Edukacja 2026, 3(178)
DOI 10.24131/3724.260301
e-ISSN 2449-8998

Otrzymano: **23.04.2026**
Zaakceptowano: **04.08.2026**
Dostępny online: **od 31.08.2026**

Samoocena kompetencji bezpieczeństwa cyfrowego nauczycieli i rodziców w Polsce

✉ ***Robert Zieliński*** / Instytut Badań Edukacyjnych – Państwowy Instytut Badawczy w Warszawie
e-mail: r.zielinski@ibe.edu.pl
ORCID: 0000-0001-8318-6784

Michał Rostworowski / Instytut Badań Edukacyjnych – Państwowy Instytut Badawczy w Warszawie
e-mail: m.rostworowski@ibe.edu.pl
ORCID: 0000-0001-6028-5480

Streszczenie

Wprowadzenie: Dynamiczny rozwój infrastruktury cyfrowej w Polsce kontrastuje z lukami kompetencyjnymi oraz izolacją działań nauczycieli i rodziców w obszarze socjalizacji cyfrowej. Dotychczasowa literatura rzadko łączy perspektywy obu tych grup w ramach zintegrowanych modeli badawczych. **Cel badań:** Celem artykułu jest analiza porównawcza struktur samooceny kompetencji bezpieczeństwa cyfrowego nauczycieli i rodziców w Polsce oraz identyfikacja obszarów wspólnych deficytów. **Metoda badań:** Badanie oparto na dwóch próbach ankietowych (N = 890 nauczycieli, dobór losowy warstwowy oraz N = 2473 rodziców, dobór celowy). Zastosowano eksploracyjną analizę czynnikową (EFA) oraz współczynnik kongruencji Tuckera (ϕ) do porównania struktur latentnych obu grup. **Wyniki:** Analizy ujawniły wysoką zbieżność struktur samooceny (ϕ=0,950). Wyodrębniono trzy wspólne wymiary: techniczno-edukacyjny, prywatności i zdrowia oraz ekologiczny. Zidentyfikowano „paradoks samooceny cyfrowej" – wysoką pewność w obszarze dobrostanu przy najniższym poczuciu sprawności w zakresie technicznej ochrony urządzeń. **Wnioski:** Homogenizacja samooceny nauczycieli i rodziców podważa tezę o głębokim rozłamie kompetencyjnym i stwarza szansę na budowę zintegrowanego ekosystemu wsparcia. Postuluje się przejście od teoretycznych ram kompetencyjnych ku praktycznym modelom mentoringowym, uwzględniającym nowe ryzyka algorytmiczne i treści syntetyczne.

Słowa kluczowe: **bezpieczeństwo cyfrowe, rodzice, nauczyciele, DigComp, ramy kompetencji**

©Instytut Badań Edukacyjnych – Państwowy Instytut Badawczy

© 2026 Autor(zy). Artykuł opublikowany w otwartym dostępie, rozpowszechniany na warunkach licencji Creative Commons Uznanie autorstwa 4.0 Międzynarodowe (CC BY 4.0). / © 2026 Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Self-Assessment of Digital Safety Competencies Among Teachers and Parents in Poland

Abstract

Introduction: The rapid growth of digital infrastructure in Poland contrasts with competency gaps and the isolation of teachers and parents in the field of digital socialization. Existing literature rarely combines the perspectives of both groups within integrated research models. **Research Aim:** The aim of the article is to conduct a comparative analysis of digital safety self-assessment structures among teachers and parents in Poland and to identify areas of common deficits. **Method:** The study is based on two survey samples (N = 890 teachers, stratified random sampling, and N = 2473 parents, purposive sampling). Exploratory Factor Analysis (EFA) and Tucker's congruence coefficient (ϕ) were used to compare the latent structures of both groups. **Results:** The analyses revealed high congruence in self-assessment structures (ϕ=0.950). Three common dimensions were identified: technical-educational, privacy and health, and ecological. A "digital self-assessment paradox" was observed – high confidence in well-being combined with the lowest perceived proficiency in technical device protection. **Conclusion:** The homogenization of self-assessment among teachers and parents challenges the thesis of a deep competency divide and offers an opportunity to build an integrated support ecosystem. A shift from theoretical frameworks to practical mentoring models is proposed, addressing new algorithmic risks and synthetic content.

Keywords: **digital safety, parents, teachers, DigComp, competency self-assessment**

1. WPROWADZENIE

Ewolucja globalnych sieci komunikacyjnych, zapoczątkowana przejściem z systemów analogowych na cyfrowe rozwiązania takie jak ISDN, uczyniła z ochrony informacji kluczowy element funkcjonowania nowoczesnego państwa i gospodarki (Burr, 1991, s. 22). W czasach, gdy dokumenty elektroniczne niemal całkowicie wypierają tradycyjną formę papierową, wzrasta ryzyko fałszerstw, oszustw oraz nieuprawnionej ingerencji w przesyłane dane (Ibidem, s. 22). Termin bezpieczeństwo cyfrowe w literaturze przedmiotu pojawił się za sprawą Bruce'a Schneiera (często zamiennie z terminem „bezpieczeństwo komputerowe"). Określa się nim zapobieganie i/lub wykrywanie nieautoryzowanych działań podejmowanych przez użytkowników systemu komputerowego (Schneier, 2004). Tak sformułowana definicja wskazuje, że bezpieczeństwo to nie tylko technologia, ale przede wszystkim proces wymagający wdrożenia spójnej polityki, czyli zbioru zasad regulujących zarządzanie i dystrybucję wrażliwych danych.

Współczesna perspektywa bezpieczeństwa cyfrowego powinna uwzględniać nie tylko działania użytkownika, ale także architekturę platform społecznościowych, która poprzez systemy rekomendacyjne i algorytmizację treści aktywnie kształtuje środowisko informacyjne dzieci i młodzieży (Youth AI Safety Institute, 2026). Bezpieczeństwo staje się zatem wypadkową kompetencji jednostki oraz technicznych mechanizmów kontroli uwagi (*attention economy*), które traktują małoletnich użytkowników analogicznie do dorosłych, ignorując specyfikę ich rozwoju poznawczego i emocjonalnego (Common Sense Media, 2026). Jak podkreśla Kreft (2022), platformy – takie jak Google czy Facebook – działają za fasadą przyjaznych interfejsów, będąc w rzeczywistości potężnymi systemami władzy, które poprzez algorytmiczne zarządzanie widocznością informacji mogą wpływać na procesy poznawcze i decyzje użytkowników.

Aktualne ramy ochrony systemów opierają się na pięciu fundamentalnych usługach: poufności, kontroli dostępu, uwierzytelnianiu, integralności danych oraz niezaprzeczalności, które stanowią standardową architekturę bezpieczeństwa dla systemów otwartych (Mitchell, 1990). Jak wskazują autorzy, wyzwanie polega obecnie na rozszerzeniu tych koncepcji na wszystkie aspekty aktywności, ponieważ w dobie hiperłączności „wszystko staje się komputerem", a nasze bezpieczeństwo zależy od ochrony krytycznych funkcji społecznych, gospodarczych i osobistych (Davis, 2019). Dzisiejsze podejście do bezpieczeństwa cyfrowego musi zatem łączyć zaawansowane mechanizmy techniczne z edukacją i psychologią, gdyż bezpieczeństwo pozostaje w dużej mierze „problemem ludzkim" (Schneier, 2000, s. 255), którego nie da się rozwiązać samą technologią bez uwzględnienia specyfiki relacji człowieka z maszyną (Schneier, 2000; Barker, 2019).

W niniejszych analizach kładzie się szczególny nacisk na samoocenę kompetencji rozumianą jako subiektywne poczucie przygotowania respondentów do radzenia sobie z wyzwaniami sieciowymi. Rozróżnienie między realnym poziomem umiejętności a deklaratywnym przekonaniem o własnej biegłości jest kluczowe, gdyż najnowsze analizy wskazują na zjawisko „złudzenia kompetencji" – głęboką dysproporcję między wysoką samooceną sprawności technologicznej a obiektywną wiedzą na temat mechanizmów działania algorytmów i modeli biznesowych platform (Pyżalski i in., 2026).

© 2026 Author(s). CC BY 4.0

Bezpieczeństwo cyfrowe przestało być domeną wyłącznie specjalistów IT, stając się fundamentalną kompetencją życiową. Polityki, strategie oraz programy dotyczące bezpieczeństwa cyfrowego uległy z czasem podwójnemu rozszerzeniu. Po pierwsze, bezpieczeństwo cyfrowe, które pierwotnie było domeną specjalistów IT, wojska, służb wywiadowczych lub operatorów sieci (Spafford, 1988; Global Public Policy Institute, 2015) stało się sprawą zarówno dzieci, młodzieży, jak i dorosłych – w tym rodziców czy nauczycieli. Po drugie, bezpieczeństwo cyfrowe ewoluowało z prostego „cyberbezpieczeństwa" (hasła, wirusy) w stronę cyfrowego dobrostanu (*digital wellbeing*), odporności na dezinformację oraz higieny cyfrowej (Waltzman, 2017; Cain i in., 2018; Vanden Abeele, 2021). W tym ujęciu bezpieczeństwo nie jest już tylko kwestią indywidualnych wyborów użytkownika, lecz wypływa z jego interakcji opartej na nieprzejrzystej architekturze platform społecznościowych. Jak wskazują najnowsze analizy Common Sense Media (2026), algorytmy rekomendacyjne dążą do maksymalizacji zaangażowania poprzez tworzenie tzw. „stanu przepływu" (*flow state*), który u dorosłych i małoletnich użytkowników może prowadzić do zatarcia poczucia czasu i utraty kontroli nad konsumowanymi treściami.

W obliczu dynamicznego rozwoju technologii, dzieci i młodzież są codziennie narażone na zagrożenia: cyberprzemoc, dostęp do nielegalnych treści, uzależnienia behawioralne od social mediów oraz naruszenia prywatności (Livingstone i Stoilova, 2021). Obecnie krajobraz ten został zdominowany przez wektory związane z generatywną sztuczną inteligencją (GenAI). Badania przeprowadzone przez konsorcjum AWO i NSPCC (2026) identyfikują siedem krytycznych kategorii ryzyka, wśród których obok CSAM i groomingu, na plan pierwszy wysuwają się zautomatyzowane nękanie oraz personalizacja treści manipulacyjnych. Szczególnie niebezpieczne staje się zjawisko „nudyfikacji", polegające na wykorzystywaniu narzędzi AI do algorytmicznego usuwania odzieży z rzeczywistych fotografii dzieci w celu wytworzenia fotorealistycznych materiałów o charakterze pornograficznym. Według danych European Parliamentary Research Service (2025), takie materiały o charakterze pornograficznym stanowią obecnie blisko 98% wszystkich niekonsensualnych treści typu deepfake krążących w sieci. Skalę zagrożenia potwierdzają raporty UNICEF (2026), wskazujące, że tylko w ciągu ostatniego roku co najmniej 1,2 miliona dzieci doświadczyło bezprawnego przetworzenia wizerunku w seksualne deepfaki. W tak zarysowanym kontekście kluczowego znaczenia nabiera analiza samooceny kompetencji dorosłych opiekunów, od których biegłości zależy skuteczność mediacji w obliczu nowych ryzyk platformowych.

W literaturze przedmiotu coraz silniej akcentuje się, że kluczem do ochrony młodych ludzi nie jest ograniczanie dostępu, lecz wzmacnianie kompetencji cyfrowych dorosłych – przede wszystkim nauczycieli i rodziców. Należy jednak precyzyjnie odróżnić obiektywne umiejętności od samooceny kompetencji, ponieważ wysokie deklaratywne poczucie przygotowania często maskuje luki poznawcze w zakresie nowych ryzyk platformowych i algorytmicznych. Dla nauczycieli koncepcja ta przekształciła się w profesjonalne kompetencje cyfrowe (*professional digital competence*), które wykraczają poza biegłość techniczną i obejmują umiejętność integracji technologii z procesem dydaktycznym, zarządzanie cyfrowym środowiskiem uczenia się oraz wspieranie autonomii uczniów (McGarr, 2024). Współczesna sprawczość nauczyciela i rodzica wymaga zatem nie tylko wiedzy o „bezpiecznych hasłach", ale przede wszystkim praktycznej umiejętności dekonstrukcji mechanizmów nudyfikacji oraz krytycznego podejścia do treści syntetycznych, co staje się fundamentem nowej pedagogiki bezpieczeństwa cyfrowego. Punktem odniesienia pozostaje europejska rama DigCompEdu, definiująca 22 kompetencje w sześciu obszarach – od profesjonalnego zaangażowania po wzmacnianie kompetencji uczniów i studentów (Redecker, 2017). Współczesna aktualizacja tych standardów, zawarta w ramie DigComp 2.2, redefiniuje tradycyjne podejście do bezpieczeństwa, wprowadzając konkretne przykłady wiedzy i postaw niezbędnych do krytycznej interakcji z systemami AI oraz zrozumienia mechanizmów generowania syntetycznych treści (Vuorikari i in., 2022). Jednak, jak trafnie zauważa McGarr (2024), ramy te, choć pomocne, mogą ograniczać sprawczość nauczycieli, jeśli stosuje się je w sposób linearny i odgórny. Z systematycznych badań przeglądowych wynika, że rzeczywisty poziom tych kompetencji wśród czynnych nauczycieli jest często niski lub średni, szczególnie w obszarze bezpośredniego rozwijania kompetencji cyfrowych uczniów. Kluczowymi predyktorami okazują się doświadczenie zawodowe oraz dostęp do wysokiej jakości szkoleń, a nie tylko staż pracy (Cicha i in., 2021). Luki te stają się szczególnie widoczne w obliczu braku systemowych polityk szkolnych dotyczących generatywnej sztucznej inteligencji; badania wskazują, że blisko 60% nastolatków uczęszcza do placówek, które nie wypracowały jasnych wytycznych w tym zakresie, co pozostawia kadrę pedagogiczną bez narzędzi do reagowania na nowe formy manipulacji algorytmicznej (European Parliamentary Research Service, 2025).

Równolegle do kompetencji nauczycielskich, w dyskursie naukowym ugruntowuje się koncepcja rodzicielstwa cyfrowego (*digital parenting*), która obejmuje trzy główne wymiary: mediację aktywną (rozmowy o treściach), mediację restrykcyjną (ustalanie limitów czasowych) oraz wspólne użytkowanie technologii (Yildirim i in., 2025). Współczesna analiza trendów mediacyjnych w krajach europejskich wskazuje na ewolucję w stronę „rodzicielstwa uważnego", które odchodzi od technicznych blokad na rzecz budowania odporności (*resilience*) dziecka (Kalmus i in., 2022). Integralnym elementem tego modelu staje się krytyczna refleksja nad zjawiskiem sharentingu. Jak wykazuje systematyczny przegląd literatury, intencjonalne publikowanie wizerunku dzieci przez rodziców jest obecnie definiowane nie tylko jako naruszenie prywatności, ale jako proces przedwczesnej i niekonsensualnej konstrukcji tożsamości cyfrowej małoletniego, co rzutuje na jego przyszłą autonomię w środowisku sieciowym (Akay, 2026). Co istotne, skuteczność interwencji skierowanych do rodziców została potwierdzona empirycznie: programy podnoszące ich wiedzę i umiejętności prowadzą nie tylko do wzrostu kompetencji, ale także do wymiernej redukcji czasu ekranowego zarówno u dzieci, jak i u samych rodziców (Economou, 2023).

© 2026 Author(s). CC BY 4.0

Organizacje międzynarodowe, takie jak OECD (2025a i b) i Komisja Europejska (European Commission, 2025), podkreślają przy tym, że tworzenie bezpiecznego środowiska cyfrowego wymaga podejścia angażującego wszystkie podmioty – rządy, dostawców usług cyfrowych, środowisko akademickie, ale przede wszystkim nauczycieli i rodziców, którzy potrzebują jasnych, praktycznych wytycznych, a nie tylko ogólnych zaleceń. W odpowiedzi na te wyzwania, OECD wraz z Komisją Europejską pracują nad ujednoliconą ramą alfabetyzacji algorytmicznej (*AI literacy framework*), której wdrożenie w 2026 roku ma pomóc opiekunom w dekonstrukcji ukrytych mechanizmów perswazyjnych stosowanych przez platformy społecznościowe w celu monetyzacji uwagi małoletnich (UNICEF, 2026; European Parliamentary Research Service, 2025).

W polskich realiach badania wskazują na istnienie wyraźnej „cyfrowej luki pokoleniowej" – rodzice z pokolenia Z sami mają często nie w pełni ukształtowane kompetencje, co komplikuje proces wychowania cyfrowego (Czepiec-Veltzé, 2025; Nesterak i Nesterak, 2023). Zjawisko to jest potęgowane przez ujawniony w najnowszych badaniach mechanizm „złudzenia kompetencji" – sytuację, w której wysoka samoocena sprawności technologicznej dorosłych nie idzie w parze z obiektywną wiedzą o ukrytych mechanizmach działania ekosystemu cyfrowego (Staksrud i in., 2026). Dlatego też w Polsce podejmuje się próby niwelowania problematyki związanej z bezpieczeństwem w oparciu o podnoszenie kompetencji cyfrowych. Przykładem tych tendencji jest przyjęta w marcu 2026 roku przez Radę Ministrów Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M. P. z 2026 r. poz. 309). Strategia ta zakłada szereg działań szkoleniowych dla obywateli, począwszy od dzieci na poziomie przedszkoli. Jednocześnie przewiduje ona podnoszenie kompetencji kadry pedagogicznej. Należy jednak przypuszczać, że działania te mogą okazać się niewystarczające bez uzupełnienia doraźnych szkoleń narzędziowych o systematyczne wspieranie metodyczne oraz krytyczne wykorzystanie technologii – zarówno w szkole, jak i w domu.

Czynnikiem minimalizującym skutki zachowań ryzykownych online jest poziom samooceny kompetencji cyfrowych osób znaczących w procesie socjalizacji młodzieży. Szczególna odpowiedzialność w tym zakresie spoczywa na dwóch grupach dorosłych: nauczycielach i rodzicach. To oni stanowią filary cyfrowej socjalizacji młodego pokolenia, modelując zachowania, reagując na zagrożenia i edukując w zakresie ochrony prywatności, danych oraz cyfrowego dobrostanu. Choć zostało przeprowadzonych wiele badań dotyczących bezpieczeństwa w sieci w obszarze szeroko pojętej edukacji (Amzeyeva i in., 2026; Fraillon i in.,2014, 2025; Ghomi i Redecker, 2019; Hämäläinen i in., 2021; Inamorato i in., 2023, Lange, 2023; Livingstone i Haddon, 2009; Penszko, 2025; Tomczyk i Srokowski, 2016; Wiechetek i Mędrek, 2022), rzadko oferują one panoramiczną wizję tego zagadnienia. Współczesna panorama bezpieczeństwa wykracza poza reaktywne korygowanie zachowań dzieci, stawiając przed dorosłymi wyzwanie zrozumienia systemowej architektury platform. Jak wskazuje analiza ekspertów NSPCC (2026), nauczyciele i rodzice pozostają często merytorycznie bezbronni wobec procesów automatyzacji i personalizacji treści, ponieważ obecne ramy prawne i edukacyjne nie nadążają za tempem rozwoju generatywnej sztucznej inteligencji. W efekcie ich subiektywne poczucie przygotowania często nie uwzględnia konieczności posiadania kompetencji „mentora algorytmicznego", który potrafi dekonstruować ukryte mechanizmy perswazyjne w celu monetyzacji uwagi użytkowników. Biorąc pod uwagę te wyzwania, niniejszy artykuł koncentruje się na analizie struktur samooceny kompetencji nauczycieli i rodziców, co stanowi niezbędny krok w stronę projektowania zintegrowanych systemów wsparcia. Bez pogłębienia tej panoramicznej wiedzy o środowisku sieciowym rola dorosłych ogranicza się jedynie do powierzchownego nadzoru technicznego, co – jak podkreślają badacze z sieci EU Kids Online V – utrwala zjawisko „złudzenia kompetencji" wśród opiekunów i pedagogów (Staksrud i in., 2026).

2. METODOLOGIA

Artykuł opiera się na triangulacji wyników dwóch odrębnych badań ankietowych, których celem był pomiar samooceny kompetencji bezpieczeństwa cyfrowego dorosłych opiekunów procesu socjalizacji cyfrowej dzieci. Pierwsze badanie skierowano do nauczycieli szkół podstawowych i ponadpodstawowych, natomiast drugie do rodziców uczniów tych samych typów placówek. Zastosowanie dwóch prób badawczych podyktowane było potrzebą zderzenia perspektywy szkolnej i domowej przy jednoczesnym uwzględnieniu odmiennych ograniczeń operacyjnych i prawnych. Z metodologicznego punktu widzenia każda z prób została dobrana w sposób optymalny dla specyfiki danej populacji, a wnioskowanie prowadzone jest odrębnie dla każdej z grup – bez bezpośredniego porównywania statystycznego wyników surowych, co mogłoby być obarczone błędem ze względu na różne procedury doboru. Badania mają charakter komplementarny i są rozłączne (żadna szkoła nie uczestniczyła w obu badaniach jednocześnie), a połączenie baz danych służy uzyskaniu panoramicznego obrazu systemu oświaty w obszarze subiektywnego poczucia przygotowania dorosłych do wyzwań cyfrowych.

W grupie nauczycieli zastosowano dobór losowy warstwowy, którego konstrukcja zapewniała wysoki stopień reprezentatywności względem populacji szkół w Polsce. Operat oparto na danych z Systemu Informacji Oświatowej (SIO), wyodrębniając szkoły podstawowe, ponadpodstawowe oraz artystyczne posiadające uprawnienia szkół publicznych (populacja generalna liczyła 22 027 placówek). Proces stratyfikacji przebiegał czterostopniowo i obejmował: województwa, typ organu prowadzącego (szkoły publiczne i niepubliczne), wielkość szkoły (małe do 150 uczniów, średnie 151–600, duże powyżej 600 uczniów) oraz lokalizację (wieś/miasto). Należy wyraźnie zaznaczyć, że jednostkę losowania stanowiła szkoła, natomiast jednostką analizy był nauczyciel. W procesie rekrutacji wyłoniono próbę 2168 szkół, co pozwoliło na zachowanie wysokiej zgodności

© 2026 Author(s). CC BY 4.0

strukturalnej (odchylenia 0,2–0,7 p.p. względem populacji). Jednakże, ze względu na deklaratywny charakter badania i dobrowolność udziału, finalna analiza (w tym eksploracyjna analiza czynnikowa EFA) została przeprowadzona na grupie N = 890 nauczycieli, którzy poprawnie wypełnili kwestionariusze (wskaźnik zwrotu 41,1%), przy założeniu, że z każdej szkoły ankietę wypełnił jeden nauczyciel. Takie podejście pozwala na ocenę wskaźników rezultatu, przy jednoczesnym uwzględnieniu błędu braku odpowiedzi jako ograniczenia badania. Uzyskany poziom zwrotu wśród nauczycieli należy uznać za umiarkowany i zgodny z obserwowanymi trendami w badaniach ankietowych prowadzonych w środowisku oświatowym. Jednocześnie należy podkreślić, że niższa partycypacja i zwrotność w badaniu może wynikać z wysokiego obciążenia obowiązkami zawodowymi oraz zjawiska tzw. „zmęczenia badaniami", co potencjalnie wpływa na reprezentatywność uzyskanych wyników.

Badanie rodziców – ze względu na specyfikę populacji, brak centralnej bazy kontaktów oraz restrykcje wynikające z RODO – wymagało zastosowania procedur innych niż probabilistyczne. Zastosowano dobór nielosowy celowy o charakterze systematycznym, w którym szkoła pełniła rolę jednostki pośredniczącej w rekrutacji. Operatem była pełna populacja szkół podstawowych i ponadpodstawowych w Polsce, z której wyeliminowano placówki uczestniczące w równoległym badaniu nauczycieli, aby zapewnić pełną niezależność obu prób. Finalny operat doboru dla tej grupy liczył 15 851 aktywnych szkół, za pośrednictwem których dotarto do rodziców i opiekunów. Proces zbierania danych trwał od 10 listopada do 10 grudnia 2025 roku i obejmował system monitów oraz przypomnień telefonicznych. Ostatecznie do analizy włączono wyniki od N = 2473 rodziców, co pozwoliło na uchwycenie szerokiego spektrum opinii, choć ze względu na nielosowy charakter doboru wnioski w tej grupie powinny być formułowane z zachowaniem niezbędnej ostrożności metodologicznej.

Proces badawczy rozpoczęto 10.11.2025 r., stosując wieloetapową procedurę kontaktu z respondentami, obejmującą dystrybucję kwestionariuszy oraz system przypomnień (monity w dniach 12.11 i 19.11. 2025 r.), a następnie telefoniczne przypomnienie realizowane w okresie od 24.11 do 10.12.2025 r., co miało na celu zwiększenie poziomu zwrotu ankiet. Od rodziców i opiekunów otrzymano 2473 wypełnionych ankiet. Pozwoliło to na dotarcie do konkretnej grupy respondentów, jednak ogranicza możliwość uogólniania wyników na całą populację ze względu na brak precyzyjnych cech demograficznych i społecznych. Z tego względu wnioski odnoszące się do tej grupy powinny być formułowane z zachowaniem ostrożności metodologicznej.

Skonstruowana na potrzeby badania ankieta objęła cztery bloki tematyczne określone w Europejskiej Ramie Kompetencji Cyfrowych dla Obywateli (DigComp 2.2) oraz dla Nauczycieli (DigCompEdu):

1. Ochrona urządzeń: umiejętności związane z zabezpieczaniem sprzętu cyfrowego, aktualizacją oprogramowania i tworzeniem kopii zapasowych.
2. Ochrona danych osobowych: kompetencje dotyczące ochrony prywatności, rozpoznawania phishingu i kontroli uprawnień aplikacji.
3. Dobrostan cyfrowy: zarządzanie czasem ekranowym, ergonomia pracy z urządzeniami i ochrona przed szkodliwymi treściami.
4. Ochrona środowiska: proekologiczne postawy związane z użytkowaniem technologii: utylizacja sprzętu i oszczędność energii.

Konstrukcja kwestionariusza została oparta na metodzie mapowania kompetencji, w której treść poszczególnych pozycji (itemów) wywodzi się bezpośrednio z deskryptorów zawartych w europejskich ramach DigComp 2.2 (dla rodziców) oraz DigCompEdu (dla nauczycieli). Zastosowana skala stanowi autorską operacjonalizację ośmiu poziomów biegłości zdefiniowanych w ramie DigComp, które dla zwiększenia czytelności i użyteczności w badaniach populacyjnych zostały zagregowane do pięciu głównych etapów rozwoju kompetencji.

Proces przygotowania narzędzia przebiegał w trzech rygorystycznych etapach:

1. Wyselekcjonowano kluczowe deskryptory dla czterech obszarów: ochrony urządzeń, danych osobowych, dobrostanu cyfrowego oraz środowiska. Pytania w obu kwestionariuszach zachowały tożsamość merytoryczną, poddano je jedynie niezbędnej adaptacji kontekstowej (np. „uczniowie" w grupie nauczycieli vs „dzieci" w grupie rodziców), co zapewniło wysoką porównywalność struktur latentnych między grupami.
2. Projekt kwestionariusza poddano ocenie niezależnych ekspertów z zakresu edukacji medialnej i cyberbezpieczeństwa. Eksperci potwierdzili trafność treściową pozycji oraz adekwatność skali do specyfiki mierzonych konstruktów.
3. Przed etapem właściwym przeprowadzono badanie pilotażowe (N=22). Na tej podstawie zoptymalizowano liczbę pytań oraz przeprowadzono standaryzację skali odpowiedzi. Dla zachowania pełnej liniowości pomiaru i rygoru statystycznego, pierwotne deklaracje respondentów zostały zmapowane na jednolitą skalę rosnącą 1–5 (gdzie 1 oznacza całkowity brak umiejętności lub poziom podstawowy, a 5. poziom wysoko specjalistyczny/ekspercki).

Rzetelność wewnętrzną narzędzia zweryfikowano za pomocą szeregu wskaźników statystycznych (Tabela 1). Uzyskane wyniki potwierdzają bardzo wysoką spójność wewnętrzną skal w obu grupach badawczych.

© 2026 Author(s). CC BY 4.0

Tabela 1 ***Parametry rzetelności kwestionariusza samooceny kompetencji bezpieczeństwa cyfrowego***

Wskaźnik	Nauczyciele	Rodzice
Alfa Cronbacha	0,928	0,931
Alfa standaryzowana	0,93	0,931
Liczba pozycji	16	16
Średnia korelacja międzypozycyjna	0,452	0,459
Zakres korelacji item–total	0,129 – 0,789	0,186 – 0,785
Zakres alfa po usunięciu pozycji	0,922 – 0,927	0,926 – 0,928
Zakres średnich pozycji	2,984 – 3,789	3,119 – 3,778
Zakres odchyleń standardowych	1,035 – 1,804	1,155 – 1,871
Zakres wariancji pozycji	1,035 – 1,804	1,155 – 1,871
Test Hotellinga T^2	T^2 = 1575,949; F(15, 874) = 68,604; p < 0,001	T^2 = 5109,142; F(15, 2457) = 317,365; p < 0,001

Źródło: *Opracowanie własne.*

Wartości współczynnika Alfa Cronbacha osiągnęły poziom 0,928 dla nauczycieli oraz 0,931 dla rodziców, co świadczy o wysokiej stabilności pomiaru. Analiza korelacji pozycji z wynikiem ogólnym (item–total) oraz średnie korelacje międzypozycyjne (0,452 dla nauczycieli i 0,459 dla rodziców) potwierdzają, że wybrane itemy w sposób spójny budują strukturę mierzonych czynników. Dodatkowo istotny statystycznie wynik testu Hotellinga T^2 ($p < 0,001$ dla obu grup) dowodzi, że średnie oceny w poszczególnych pozycjach różnią się od siebie w sposób istotny, co uzasadnia wielowymiarowe podejście do analizy samooceny kompetencji. Tak wysokie parametry psychometryczne, w połączeniu z procedurą sędziowską i mapowaniem deskryptorów europejskich ram kompetencji, uprawniają do traktowania narzędzia jako w pełni zwalidowanej matrycy badawczej, pozwalającej na rzetelną ocenę subiektywnego poczucia przygotowania dorosłych do wyzwań cyfrowych.

3. WYNIKI

W celu dokonania zarysu rozkładu ocen respondentów w czterech blokach tematycznych przeprowadzono analizę statystyk opisowych. W Tabeli 2 przedstawiono wartości średnich arytmetycznych ($\bar{x}$), odchyleń standardowych (SD), wariancji (s2) oraz kurtozy (Kurt) dla grup nauczycieli i rodziców.

Tabela 2 ***Statystyki opisowe***

Grupa badana	Statystyka	Ochrona urządzeń	Ochrona danych osobowych	Ochrona dobrostanu	Ochrona środowiska
Nauczyciele	Średnia (M)	2,37	2,45	2,66	2,58
	Odchylenie standardowe (SD)	1,46	1,53	1,515	1,674
	Wariancja (SD^2)	2,132	2,641	2,295	2,802
	Kurtoza	-1,263	-1,151	-0,901	-1,31
Rodzice	Średnia (M)	2,39	2,44	2,64	2,55
	Odchylenie standardowe (SD)	1,539	1,586	1,53	1,653
	Wariancja (SD^2)	2,367	2,516	2,341	2,731
	Kurtoza	-1,343	-1,329	-0,979	-1,324

Źródło: *Opracowanie własne.*

© 2026 Author(s). CC BY 4.0

Średnie arytmetyczne w obu grupach badanych mieściły się w wąskim przedziale od 2,37 do 2,66, co świadczy o umiarkowanie wysokim poziomie postrzeganej ważności analizowanych obszarów, zwłaszcza w obszarze ochrony dzieci w środowisku cyfrowym. Najwyższe wartości średnich odnotowano w bloku Ochrona dobrostanu (nauczyciele: $\bar{x}$ = 2,66; rodzice: $\bar{x}$ = 2,64), natomiast najniższe w bloku Ochrona urządzeń (nauczyciele: $\bar{x}$ = 2,37; rodzice: $\bar{x}$ = 2,39). Charakterystyczną cechą uzyskanych rozkładów jest umiarkowana zmienność odpowiedzi typowa dla skal Likertowskich. Odchylenia standardowe wynosiły od 1,460 do 1,674. Najmniejszy rozrzut stwierdzono w bloku Ochrona urządzeń w grupie nauczycieli (SD = 1,460). Grupa nauczycieli wykazywała nieznacznie niższe wartości odchyleń standardowych (średnie SD ≈ 1,545) w porównaniu z grupą rodziców (średnie SD ≈ 1,577), co wskazuje na nieco większą homogeniczność ocen w populacji nauczycielskiej.

Analiza kurtozy ujawniła dominację rozkładów platykurtycznych (ujemna kurtoza we wszystkich 8 przypadkach). Kurtoza we wszystkich blokach była ujemna, co wskazuje na spłaszczone rozkłady w porównaniu z rozkładem normalnym.

Uzyskane statystyki opisowe wskazują na wysoką zbieżność poziomu ocen oraz rozrzutu między grupami nauczycieli i rodziców. Różnice w wartościach centralnych i miarach zmienności są minimalne, co pozwala wnioskować o istnieniu skupienia, szerokiego konsensusu w postrzeganiu ważności ochrony dzieci w środowisku cyfrowym. Brak dodatniej kurtozy wyklucza występowanie polaryzacji opinii lub znaczących grup „ekstremalnych" wśród nauczycieli i rodziców. W żadnym z czterech bloków nie stwierdzono istotnej statystycznie różnicy między tymi grupami. Nauczyciele ogółem nie wykazują przewagi nad rodzicami pod względem subiektywnego poczucia przygotowania w zakresie samooceny kompetencji w obszarze bezpieczeństwa cyfrowego.

3.1 Analizy czynnikowe

W celu zweryfikowania, czy obie grupy postrzegają samoocenę omawianych kompetencji w podobny sposób, przeprowadzono eksploracyjną analizę czynnikową (EFA) oddzielnie dla każdej próby – losowej wśród nauczycieli (N = 890) oraz nielosowej wśród rodziców (N = 2473). Do ekstrakcji zastosowano metodę głównych składowych, a analizy przeprowadzono na macierzy korelacji Pearsona. Braki danych traktowano zgodnie z procedurą listwise deletion, co oznaczało wykluczanie obserwacji zawierających braki w którejkolwiek z analizowanych zmiennych, zapewniając rzetelność obliczeń dla pełnych zestawów odpowiedzi. Adekwatność macierzy korelacji do analizy czynnikowej potwierdziły wartości wyznacznika (determinantu). W grupie nauczycieli determinant wyniósł 9,817×10-6, natomiast w grupie rodziców 1,715×10-5. Tak niskie wartości wskazują na silne powiązania między pozycjami oraz brak problemów z osobliwością macierzy, co uzasadnia zastosowanie analizy czynnikowej.

Liczbę czynników dla obu grup ustalono na podstawie kryterium Kaisera (wartości własne > 1), analizy wykresu osypiska oraz merytorycznej interpretowalności rozwiązań. W tym wypadku, porównanie struktur czynnikowych wymaga zastosowania procedur dedykowanych do niezależnych macierzy ładunków. Metoda ta jest stosowana, gdy nie dysponujemy danymi surowymi umożliwiającymi wielogrupową analizę konfirmacyjną (multi-group CFA) lub gdy próby pochodzą z odmiennych populacji i różnią się doborem (por. Osborne, 2015; Lorenzo-Seva i ten Berge, 2006). W procedurze rotacji macierzy zastosowano metodę Varimax z normalizacją Kaisera. Wybór ten podyktowany był faktem, iż wstępne korelacje między czynnikami były umiarkowane, a celem badania było uzyskanie prostych, ortogonalnych ładunków ułatwiających przejrzyste porównanie struktur między niezależnymi próbami nauczycieli i rodziców. Dodatkowo, w celu weryfikacji rzetelności rozwiązania, przeprowadzono równoległą rotację Oblimin, która dała zbliżone wyniki, co potwierdza wysoką stabilność latentnej struktury narzędzia i uzasadnia raportowanie rotacji Varimax jako głównej.

3.2 Porównanie jakości modeli EFA

Obie analizy spełniały kryteria adekwatności doboru próby (Tabela 2). Miara adekwatności próby KMO osiągnęła wartość 0,929 w grupie nauczycieli i 0,928 w grupie rodziców, co wskazuje na bardzo dobrą przydatność danych do wyodrębniania czynników. Test sferyczności Bartletta był istotny statystycznie w obu przypadkach (nauczyciele: χ^2 = 10 180,255, df = 120, $p < 0,001$; rodzice: χ^2 = 27 058,839, df = 120, $p < 0,001$).

© 2026 Author(s). CC BY 4.0

Tabela 3 ***Wskaźniki jakości modeli EFA w obu grupach***

Wskaźniki	Nauczyciele (N = 890)	Rodzice (N = 2473)
Miara adekwatności próby KMO	0,929	0,928
Test sferyczności Bartletta (χ^2)	10 180,255	27 058,839
df	120	120
Istotność (p)	< 0,001	< 0,001
Liczba wyodrębnionych składowych	3	3
Wyjaśniona wariancja po rotacji	70,989 %	69,500 %

Źródło: *Opracowanie własne.*

Decyzję o zatrzymaniu trzech czynników wsparły zarówno kryterium Kaisera (wartości własne > 1), jak i analiza wykresu osypiska (scree plot). W obu grupach wykres wykazywał wyraźny „łokieć" już po trzecim czynniku. Początkowe wartości własne dla nauczycieli wynosiły kolejno: 7,853 (co wyjaśnia 49,08% wariancji), 2,468 (15,43%) oraz 1,037 (6,48%), po czym gwałtownie spadały do poziomu 0,797. W grupie rodziców wartości własne wynosiły odpowiednio: 7,931 (49,57%), 2,168 (13,55%) i 1,021 (6,38%), z kolejnym spadkiem do poziomu 0,736. Stabilizacja linii po trzecim czynniku była widoczna i niemal identyczna w obu próbach, co potwierdza zasadność trzyczynnikowego rozwiązania struktury samooceny kompetencji.

Po zastosowaniu rotacji Varimax z normalizacją Kaisera łączna wyjaśniona wariancja wyniosła 70,989% u nauczycieli oraz 69,500% u rodziców, co świadczy o wysokiej zdolności modelu do wyjaśniania zmienności subiektywnych ocen respondentów.

Tabela 4 ***Początkowe wartości własne i procent wyjaśnianej wariancji dla trzech wyodrębnionych składowych***

Grupy badane	Składowe			
	1	2	3	4+
Nauczyciele (N = 890)	7,853 (49,082%)	2,468 (15,425%)	1,037 (6,482%)	< 1,0
Rodzice (N = 2473)	7,931 (49,571%)	2,168 (13,550%)	1,021 (6,379%)	< 1,0

Źródło: *Opracowanie własne.*

3.3 Struktura czynnikowa w każdej grupie

Analiza macierzy ładunków rotowanych ujawniła zarówno wyraźne podobieństwa, jak i subtelne różnice wynikające z kontekstu roli pełnionej przez respondentów. Macierz przedstawiona w Tabeli 5 umożliwia szczegółową analizę sposobu, w jaki nauczyciele i rodzice konceptualizują własną samoocenę kompetencji związanych z bezpieczeństwem cyfrowym. Zastosowana procedura EFA ujawniła stabilne, dobrze odseparowane wymiary, co potwierdza wysoką trafność konstrukcyjną narzędzia i spójność jego struktury w dwóch odmiennych populacjach. W grupie nauczycieli wyodrębniono trzy względnie wyraźne wymiary samooceny: pierwszy czynnik (Postawy i Ekologia) obejmował przede wszystkim odpowiedzialne korzystanie z technologii oraz troskę o środowisko, drugi (Prywatność i Prewencja) – subiektywne poczucie kontroli ochrony prywatności i danych osobowych, natomiast trzeci (Biegłość techniczna) – deklarowaną sprawność w zakresie ochrony urządzeń (aktualizacje, backup, zarządzanie uprawnieniami).W grupie rodziców struktura była silniej zintegrowana z rolą wychowawczą. Pierwszy czynnik (Techniczne bezpieczeństwo i Edukacja) łączył deklarowane umiejętności techniczne z edukacją dzieci, drugi skupiał się na samoocenie ochrony prywatności i zdrowiu psychicznym (w tym przekazywaniu zasad dzieciom), natomiast trzeci czynnik – podobnie jak u nauczycieli – był bardzo wyraźnym, niemal czystym wymiarem ekologicznym. Mimo drobnych różnic w brzmieniu pytań wynikających z adaptacji kontekstowej, latentna struktura samooceny kompetencji cyfrowych okazała się stabilna.

© 2026 Author(s). CC BY 4.0

Tabela 5 ***Macierz ładunków rotowanych (Varimax) dla trzech czynników wyodrębnionych metodą głównych składowych w grupach nauczycieli i rodziców***

Nauczyciele (N = 890)			
Item	Odpowiedzialne/Ekologia	Prywatność	Techniczne bezpieczeństwo urządzeń
Zachęcam uczniów do odpowiedzialnego korzystania z technologii cyfrowych	**0,868**	0,175	0,126
Dbam o to, aby urządzenia elektroniczne nie zużywały energii bez potrzeby	**0,866**	0,216	0,072
Zwracam uwagę na recykling sprzętu	**0,838**	0,184	0,1
Zarządzam czasem spędzonym przy urządzeniach cyfrowych	**0,663**	0,434	0,117
Dbam o ergonomię pracy z urządzeniami cyfrowymi	**0,634**	0,478	0,161
Rozpoznaję podejrzane wiadomości e-mail	0,306	**0,79**	0,227
Sprawdzam bezpieczeństwo stron internetowych	0,259	**0,775**	0,322
Sprawdzam polityki prywatności usług cyfrowych	0,172	**0,758**	0,365
Ograniczam dostęp do lokalizacji	0,273	**0,745**	0,253
Chronię się przed hejtem i cyberprzemocą	**0,569**	**0,583**	0,145
Korzystam z narzędzi wspierających osoby starsze lub o specjalnych potrzebach	0,404	**0,535**	0,264
Monitoruję i kontroluję uprawnienia aplikacji	0,047	0,218	**0,856**
Odzyskuję informacje z kopii zapasowej	0,019	0,167	**0,831**
Edukuję uczniów w zakresie ochrony urządzeń	0,181	0,222	**0,801**
Konfiguruję zabezpieczenia dostępu	0,133	0,258	**0,759**
Monitoruję i aktualizuję system operacyjny	0,177	0,214	**0,757**
Rodzice (N=2473)			
Item	Techniczne/Edukacja	Prywatność/Zdrowie	Ekologia
Odzyskuję informacje z kopii zapasowej (techniczne)	**0,858**	0,067	0,084
Monitoruję i kontroluję uprawnienia aplikacji	**0,814**	0,266	0,1
Monitoruję i aktualizuję system operacyjny	**0,781**	0,178	0,109
Odzyskuję informacje z kopii zapasowej (prywatność)	**0,742**	0,259	0,068
Edukuję dzieci w zakresie ochrony urządzeń	**0,701**	0,378	0,157
Monitoruję uprawnienia (prywatność)	**0,676**	0,443	0,103
Konfiguruję zabezpieczenia dostępu	**0,66**	0,282	0,202
Chronię się przed hejtem i cyberprzemocą	0,23	**0,772**	0,244
Przekazuję dzieciom zasady ochrony urządzeń	0,313	**0,763**	0,258
Rozpoznaję podejrzane wiadomości e-mail	0,285	**0,729**	0,18
Ograniczam dostęp do lokalizacji	0,3	**0,711**	0,174
Zarządzam czasem ekranowym	0,236	**0,676**	0,345
Dbam o ergonomię pracy	0,209	**0,673**	0,36
Przekazuję dzieciom postawy ekologiczne	0,159	0,314	**0,861**
Dbam o oszczędzanie energii	0,121	0,27	**0,857**
Zwracam uwagę na recykling sprzętu	0,119	0,281	**0,843**

Źródło: *Opracowanie własne.*

© 2026 Author(s). CC BY 4.0

Dane zaprezentowane w Tabeli 5 pozwalają na identyfikację konkretnych wag czynnikowych, które definiują strukturę samooceny obu grup. W populacji nauczycieli najwyższy stopień spójności odnotowano w obrębie wymiaru Postawy i Ekologia, gdzie pozycje dotyczące zachęcania uczniów do odpowiedzialności (0,868) oraz dbałości o energię (0,866) wykazują najsilniejszy związek z czynnikiem. Drugi wymiar (Prywatność) jest najsilniej reprezentowany przez deklarowaną zdolność rozpoznawania phishingu (0,790) oraz weryfikację bezpieczeństwa witryn (0,775). Z kolei samoocena biegłości technicznej (Czynnik 3) opiera się na wysokim poczuciu sprawności w monitorowaniu uprawnień aplikacji (0,856) oraz odzyskiwaniu danych z kopii zapasowej (0,831). Odnotowane w tej grupie obciążenie krzyżowe (*cross-loading*) pozycji dotyczącej ochrony przed hejtem (0,569 w C1 i 0,583 w C2) stanowi statystyczny dowód na to, że nauczyciele postrzegają przeciwdziałanie agresji online jako zjawisko nierozerwalnie łączące etykę korzystania z sieci z techniczną i społeczną prewencją.

W grupie rodziców tabela uwidacznia specyficzne dla tej roli splatanie się technologii z funkcją opiekuńczą. Subiektywne poczucie biegłości technicznej w C1 silnie koreluje z procesem edukowania dzieci, o czym świadczą ładunki dla pozycji dotyczących backupu (0,858) oraz edukacji dzieci w zakresie ochrony urządzeń (0,701). Czynnik drugi (Prywatność i Zdrowie) jest najsilniej definiowany przez samoocenę przygotowania do ochrony przed hejtem (0,772) oraz przekazywanie dzieciom zasad ochrony (0,763). Wymiar ekologiczny (C3) u rodziców jest konstruktem o najwyższym stopniu statystycznej separacji i czystości, co potwierdzają ładunki powyżej 0,840 dla wszystkich trzech pozycji składowych (postawy: 0,861; energia: 0,857; recykling: 0,843). Wskazuje to na klarowne oddzielenie świadomości środowiskowej od operacyjnych aspektów zabezpieczania infrastruktury cyfrowej w percepcji rodziców.

3.4 Porównanie podobieństwa struktur samooceny

Do ilościowego porównania niezależnych rozwiązań czynnikowych zastosowano współczynnik kongruencji Tuckera (Tucker's φ), który jest uznawany za najbardziej wiarygodną miarę podobieństwa macierzy ładunków (Lorenzo-Seva i ten Berge, 2006). Wzór obliczeniowy dla pary czynników ma postać:

$$\emptyset\, AB = \frac{\Sigma_{i=1}^{16} - a_i b_i}{\sqrt{\left(\Sigma_{i=1}^{16} a_i^2\right) + \left(\Sigma_{i=1}^{16} b_i^2\right)}}$$

Gdzie:

Φ AB – współczynniki kongruencji Tuckera;

a_i i b_i – ładunki standaryzowane i-tej pozycji w danym czynniku.

Wysoka wartość kongruencji Tuckera, choć wskazuje na podobieństwo „kształtu" i konfiguracji czynników, nie jest tożsama z dowodem na pełną inwariancję pomiarową (*measurement invariance*) między grupami. Oznacza to, że choć struktura latentna postrzegania bezpieczeństwa jest zbliżona, rodzice i nauczyciele mogą w odmienny sposób interpretować poszczególne poziomy skali samooceny, co nakazuje ostrożność w bezpośrednim porównywaniu wyników surowych.

Po optymalnym przyporządkowaniu czynników uzyskano wartości kongruencji (Tabela 6), z których wynika, iż średnia wartość φ po dopasowaniu wyniosła 0,950, co wskazuje na bardzo wysoką zgodność struktur samooceny czynnikowych między nauczycielami a rodzicami.

Tabela 6 ***Współczynniki kongruencji Tuckera (ϕ) między czynnikami***

	Rodzice C1	Rodzice C2	Rodzice C3
Nauczyciele C1	0,701	**0,928**	0,546
Nauczyciele C2	**0,955**	0,539	0,324
Nauczyciele C3	0,406	0,756	**0,965**

Źródło: *Opracowanie własne.*

Wysoka wartość współczynnika kongruencji (0,950) świadczy o tym, że pomimo różnic w doborze próby i adaptacji pytań, kwestionariusz identyfikuje zbliżone wymiary subiektywnego poczucia przygotowania w obu populacjach. Największa zbieżność dotyczy wymiaru techniczno-edukacyjnego (ϕ = 0,955) oraz wymiaru ekologicznego (ϕ = 0,965). Nieco niższa, choć nadal bardzo dobra zgodność wystąpiła w wymiarze prywatności i ochrony zdrowia (ϕ = 0,928). U rodziców deklarowana po-

© 2026 Author(s). CC BY 4.0

trzeba edukacji dzieci silniej splata się z własną samooceną sprawności technicznej. Analiza szczegółowa powiązań wskazuje, że u rodziców deklarowana potrzeba edukacji dzieci silniej splata się z własną samooceną sprawności technicznej, podczas gdy u nauczycieli te sfery są bardziej odseparowane. Wyniki prowadzą do wniosku, że struktura samooceny kompetencji obu grup jest w wysokim stopniu zbieżna, co pozwala traktować nauczycieli i rodziców jako posiadających wspólną przestrzeń postrzegania wyzwań cyfrowych. Stanowi to istotną przesłankę do projektowania spójnych inicjatyw edukacyjnych skierowanych jednocześnie do obu grup opiekunów.

4. DYSKUSJA

Wyniki przeprowadzonej eksploracyjnej analizy czynnikowej (EFA) wskazują na wysoką zbieżność między nauczycielami a rodzicami w samoocenie własnych umiejętności, co stanowi przesłankę do rewizji tezy o głębokim rozłamie w subiektywnym poczuciu przygotowania między środowiskiem domowym a szkolnym. Współczynnik kongruencji Tuckera na poziomie $\phi = 0{,}950$ świadczy o wysokim podobieństwie struktur postrzegania wyzwań cyfrowych, co można interpretować jako efekt „wymuszonej synergii popandemicznej", która ujednoliciła słownik pojęć związanych z zagrożeniami sieciowymi. Należy jednak wyraźnie zaznaczyć, że wysoka wartość kongruencji, choć wskazuje na zbieżność map pojęciowych obu grup, nie dowodzi pełnej inwariancji pomiarowej między populacjami, co nakazuje ostrożność w bezpośrednim zestawianiu deklarowanych poziomów biegłości. Pandemia COVID-19 wymusiła na obu grupach dorosłych opiekunów szybkie dostosowanie się do realiów edukacji zdalnej i hybrydowej, co doprowadziło do konwergencji percepcji kompetencji i wspólnego doświadczenia deficytów technicznych (Polski Instytut Ekonomiczny, 2021; Związek Cyfrowa Polska, 2024).

Brak statystycznej przewagi nauczycieli nad rodzicami w zakresie deklarowanego przygotowania do zapewnienia bezpieczeństwa cyfrowego może stanowić przesłankę do dyskusji nad ewolucją instytucjonalnego statusu szkoły jako technologicznej „bezpiecznej przystani". W konsekwencji można przypuszczać, że proces socjalizacji cyfrowej młodzieży odbywa się w warunkach potencjalnie ograniczonego wsparcia technicznego ze strony dorosłych, gdyż jedynie mniejszość opiekunów z badanych grup postrzega siebie w roli autentycznego przewodnika technologicznego.

Samoocena kompetencji nauczycieli i rodziców kształtuje się na podobnych poziomach, co może utrudniać budowanie spójnego, komplementarnego systemu wsparcia dla dzieci i młodzieży (Związek Cyfrowa Polska, 2024). Ta wspólna struktura deficytów ujawnia się najwyraźniej w występowaniu tzw. paradoksu samooceny cyfrowej – obie grupy deklarują najwyższą pewność w obszarze ochrony dobrostanu i walki z hejtem (nauczyciele: 2,66; rodzice: 2,64), przy jednoczesnym subiektywnym poczuciu niższej sprawności wobec technicznych aspektów ochrony urządzeń (nauczyciele: 2,37; rodzice: 2,39). Postrzegana koncentracja na „miękkich" skutkach behawioralnych przy jednoczesnym deklarowanym deficycie biegłości w zakresie technologicznych przyczyn zagrożeń stanowi istotne wyzwanie dla systemu oświaty. Ochrona dzieci może stawać się przez to niepełna, ograniczając się do zaleceń wychowawczych przy subiektywnie odczuwanym niedoborze umiejętności w obszarze zabezpieczania infrastruktury i danych osobowych.

W literaturze międzynarodowej, w tym w analizach OECD, podkreśla się, że formalne modele kompetencji cyfrowych nauczycieli nie zawsze przekładają się na ich zdolność do działania w rzeczywistych sytuacjach problemowych, zwłaszcza w obszarze cyberbezpieczeństwa (OECD, 2025a, 2025b). Badania empiryczne potwierdzają tę lukę – nauczyciele najczęściej uzyskują najniższe wyniki właśnie w obszarze „Ochrona danych i bezpieczeństwo cyfrowe" w ramach DigCompEdu (Cattaneo i in., 2022). W tym kontekście coraz częściej wskazuje się na potrzebę uzupełnienia podejścia systemowego o rozwiązania o charakterze praktycznym, takie jak modele wsparcia *on-demand* (tzw. „pogotowie cyfrowe") oraz programy mentoringowe, w których doświadczeni praktycy wspierają nauczycieli i rodziców w rozwiązywaniu konkretnych problemów technologicznych. Sugeruje to, że same teoretyczne ramy mogą być niewystarczające bez odniesienia do dynamicznie zmieniającego się krajobrazu ryzyk, takich jak manipulacje algorytmiczne czy treści syntetyczne (Staksrud i in., 2026).

W Polsce dotychczasowe doświadczenia w zakresie wdrażania ram kompetencyjnych, w tym DigCompEdu, tworzą solidną podstawę do dalszego doskonalenia systemu rozwijania kompetencji cyfrowych. Choć badanie koncentrowało się na subiektywnych deklaracjach dorosłych, uzyskane wyniki stanowią istotny kapitał dla projektowania polityki publicznej, w której możliwe jest pogłębienie komponentu praktycznego oraz lepsze powiązanie działań szkoleniowych z realnymi wyzwaniami użytkowników. Podejście to nabiera szczególnego znaczenia w zderzeniu z najnowszymi wynikami badań reprezentatywnych (Tomczyk, 2026), które wskazują na występowanie u młodzieży zjawiska „złudzenia kompetencji" – głębokiej dysproporcji między wysoką samooceną a niskim poziomem obiektywnej wiedzy o mechanizmach sieci, co czyni rolę merytorycznie przygotowanego opiekuna – mentora kwestią krytyczną.

Uporządkowana struktura oraz spójność z europejskimi standardami sprzyjają budowaniu wspólnego języka opisu samooceny umiejętności i potrzeb szkoleniowych (M.P. 2026 r. poz. 309). Stanowi to istotny kapitał dla projektowania kolejnych etapów polityki publicznej, w których możliwe jest pogłębienie komponentu praktycznego oraz lepsze powiązanie działań szkoleniowych z realnymi wyzwaniami użytkowników. W tym ujęciu analiza i rozwój założeń Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. 2026 r. poz. 309) może przyczynić się do wypracowania bardziej zintegrowanych i efektywnych modeli wsparcia, łączących dorobek podejścia systemowego z rozwiązaniami odpowiadającymi na bieżące potrzeby

© 2026 Author(s). CC BY 4.0

deklarowane przez respondentów. Jednocześnie wyniki analiz empirycznych wskazują, że szczególny potencjał integracyjny posiada wymiar określany jako „ekologia cyfrowa", dla którego odnotowano bardzo wysoki poziom zgodności struktur czynnikowych (ϕ = 0,965). Należy jednak zaznaczyć, że choć wynik ten świadczy o zbieżności „mapy pojęciowej" obu grup, nie stanowi on bezpośredniego dowodu na pełną inwariancję pomiarową między populacjami.

Niemniej jednak sugeruje to, że świadomość środowiskowych konsekwencji korzystania z technologii stanowi relatywnie spójny poznawczo obszar, sprzyjający budowaniu wspólnych ram interpretacyjnych między różnymi grupami interesariuszy. Wykorzystanie tego komponentu jako punktu wyjścia może sprzyjać projektowaniu bardziej zintegrowanych środowisk edukacyjnych, w których szkoła i dom funkcjonują w sposób komplementarny, wspierając rozwój bezpiecznych i odpowiedzialnych praktyk cyfrowych (por. Ricoy i in., 2022). Podejście to wpisuje się w postulaty płynące z najnowszych badań *EU Kids Online* (2026) wskazujących na konieczność wielostronnego wsparcia dzieci w obliczu nowych ryzyk platformowych, takich jak algorytmizacja treści czy deepfaki.

Obserwowana zbieżność samooceny deficytów kompetencyjnych między nauczycielami a rodzicami nie jest zjawiskiem marginalnym, lecz strukturalnym efektem postpandemicznej transformacji (Polski Instytut Ekonomiczny, 2021). Wyniki te sugerują potrzebę ewolucji programów szkoleniowych w stronę modelu zintegrowanego ekosystemu edukacyjno-rodzinnego. Wykorzystanie obszarów wspólnej percepcji – takich jak ekologia cyfrowa – oraz wdrożenie praktycznych, mentoringowych form wsparcia może sprzyjać wzmocnieniu roli dorosłych w pełnieniu funkcji przewodników w cyfrowej socjalizacji młodzieży.

5. WNIOSKI

Analiza zebranego materiału badawczego oraz przeprowadzone operacje statystyczne wnoszą nowe przesłanki do dyskusji nad relacją między szkołą a domem w procesie socjalizacji cyfrowej. Najważniejszą konkluzją, rzucającą nowe światło na polski system oświaty, jest zauważalne zacieranie się tradycyjnej hierarchii kompetencyjnej, w której nauczyciel pełnił rolę eksperta i przewodnika dla rodzica. Badania dowiodły występowanie zjawiska homogenizacji samooceny kompetencyjnej. Przejawia się ona brakiem statystycznie istotnych różnic w poczuciu przygotowania do zapewnienia bezpieczeństwa cyfrowego między kadrą pedagogiczną a opiekunami. Wynik ten może sugerować ewolucję instytucjonalnego statusu szkoły jako technologicznej „bezpiecznej przystani". Wskazuje to na potrzebę wzmocnienia obiektywnej wiedzy dorosłych, gdyż – jak potwierdzają najnowsze analizy europejskie (Stoilova i in., 2025) – wysokie poczucie pewności opiekunów nie zawsze chroni dzieci przed nowymi ryzykami, takimi jak algorytmizacja treści czy manipulacje z wykorzystaniem generatywnej sztucznej inteligencji (GenAI).

Doświadczenie edukacji zdalnej ujednoliciło słownik pojęć i subiektywną percepcję zagrożeń, niwelując dotychczasowe różnice między domem a szkołą (Ptaszek i in., 2020; Vegas i Winthrop, 2020), co z jednej strony obnaża wspólne deficyty, a z drugiej stanowi unikalną okazję do budowy zintegrowanego ekosystemu edukacyjno-rodzinnego. Skoro obie grupy posługują się zbliżoną matrycą postrzegania problemów, przyszłe programy wsparcia powinny być projektowane jako wspólne platformy wymiany doświadczeń, a nie izolowane kursy dla poszczególnych grup. Badania ujawniły istnienie głębokiego rozwarstwienia między deklarowaną świadomością zagrożeń a poczuciem przygotowania do ich praktycznej neutralizacji, co można określić mianem „paradoksu samooceny cyfrowej".

Zarówno rodzice, jak i nauczyciele najwyżej oceniają swoją samoocenę kompetencji w obszarze ochrony dobrostanu i przeciwdziałania hejtowi, co sugeruje sprawne poruszanie się w sferze „miękkich" zaleceń wychowawczych. Jednocześnie te same grupy wykazują najniższą pewność w zakresie technicznej ochrony urządzeń i danych. Wniosek ten nabiera szczególnej wagi w zderzeniu z raportami dokumentującymi drastyczny (o 1325%) wzrost zgłoszeń materiałów CSEA generowanych przez AI w ujęciu rocznym oraz masową skalę „nudyfikacji" wizerunków dzieci (co najmniej 1,2 mln ofiar rocznie) (NCMEC, 2025).

Dane z reprezentatywnego badania polskich uczniów obalają dodatkowo mit o „naturalnych" kompetencjach młodzieży, wykazując, że aż 62,9% respondentów uzyskuje niskie wyniki w obiektywnych testach wiedzy o mechanizmach sieci (algorytmy, modele biznesowe), mimo wysokiej samooceny (Tomczyk, 2026, s. 49–50). Ponadto ujawniona zbieżność struktur samooceny rodziców i nauczycieli daje unikalną szansę na przełamanie tzw. bariery milczenia – co piąty nastolatek po trudnym doświadczeniu w sieci nie szuka pomocy u nikogo z lęku przed restrykcyjną reakcją dorosłych, najczęściej utożsamianą z odebraniem telefonu. Świadomość wpływu technologii na środowisko stała się elementem szerszej odpowiedzialności społecznej Polaków. Komponent proekologiczny może pełnić rolę „pomostu komunikacyjnego" ułatwiającego wprowadzanie trudniejszych tematów z zakresu cyberbezpieczeństwa.

W obliczu uzyskanych wyników, dotychczasowe modele podnoszenia samooceny kompetencji cyfrowych oparte na teoretycznych ramach typu DigCompEdu, mogą wykazywać ograniczoną skuteczność w budowaniu realnej odporności cyfrowej. Należy jednak wyraźnie podkreślić, że zaprezentowane wyniki mają charakter deklaratywny i odzwierciedlają autodiagnozę respondentów, co niesie ryzyko błędu wynikającego z subiektywnej oceny własnych zdolności. Istnieje wysokie prawdopodobieństwo, że realne umiejętności techniczne są niższe, niż wynika to z deklaracji, co koresponduje ze zdiagnozowanym w najnowszych badaniach reprezentatywnych zjawiskiem „złudzenia kompetencji". Jak wykazano w polskiej edycji międzynarodowego projektu badawczego, aż 62,9% uczniów uzyskuje niskie wyniki w obiektywnych testach

© 2026 Author(s). CC BY 4.0

wiedzy o mechanizmach sieci (algorytmy, modele biznesowe), mimo ich wysokiej subiektywnej pewności (Tomczyk, 2026).

Dlatego kluczowym postulatem badawczym jest przejście od metod ankietowych do obiektywnych pomiarów opartych na zadaniach praktycznych. Tylko takie podejście pozwoli na precyzyjne zidentyfikowanie luk i stworzenie programów szkoleniowych, które zamiast replikować ogólną wiedzę, wyposażą nauczycieli i rodziców w autentyczną sprawczość cyfrową. Jest ona warunkiem koniecznym do pełnienia roli merytorycznych mentorów, zdolnych do wspierania dzieci w konfrontacji z nowymi, zautomatyzowanymi wektorami zagrożeń – od manipulacji algorytmicznych po treści syntetyczne generowane przez sztuczną inteligencję (Staksrud i in., 2026; UNICEF, 2026). Niniejszy artykuł, poprzez panoramiczne ujęcie samooceny obu grup, stanowi fundament pod nową dyskusję o konieczności integracji działań nauczycieli i rodziców/opiekunów w celu zapewnienia dzieciom bezpieczeństwa, które nie będzie jedynie teoretycznym postulatem, lecz praktyczną rzeczywistością.

Finansowanie: W ramach działań statutowych IBE PIB realizowanych przez Zespół Cyfryzacji Edukacji, stanowiących wsparcie dla Ministerstwa Edukacji Narodowej w obszarze cyfryzacji w oświacie.
Konflikt interesów: Brak.
Podziękowania: Dla Ministerstwa Edukacji Narodowej.
Informacja o dostępności danych: Dane są w posiadaniu IBE PIB.

REFERENCES

Akay, O. (2026). Children's privacy, autonomy, and digital identity in sharenting research: A scoping review with bibliometric mapping. *Frontiers in Psychology, 17,* Article 1845715. https://doi.org/10.3389/fpsyg.2026.1845715

Amzeyeva, A., Zhumabayeva, A., Kussainov, A., Zhunusbekova, A., Tynyskhanova, A., & Zhanadilova, K. (2026). Cybersecurity awareness and digital hygiene among pre-service primary school teachers: A case study of Kazakhstan. *International Journal of Information and Education Technology, 16*(1), 186–195.

AWO & NSPCC (2026). *Generative AI and child safety: What are the risks and how can we solve them?* https://learning.nspcc.org.uk/media/1drdecrn/gen-ai-research.pdf

Barker, J. (2019). The human nature of cybersecurity. *Educause Review, 54*(2). https://er.educause.edu/articles/2019/3/the-human-nature-of-cybersecurity

Burr, W. E. (1991). *Security in ISDN.* National Institute of Standards and Technology.

Cain, A. A., Edwards, M. E. & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42,* 36–45.

Cattaneo, A. A. P., Antonietti, C., & Rauseo, M. (2022). How digitalised are vocational teachers? Assessing digital competence in vocational education and looking at its underlying factors. *Computers & Education, 176,* 104364. https://doi.org/10.1016/j.compedu.2021.104364

Cicha, K., Rutecka, P., Rizun, M., & Strzelecki, A. (2021). Digital and media literacies in the Polish education system – Pre- and post-COVID-19 perspective. *Education Sciences, 11*(9), 532. https://doi.org/10.3390/educsci11090532

Common Sense Media. (2026). *AI risk assessment: Recommendation systems in social media*. Youth AI Safety Institute. https://institute.commonsensemedia.org/sites/default/files/ra-import/csm-ai-risk-assessment-recommendation-systems-in-social-media-01132026.pdf

Czepiec-Veltzé, K. (2025). Kompetencje cyfrowe i relacje z nowymi technologiami rodziców „zetek": Przyczynek do badań nad pokoleniem cyfrowej luki. *Annales Universitatis Paedagogicae Cracoviensis. Studia De Cultura, 17*(3), 7–29. https://doi.org/10.24917/20837275.17.3.1

Davis, J. (2019, 12 września). *Cyber canon book review: Click here to kill everybody: Security and survival in a hyper-connected world.* Palo Alto Networks. https://www.paloaltonetworks.com/blog/2019/09/cyber-canon-click-here-to-kill-everybody/

© 2026 Author(s). CC BY 4.0

Economou, A. (2023). *SELFIEforTEACHERS: Designing and developing a self-reflection tool for teachers' digital competence* (EUR 31475 EN). Publications Office of the European Union. https://doi.org/10.2760/01503

European Commission. (2025). *Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065 (Digital Services Act)*. https://digital-strategy.ec.europa.eu/en/library/guidelines-protection-minors-under-digital-services-act

Fraillon, J. (red.). (2024). *An international perspective on digital literacy: Results from ICILS 2023 (ICILS 2023 international report)*. International Association for the Evaluation of Educational Achievement (IEA). https://www.iea.nl/publications/study-reports/icils-2023-international-report

Fraillon, J., Ainley, J., Schulz, W., Friedman, T., & Gebhardt, E. (2014). *Preparing for life in a digital age: The IEA International Computer and Information Literacy Study international report*. Springer Nature.

Ghomi, M., & Redecker, C. (2019). Digital competence of educators (DigCompEdu): Development and evaluation of a self-assessment instrument for teachers' digital competence. *CSEDU 2019 – 11th International Conference on Computer Supported Education*, 541–548.

Global Public Policy Institute. (2015). *CSIRT basics for policy-makers: The history, types and culture of computer security incident response teams*. https://gppi.net/assets/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf

Hämäläinen, R., Nissinen, K., Mannonen, J., Lämsä, J., Leino, K., & Taajamo, M. (2021). Understanding teaching professionals' digital competence: What do PIAAC and TALIS reveal about technology-related skills, attitudes, and knowledge? *Computers in Human Behavior, 117,* Artykuł 106672. https://doi.org/10.1016/j.chb.2020.106672

Inamorato dos Santos, A., Chinkes, E., Carvalho, M. A. G., Solórzano, C. M. V., & Marroni, L. S. (2023). The digital competence of academics in higher education: Is the glass half empty or half full? *International Journal of Educational Technology in Higher Education, 20,* Artykuł 9. https://doi.org/10.1186/s41239-022-00376-0

Kreft, J. (2022). *Władza platform. Za fasadą Google, Facebooka i Spotify*. Wydawnictwo Uniwersytetu Jagiellońskiego.

Lange, R., Wrońska, A., Kamiński, K., Błażej, M., & Jankiewicz, A. (2023). *Nastolatki 3.0: Raport z ogólnopolskiego badania uczniów i rodziców*. NASK – Państwowy Instytut Badawczy.

Livingstone, S., & Haddon, L. (2009). *EU kids online: Final report 2009*. EU Kids Online / LSE. https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/Final-report.pdf

Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying online risk to children*. (CO:RE Short Report Series on Key Topics). Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI). https://doi.org/10.21241/ssoar.71817

Lorenzo-Seva, U., & ten Berge, J. M. F. (2006). Tucker's congruence coefficient as a meaningful index of factor similarity. *Methodology, 2*(2), 57–64.

McGarr, O. (2024). Exploring and reflecting on the influences that shape teacher professional digital competence frameworks. *Teachers and Teaching: Theory and Practice*. https://doi.org/10.1080/13540602.2024.2313641

Mitchell, C. J. (1990). *Management of secure systems and security within OSI*. University of London.

Negreiro, M. (2025). *Children and deepfakes: Evolution, spread and societal impact* (Briefing PE 775.855). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf

Nesterak, N., & Nesterak, J. (2023). Różnice w postrzeganiu nowoczesnych technologii cyfrowych w zróżnicowanych grupach wiekowych – wyniki autorskich badań. W: J. Nesterak & A. Wodecka-Hyjek (red.), *Aktualne trendy i wyzwania cyfrowe* (s. 28–46). Instytut Nauk Ekonomicznych PAN.

OECD. (2025a). *How's life for children in the digital age?* OECD Publishing. https://doi.org/10.1787/0854b900-en

© 2026 Author(s). CC BY 4.0

OECD. (2025b). *Preparing teachers for digital education: Continuing professional learning on digital skills and pedagogies* (OECD Education Policy Perspectives No. 122). OECD Publishing. https://doi.org/10.1787/af442d7a-en

Osborne, J. W. (2015). *Best practices in exploratory factor analysis*. CreateSpace.

Penszko, P. (2025). *Kompetencje cyfrowe uczniów w Polsce – co wiemy z badań międzynarodowych?* (Analizy IBE dla polityki publicznej, nr 3). Instytut Badań Edukacyjnych – Państwowy Instytut Badawczy. https://doi.org/10.24131/r20250710

Polski Instytut Ekonomiczny. (2021). *Cyfrowe wyzwania stojące przed polską edukacją*. https://pie.net.pl/wp-content/uploads/2021/02/PIE-62020_Cyfrowe_wyzwania-ostateczne-red..pdf

Ptaszek, G., Stunża, G. D., Pyżalski, J., Dębski, M., & Bigaj, M. (2020). *Edukacja zdalna: Co stało się z uczniami, ich rodzicami i nauczycielami?* Gdańskie Wydawnictwo Psychologiczne.

Pyżalski, J., Plichta, P., & Tomczyk, Ł. (2026). *Raport EU Kids Online 2026: Polscy uczniowie to „cyfrowi tubylcy" tylko z nazwy? Nowe dane obalają mity o internecie młodych*. Fundacja Orange / PAP. https://fundacja.orange.pl/app/uploads/2026/04/raport-eu-kids-online-2026.pdf

Rada Ministrów Rzeczypospolitej Polskiej. (2026). Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. *Monitor Polski*, 2026, poz. 309.

Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu*. Publications Office of the European Union. https://doi.org/10.2760/159770

Ricoy, M. C., Martínez, M. D., & Sánchez, J. (2022). Raising ecological awareness and digital literacy in primary school children through gamification. *International Journal of Environmental Research and Public Health, 19*(3), Artykuł 1149. https://doi.org/10.3390/ijerph19031149

Schneier, B. (2004). *Secrets and lies: Digital security in a networked world*. Wiley Publishing, Inc.

Spafford, E. H. (1988). *The Internet worm program: An analysis* (Technical Report CSD-TR-823). Purdue University e-Pubs. https://docs.lib.purdue.edu/cstech/70/

Staksrud, E., Mascheroni, G. i in. (2026). *European children's use and understanding of generative AI*. EU Kids Online V / London School of Economics and Political Science. https://researchonline.lse.ac.uk/id/eprint/137132/

Tomczyk, Ł. (2026). Samoocena umiejętności cyfrowych i wiedza o świecie online. W: J. Pyżalski, P. Plichta & Ł. Tomczyk, *Polskie badanie EU Kids Online 2026. W stronę nowych wyzwań. Reprezentatywne badanie polskich uczniów i uczennic w wieku 10–16 lat* (s. 39–54). Wydawnictwo Naukowe UAM. https://doi.org/10.14746/amup.9788323245308.3

Tomczyk, Ł., & Srokowski, Ł. (2016). *Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole. Raport z badań*. Stowarzyszenie „Miasta w Internecie".

UNICEF (2025). *Guidance on AI and children 3.0: Recommendations for policies and systems that uphold child rights*. https://www.unicef.org/innocenti/reports/policy-guidance-ai-children

UNICEF (2026, 22 stycznia). *Deepfake abuse is abuse: Statement by UNICEF on AI-generated sexualised images of children*. https://www.unicef.org/press-releases/deepfake-abuse-is-abuse

Vanden Abeele, M. M. P. (2021). Digital wellbeing as a dynamic construct. *Communication Theory, 31*(4), 932–955. https://doi.org/10.1093/ct/qtaa024

Vegas, E., & Winthrop, R. (2020, 8 września). *Beyond reopening schools: How education can emerge stronger than before COVID-19*. Brookings Institution. https://www.brookings.edu/articles/beyond-reopening-schools-how-education-can-emerge-stronger-than-before-covid-19/

© 2026 Author(s). CC BY 4.0

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The digital competence framework for citizens – with new examples of knowledge, skills and attitudes* (EUR 31006 EN). Publications Office of the European Union. https://doi.org/10.2760/115376

Waltzman, R. (2017). *The weaponization of information: The need for cognitive security*. RAND Corporation. https://www.rand.org/pubs/testimonies/CT468.html

Wiechetek, Ł., & Mędrek, M. (2022). Human factors in security – cybersecurity education and awareness of business students. *Annales Universitatis Mariae Curie-Skłodowska, sectio H – Oeconomia, 56*(1), 119–142. https://doi.org/10.17951/h.2022.56.1.119-142

Yildirim, E. i in. (2025). Shaping children's digital futures: The role of parenting strategies in regulating children's technology use. *Acta Psychologica, 252*, artykuł 104578. https://doi.org/10.1016/j.actpsy.2024.104578

Związek Cyfrowa Polska. (2024). *Raport Cyfrowa Szkoła 4.0*. https://cyfrowapolska.org/wp-content/uploads/2024/03/Raport_Cyfrowa_Szkola_4.pdf

© 2026 Author(s). CC BY 4.0