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców (Dz. U. z 2025 r. poz. 423) oraz art. 19 ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2026 r. poz. 549 i 1340) do następujących podmiotów:
1) Związku Pracodawców – Business Centre Club;

2) Pracodawców Rzeczypospolitej Polskiej;
3) Konfederacji „Lewiatan”;
4) Związku Przedsiębiorców i Pracodawców;
5) Związku Rzemiosła Polskiego;
6) Polskiego Towarzystwa Gospodarczego;
7) Federacji Przedsiębiorców Polskich;
8) Niezależnego Samorządnego Związku Zawodowego „Solidarność”;
9) Ogólnopolskiego Porozumienia Związków Zawodowych;
10) Forum Związków Zawodowych;
11) Związku Przedsiębiorców i Pracodawców;
12) Komisji Krajowej NSZZ „Solidarność 80”;
13) Niezależnego Samorządnego Związku Zawodowego Pracowników Schronisk dla Nieletnich i Zakładów Poprawczych;
14) Sekcji Krajowej Oświaty i Wychowania NSZZ „Solidarność”;
15) Sekcji Oświaty KNSZZ „Solidarność 80”;
16) Wolnego Związku Zawodowego „Sierpień 80” Komisji Krajowej;
17) Wolnego Związku Zawodowego „Solidarność-Oświata”;
18) Zarządu Głównego Związku Nauczycielstwa Polskiego;
19) Zarządu Głównego Związku Zakładów Doskonalenia Zawodowego;
20) Związku Zawodowego Pracowników Oświaty i Wychowania „Oświata”;
21) Związku Zawodowego „Rada Poradnictwa”.

Projekt ustawy zostanie także przekazany do zaopiniowania do Rady Dialogu Społecznego, Rady Działalności Pożytku Publicznego i Rady Dialogu z Młodym Pokoleniem.

Projekt ustawy zostanie również przekazany do zaopiniowania przez Komisję Wspólną Rządu i Samorządu Terytorialnego i Komisję Wspólną Rządu i Mniejszości Narodowych i Etnicznych.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2026 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0,28	0,63	0,67	0,69	0,71	0,73	0,75	0,76	0,78	0,81	0,83	7,63
budżet państwa	0,00	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,19
JST	0,03	0,09	0,09	0,10	0,10	0,10	0,11	0,11	0,11	0,12	0,12	1,08
NFZ	0,05	0,10	0,11	0,11	0,11	0,11	0,12	0,12	0,12	0,13	0,13	1,21
ZUS	0,19	0,40	0,42	0,43	0,44	0,45	0,46	0,48	0,49	0,50	0,51	4,77
Fundusz Solidarnościowy	0,01	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,23
Fundusz Pracy	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,02	0,02	0,02	0,16
Wydatki ogółem	**2,56**	**1,87**	**1,88**	**1,91**	**2,11**	**2,98**	**2,14**	**2,18**	**2,22**	**2,38**	**3,48**	**25,71**
budżet państwa	2,56	1,87	1,88	1,91	2,11	2,98	2,14	2,18	2,22	2,38	3,48	25,71
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**-2,29**	**-1,24**	**-1,21**	**-1,22**	**-1,40**	**-2,26**	**-1,40**	**-1,41**	**-1,43**	**-1,57**	**-2,65**	**-18,08**
budżet państwa	-2,56	-1,86	-1,86	-1,90	-2,09	-2,96	-2,12	-2,16	-2,20	-2,35	-3,46	-25,52
JST	0,03	0,09	0,09	0,10	0,10	0,10	0,11	0,11	0,11	0,12	0,12	1,08
NFZ	0,05	0,10	0,11	0,11	0,11	0,11	0,12	0,12	0,12	0,13	0,13	1,21

ZUS	0,19	0,40	0,42	0,43	0,44	0,45	0,46	0,48	0,49	0,50	0,51	4,77
Fundusz Solidarnościowy	0,01	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,23
Fundusz Pracy	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,02	0,02	0,02	0,16

Źródła finansowania	Wszelkie koszty po stronie Prezesa UKE będą finansowane z części budżetowej 76 - Urząd Komunikacji Elektronicznej. Zadania nałożone na Prezesa UKE na podstawie projektowanej regulacji spowodują konieczność zwiększenia realizowanego w ramach planowanego corocznie w ustawie budżetowej limitu wydatków w cz. 76 – Urząd Komunikacji Elektronicznej. Wydatki budżetu państwa wynikające z wejścia w życie ustawy przewidziane na lata 2027–2037 wynikające z zadań Prezesa UKE wyniosą 20 129 618,47 zł. Są to wydatki Prezesa UKE wynikające z wejścia w życie ustawy. Wydatki te są związane z koniecznością utworzenia dodatkowych 6 etatów specjalistycznych, w tym jednego stanowiska kierowniczego oraz z potrzebą utworzenia i utrzymania rejestru. Podyktowane to jest skalą i zakresem nowych zadań związanych z prowadzeniem rejestru oraz zadań o charakterze kontrolno-nadzorczych nakładanych na Prezesa UKE. Analiza pracochłonności w zakresie nowych zadań dla Urzędu Komunikacji Elektronicznej, zwanego dalej „UKE”: Założenia Liczba dni roboczych w roku – 252 Liczba godzin poświęcanych przez 1 pracownika swoim zadaniom w dniu roboczym – 7 Liczba dni urlopowych 1 pracownika w roku – 26 Liczba dni chorobowych 1 pracownika w roku – 10 Liczba dni szkoleniowych 1 pracownika w roku – 7 Liczba roboczogodzin oferowanych w roku przez 1 pracownika – 1463 Roczna pracochłonność zadań obszaru (wg wykazu najważniejszych zadań) – 9190 godz. Wyliczona liczba personelu – 6,28 Minimalna liczba etatów personelu – 6 Wydatki związane z dostosowaniem aplikacji mObywatel do nowych przepisów oraz prowadzeniem listy zaufanych rozwiązań w zakresie weryfikacji wieku będą dokonywane z budżetu państwa w części 27 – Informatyzacja.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Koszty związane z dostosowaniem aplikacji mObywatel do nowych regulacji szacuje się na łączną kwotę 5 695 674,88 zł. Zapewnienie funkcjonowania przez ministra właściwego do spraw informatyzacji listy zaufanych rozwiązań w zakresie weryfikacji następować będzie w ramach strony podmiotowej tego ministra w BIP i następować będzie w oparciu o dotychczasowe zasoby kadrowe tego ministra. W związku z powyższym rozwiązanie to nie wygeneruje dodatkowych kosztów.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki

Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
	(dodaj/usuń)							

W ujęciu niepieniężnym	duże przedsiębiorstwa		Wdrożenie mechanizmu weryfikacji wieku ma na celu ustalenie wieku użytkownika i uniemożliwienie usługobiorcom, którzy nie ukończyli 15. roku życia uzyskania dostępu do internetowych serwisów społecznościowych. Możliwość oferowania rozwiązań komercyjnych dot. zaufanych rozwiązań w zakresie weryfikacji wieku.
	sektor mikro-, małych i średnich przedsiębiorstw		Wdrożenie mechanizmu weryfikacji wieku ma na celu ustalenie wieku użytkownika i uniemożliwienie usługobiorcom, którzy nie ukończyli 15. roku życia uzyskanie dostępu do internetowych serwisów społecznościowych. Możliwość oferowania rozwiązań komercyjnych dot. zaufanych rozwiązań w zakresie weryfikacji wieku.
	rodzina, obywatele oraz gospodarstwa domowe		Rodzice zostaną odciążeni od indywidualnej kontroli swoich dzieci. Dzieci nie będą mogły używać argumentu „wszyscy mają”. Wprowadzona regulacja może mieć pozytywny wpływ na rodziny, obywateli i gospodarstwa domowe. Bezpieczne i odpowiedzialne korzystanie z nowych technologii, zwiększenie świadomości zagrożeń występujących w przestrzeni cyfrowej oraz umiejętność prawidłowego zachowania w sytuacji zagrożenia mogą zadziałać jak tarcza prewencyjna na rodziny uczniów objętych regulacją. Może nastąpić ograniczenie strat finansowych z tytułu cyberprzestępczości, w sytuacji wczesnego dostrzeżenia próby oszustwa. Wczesna profilaktyka polegająca na wpojeniu prawidłowych nawyków korzystania z nowych technologii może zredukować liczbę dzieci wymagających terapii psychologicznych, psychiatrycznych oraz leczenia uzależnień behawioralnych.
Niemierzalne	(dodaj/usuń)		
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń			**Wpływ na przedsiębiorców** Dokonując oceny wpływu projektowanych zmian należy zwrócić uwagę, że precyzyjne oszacowanie skutków przedmiotowych regulacji jest niemożliwe.

	Ustawa nakłada nowe obowiązki na dostawców internetowych serwisów społecznościowych. Nie jest możliwe wskazanie kosztów wdrożenia mechanizmu weryfikacji wieku, gdyż zależy to od wielkości usługi (zarówno pod kątem technicznej organizacji usługi, jak i liczby użytkowników z niej korzystających) i jej charakteru (w tym w zakresie wykorzystywanych przez usługodawcę środków technicznych i organizacyjnych). Projekt umożliwi także oferowanie przez przedsiębiorców nowych usług z zakresu weryfikacji wieku.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Komentarz:

Istotne regulacje obejmą dostawców internetowych serwisów społecznościowych. Będą oni zobowiązani do wdrożenia mechanizmu weryfikacji wieku, co ma na celu pozbawienie osób, które nie ukończyły 15. roku życia dostępu do dostarczanych przez nich usług.

Należy wskazać, że kwestia dostępu dzieci, które nie ukończyły 15 roku życia do internetowych serwisów społecznościowych i związanych z tym zagrożeń wymaga pilnej regulacji, co wynika z licznych, przywołanych wyżej badań. W przypadku zatem tej materii uzasadnione jest wprowadzenie dodatkowych obciążeń regulacyjnych, bez których nie byłoby możliwe zwiększenie bezpieczeństwa małoletnich. Obowiązki nie będą różnicowane ze względu na wielkość usługodawców; będą jednakowe i powszechne dla każdego, kto jest dostawcą internetowego serwisu społecznościowego. Nie jest zasadne różnicowanie obowiązków pod względem wielkości przedsiębiorców, gdyż nawet w przypadku, gdy dany podmiot spełnia kryteria posiadania statusu mikro lub małego przedsiębiorcy, skutki jego działania mogą mieć znacznie większe rozmiary, ze względu na specyfikę dostarczanej przez niego usługi i liczbę usługobiorców. Różnicowanie obowiązków pod względem zakresu podmiotowego lub wprowadzenie wyłączeń podmiotowych spowodowałoby nierówny poziom ochrony małoletnich. Jednakże w przypadku każdego podmiotu ocena działań podejmowanych przez podmiot ze strony organu nadzorczego zależna będzie od uwarunkowań organizacyjnych podmiotu i cech oferowanej usługi.

Jednocześnie mając na uwadze zasady określone w art. 67 ustawy z dnia 6 marca 2018 r – Prawo przedsiębiorców, proponuje się zmniejszyć obciążenia administracyjne poprzez funkcjonowanie nowej usługi w aplikacji mObywatel w zakresie weryfikacji wieku. Usługa ta będzie umożliwiać użytkownikowi aplikacji mObywatel, pod jego wyłączną kontrolą, selektywne przekazywanie

informacji dotyczącej: daty urodzenia, posiadania określonego wieku, osiągnięcia określonego progu wiekowego lub osiągnięcia wieku w określonym przedziale wiekowym. Dzięki uregulowaniu funkcjonowania tej usługi na poziomie ustawowym możliwe stanie się jej uznawanie w tych przypadkach, gdzie dotychczas weryfikacja wieku mogła następować tylko na podstawie dokumentu tożsamości.

Konsekwencją wejścia w życie projektu będzie konieczność dostosowania usług oferowanych przez dostawców internetowych serwisów społecznościowych. Projekt będzie mieć wpływ także na osoby korzystające z tego typu usług, które będą musiały potwierdzić spełnienie wymogu w zakresie wieku.

9. Wpływ na rynek pracy

Nie przewiduje się wpływu na rynek pracy projektowanych przepisów. W przypadku największych portali i stron internetowych może pojawić się potrzeba zatrudnienia specjalistów do nadzorowania mechanizmu weryfikacji wieku.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☒ zdrowie
Omówienie wpływu	Projekt ma na celu ochronę dzieci, które nie ukończyły poniżej 15 roku życia przed zagrożeniami płynącymi ze zbyt wczesnego rozpoczęcia korzystania z internetowych serwisów społecznościowych. Do zagrożeń tych należą między innymi spadek aktywności fizycznej, zwiększone ryzyko krótkowzroczności i zaburzeń snu, objawy depresyjne i lękowe, obniżone poczucie własnej wartości, negatywny wpływ na procesy uczenia się i rozwój poznawczy, zaburzenia odżywiania, osłabienie empatii, poczucie samotności oraz zachowania o charakterze uzależniającym. Nieletni narażeni są ponadto na cyberprzemoc, hejt, dezinformację i manipulację, a także na niegodziwe traktowanie w celach seksualnych i nagabywanie seksualne (grooming), co może prowadzić do poważnych konsekwencji emocjonalnych i społecznych. Szersza realizacja uwzględnionych w podstawie programowej wychowania przedszkolnego i podstawie programowej kształcenia ogólnego dla poszczególnych typów szkół treści z zakresu zasad higieny cyfrowej, w tym dotyczących wpływu nadużywania urządzeń ekranowych na zdrowie psychiczne i fizyczne, zasad cyberbezpieczeństwa, w tym ochrony prywatności i bezpieczeństwa w cyfrowym świecie, oraz zagrożeń wynikających z niewłaściwego używania technologii informacyjno-komunikacyjnych, w tym w szczególności odnoszących się do cyberprzemocy i mowy nienawiści, uzależnienia od Internetu i gier komputerowych, niebezpiecznych kontaktów w sieci umożliwi systemowi edukacji lepsze przygotowanie młodego człowieka do życia w społeczeństwie informacyjnym i rozpoznanie ryzyk związanych z korzystaniem z nowoczesnych technologii.	

11. Planowane wykonanie przepisów aktu prawnego

Ustawa wejdzie w życie z dniem 1 września 2027 r.
Na dzień docelowego terminu wejścia w życie ustawy (tj. 1 września 2027 r.) zapewnione zostanie funkcjonowanie zapewnianego przez Polskę europejskiego portfela tożsamości cyfrowej (co wynika z brzmienia przepisów projektu UC122). Na ten sam dzień planuje się także udostępnienie przewidzianej w projekcie usługi w aplikacji mObywatel, umożliwiającej weryfikację wieku. Od dnia 1 września

2027 r. zapewniona zostanie także możliwość wpisania się przez podmioty zainteresowane na listę zaufanych rozwiązań w zakresie weryfikacji wieku.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Ewaluacja realizacji obowiązków internetowych serwisów społecznościowych będzie dokonywana w ramach stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), w szczególności stosowania jego art. 28, który dotyczy ochrony małoletnich w internecie.

Efekty wprowadzanych regulacji prawnych będą miały charakter długofalowy. Będą weryfikowane w ramach zadań realizowanych na zlecenie Ministra Edukacji przez Instytut Badań Edukacyjnych – Państwowy Instytut Badawczy, związanych z monitorowaniem wdrażania Polityki Cyfrowej Transformacji Edukacji, tj.

1.7. Monitorowanie funkcjonowania w praktyce przedszkolnej podstawy programowej wychowania przedszkolnego w obszarze wychowania cyfrowego;

1.8. Monitorowanie funkcjonowania w praktyce szkolnej podstawy programowej kształcenia ogólnego w obszarze rozwijania umiejętności cyfrowych dzieci i młodzieży;

1.9. Monitorowanie funkcjonowania w praktyce podstawy programowej informatyki w zakresie efektów nauczania nowych technologii.

Ponadto Ministerstwo Edukacji Narodowej planuje zlecenie Instytutowi Badań Edukacyjnych – Państwowemu Instytutowi Badawczemu monitorowania skuteczności wprowadzonych ustawą rozwiązań w zakresie ograniczenia korzystania z mediów społecznościowych dla użytkowników poniżej 15 roku życia, w tym wpływu na szeroko rozumiany dobrostan dzieci i młodzieży.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Nie dotyczy.