

SAMOOCENA KOMPETENCJI SPOŁECZEŃSTWA INFORMACYJNEGO WŚRÓD CYFROWYCH TUBYLCÓW

Paweł A. Nowak

Katedra Informatyki Ekonomicznej i Medycznej, UŁ
90-214 Łódź, Rewolucji 1905 r. 37/39
pawel.nowak@uni.lodz.pl

Abstract. *This paper analyzes self-assessments of information society competencies among digital natives, with a focus on first-year IT students. The study, based on a survey (N=187), reveals a gap between the declared technological proficiency and the actual information, critical, and communication skills. Although students feel confident in their abilities, they show weaknesses in cybersecurity and critical source verification. The findings suggest the need for educational solutions that would bridge the gap between the sense of proficiency and practical readiness, with a special emphasis on critical thinking and ethical reflection.*

1. Wprowadzenie

Cyfrowi tubylcy, rozumiani jako pokolenia wychowane w środowisku nasyconym technologią, skłonni są traktować własne sprawności cyfrowe jako oczywistość. Samo przekonanie o biegłości technologicznej nie musi jednak przekładać się na rzeczywiste kompetencje informacyjne, krytyczne i komunikacyjne. Pomimo powszechności technologii, obserwujemy bowiem rozbieżność między deklarowaną sprawnością a mierzalnymi umiejętnościami w obszarach takich jak wyszukiwanie, selekcja i weryfikacja informacji, rozumienie mechanizmów algorytmicznych, zarządzanie tożsamością i bezpieczeństwem w sieci, a także etyczne i odpowiedzialne korzystanie z treści. Ta dycho-
tomia staje się szczególnie wyraźna w środowisku akademickim, gdzie oczekuje się samodzielności badawczej, krytycznego myślenia oraz umiejętności współpracy w różnorodnych, wieloplatformowych ekosystemach.

Celem artykułu jest analiza samooceny kompetencji niezbędnych do funkcjonowania w społeczeństwie informacyjnym w specyficznej kohorcie cyfrowych tubylców: studentów pierwszego roku kierunków informatyka, informatyka ekonomiczna oraz bankowość i finanse cyfrowe (Uniwersytet Łódzki, Uniwersytet Dolnośląski DSW). Z pełną

świadomością ograniczeń i ryzyk związanych z pomiarem opartym na samoocenie, podjęto również próbę interpretacji uzyskanych wyników w perspektywie implikacji dydaktycznych dla „kierunków informatycznych” na polskich uczelniach.

W proponowanym ujęciu cyfrowi tubylcy to nie tylko osoby biegle posługujące się urządzeniami i aplikacjami, lecz także użytkownicy zanurzeni w kulturze cyfrowej, której normy i praktyki kształtują ich nawyki poznawcze, strategie uczenia się oraz sposoby wchodzenia w interakcje społeczne. W związku z tym artykuł koncentruje się na samoocenie kompetencji kluczowych dla efektywnego funkcjonowania w społeczeństwie informacyjnym, obejmując m.in. kompetencje informacyjne (np. formułowanie zapytań, ocena wiarygodności źródeł, rozumienie metadanych), kompetencje krytyczne (analiza stronniczości, rozpoznawanie dezinformacji, rozumienie kontekstu społecznego i ekonomicznego technologii) oraz kompetencje komunikacyjne (netykieta, współpraca zdalna, prezentacja i wizualizacja danych). Badana kohorta obejmuje studentów pierwszego roku na kierunkach informatyka, informatyka ekonomiczna oraz bankowość i finanse cyfrowe (N=187) z dwóch publicznych uczelni, czyli grupę, po której można oczekiwać stosunkowo wysokiego poziomu biegłości technicznej, ale niekoniecznie wykształconych kompetencji przekrojowych, które warunkują odpowiedzialne i świadome korzystanie z narzędzi cyfrowych w praktyce akademickiej i zawodowej. Dodatkowym celem jest zaproponowanie, choćby jako przyczynek do dyskusji, takich rozwiązań dydaktycznych, które pomogą zredukować lukę między „poczuciem biegłości” a rzeczywistą gotowością do pracy w złożonym, szybko zmieniającym się ekosystemie informacyjnym.

2. Tło teoretyczne i przegląd literatury

Rozumienie społeczeństwa informacyjnego obejmuje zarówno wymiar technologiczny, jak i instytucjonalny oraz kulturowy. Oznacza to nie tylko dyfuzję infrastruktury sieciowej i narzędzi cyfrowych, lecz także przemiany modeli organizacyjnych, form regulacji, norm komunikacyjnych i praktyk codziennych, które współkształtują te technologie. Castells wskazywał, że „sieciowa logika” staje się strukturyzującą zasadą nowoczesnych społeczeństw, determinując przepływy informacji, kapitału i władzy, a także rekonfigurując relacje między jednostkami, rynkami i państwem [3].

W tej perspektywie kluczowe staje się analizowanie architektury platform, protokołów komunikacyjnych oraz algorytmicznych mechanizmów selekcji treści, które kształtują widoczność informacji i wpływają na dynamikę życia publicznego. Jednocześnie dostęp do technologii nie jest tożsamy z kompetentnym uczestnictwem – literaturę w tym zakresie organizuje koncepcja podziałów cyfrowych kolejnych rzędów [5], która akcentuje znaczenie umiejętności, praktyk i kapitałów cyfrowych. O ile pierwszy rząd dotyczy fizycznego dostępu do infrastruktury, o tyle drugi obejmuje różnice w umiejętnościach wyszukiwania, oceny i krytycznej interpretacji informacji, a trzeci – zdolność

przekuwania aktywności online w realne zasoby społeczne i ekonomiczne. Ujęcie to uzupełniają badania nad nierównościami w zakresie motywacji, wsparcia społecznego, kompetencji metapoznawczych oraz różnic kulturowych, które warunkują sposoby korzystania z mediów cyfrowych. W konsekwencji, polityki publiczne i strategie edukacyjne wymagają projektowania interwencji nie tylko infrastrukturalnych, lecz także rozwojowych i włączających, uwzględniających kontekst społeczny użytkowników.

W obszarze edukacji informatycznej rośnie znaczenie myślenia komputacyjnego jako „uniwersalnej kompetencji rozwiązywania problemów” [7], obejmującej dekompozycję, abstrakcję, rozpoznawanie wzorców oraz projektowanie algorytmów. Rozszerzając się zastosowania tych kompetencji – od nauk przyrodniczych po humanistykę cyfrową – łączą się z potrzebą rozwijania umiejętności programistycznych, pracy z danymi oraz współpracy człowiek–maszyna. Równolegle wskazuje się na krytyczną potrzebę kształcenia w zakresie selekcji informacji i bezpieczeństwa, w tym zarządzania tożsamością cyfrową, ochrony prywatności, higieny haseł, rozumienia polityk platform oraz rozpoznawania manipulacji informacyjnych i wzorców inżynierii społecznej [2][1]. Tak rozumiane kompetencje cyfrowe powinny być rozwijane spiralnie – od edukacji wczesnoszkolnej po kształcenie ustawiczne – i osadzone w praktycznych kontekstach życia obywatelskiego oraz zawodowego.

Z perspektywy literatury o dezinformacji i przeciążeniu informacyjnym uznaje się, że natłok treści i niepewność co do ich wiarygodności obniżają trafność decyzji i zaufanie społeczne [1]. Mechanizmy te dodatkowo wzmacniają algorytmiczne filtry, brak umiejętności koncentracji uwagi oraz podatność na wiralowe treści, co sprzyja wzmocnieniu emocjonalnych przekazów kosztem rzetelności. Skutkiem tych zjawisk jest polaryzacja opinii, efekt echa oraz erozja konsensusu poznawczego.

Wreszcie, obszar etyki technologii zwraca uwagę na napięcia między innowacyjnością społeczeństwa informacyjnego a ochroną praw i wolności, proponując podejścia typu *ethics-by-design* [4]. Ramy te obejmują m.in. zasady sprawiedliwości, przejrzystości, odpowiedzialności i minimalizacji szkód, które powinny przenikać cały cykl życia systemów – od definicji problemu, przez pozyskiwanie danych i trenowanie modeli, po wdrożenie i ewaluację skutków społecznych. W praktyce oznacza to konieczność interdyscyplinarnej współpracy, audytowalności algorytmów, dokumentowania decyzji projektowych oraz mechanizmów odwoławczych dla użytkowników, a także budowania kultury organizacyjnej sprzyjającej refleksyjności i odpowiedzialności społecznej.

3. Cele badania i pytania badawcze

Celem głównym jest uchwycenie profilu samoocenianych kompetencji studentów I roku kierunków informatycznych oraz identyfikacja dominujących sposobów rozumienia społeczeństwa informacyjnego. Cele szczegółowe:

- opis intensywności i modelu korzystania z ICT;

- diagnoza rozumienia pojęcia „społeczeństwo informacyjne” i jego cech;
- hierarchizacja postrzeganych „kompetencji kluczowych” dla funkcjonowania cyfrowego;
- samoocena w wybranych domenach (użytkowe, informacyjne, bezpieczeństwo);
- identyfikacja postrzeganych barier i problemów;
- ocena postaw wobec etycznego ograniczania technologii.

Na tej podstawie sformułowano następujące pytania badawcze: (P1) Jaki jest rozkład intensywności wykorzystania urządzeń dostępowych w badanej grupie? (P2) Jak studenci konceptualizują społeczeństwo informacyjne? (P3) Które kompetencje uznają za kluczowe? (P4) W jakich obszarach ich samoocena jest najwyższa, a w jakich najniższa? (P5) Jakie bariery i zagrożenia wskazują? (P6) Jak kształtują się postawy wobec regulacji etycznych technologii?

4. Metodologia

Próba: N=187 studentów pierwszego roku trzech kierunków: informatyka, informatyka ekonomiczna, bankowość i finanse cyfrowe (Uniwersytet Łódzki, Uniwersytet Dołężycki DSW).

Procedura: badanie ankietowe z użyciem ustrukturyzowanego arkusza samooceny online, realizowane w warunkach zajęć wprowadzających.

Narzędzia i wymiary:

- Intensywność i model korzystania z ICT (częstotliwość, urządzenie dominujące);
- Rozumienie społeczeństwa informacyjnego (pytania zamknięte jednokrotnego wyboru i wielokrotnego wyboru);
- Hierarchia „kompetencji kluczowych” (lista wielokrotna);
- Skale samooceny (1–5) dla: obsługa urządzeń, wyszukiwanie informacji, selekcja/weryfikacja, korzystanie z usług cyfrowych, oprogramowanie biurowe, cyberbezpieczeństwo;
- Bariery dostępu i korzystania (wielokrotny wybór);
- Postawy wobec etycznych ograniczeń technologii (skala Likerta 1–5).

Analiza danych: statystyki opisowe (procenty, średnie, odchylenia standardowe), interpretacja w świetle literatury przedmiotu.

Ograniczenia: charakter samooceny, brak weryfikacji testami kontrolnymi, możliwa stronniczość społecznej aprobaty, specyfika kierunków informatycznych ograniczająca możliwość uogólnień.

5. Wyniki i interpretacja

1) Intensywność i niejednorodność użytkowania ICT

95,2% badanych korzysta z Internetu kilka razy dziennie. Samooceńa codziennego użycia ICT: wysoka 64,2%, średnia 29,4%, niska/minimalna 6,4%.

Interpretacja: Dominuje profil „heavy users”, ale obecny jest „ogon” o niskiej intensywności, co sugeruje zróżnicowane kapitały cyfrowe na starcie oraz odmienne doświadczenia szkolne/rodzinne. W praktyce oznacza to, że część studentów posiada zaawansowane nawyki i płynność w korzystaniu z technologii (w tym złożone strategie wyszukiwania, zarządzania informacją i współpracy online), podczas gdy inna grupa dopiero rozwija podstawowe umiejętności operacyjne, ma ograniczone doświadczenia projektowe oraz niższy poziom świadomości ryzyka i higieny cyfrowej. Różnice te mogą wynikać z wcześniejszego dostępu do infrastruktury, jakości wsparcia nauczycielskiego i rodzinnego, a także z kapitału kulturowego oraz motywacji do samodzielnego uczenia się.

2) Smartfonocentryczność jako główny model dostępu

Urządzenie dominujące: smartfon 73,3%, komputer stacjonarny 19,3%, laptop 4,8%.

Interpretacja: Nawet wśród studentów informatyki podstawowym terminalem jest smartfon, co sprzyja krótszym formom, konsumpcji treści i wielozadaniowości, a osłabia praktyki produkcyjne (praca na plikach, konfiguracja środowisk). Jednocześnie wskazuje to na preferencję do aplikacji o niskim progu wejścia, interfejsów dotykowych i usług chmurowych, które ułatwiają szybkie interakcje, ale ograniczają głęboką pracę twórczą oraz rozwój nawyków związanych z kontrolą wersji, automatyzacją i architekturą oprogramowania. W efekcie rośnie rozbieżność między kompetencjami konsumenckimi (szybka nawigacja, wyszukiwanie, mikrozadania) a kompetencjami inżynierskimi (planowanie pracy, strukturyzacja projektów, narzędzia linii komendy).

3) Rozumienie społeczeństwa informacyjnego: przewaga podejścia systemowego

Definicje (wybór jednej): 43,9% – integracja kluczowych procesów (edukacja, administracja, praca) z ICT; 24,1% – kluczowe znaczenie ICT i szybkiego dostępu do danych dla jakości życia; 16,6% – wpływ dostępu do informacji/usług online na decyzje i załatwianie spraw; 12,8% – duży wpływ ICT, ale nie definiuje całego społeczeństwa; 2,7% – brak wyraźnego związku.

Interpretacja: Większość przyjmuje perspektywę instytucjonalno-procesową („makro”), lecz istotna mniejszość redukuje SI do poziomu usługowego. Rozkład tych postaw sugeruje, że w dominującym ujęciu SI postrzegana jest jako ekosystem wpływający na

reguły działania organizacji, strukturę władzy i przepływy informacji, podczas gdy mniejszość koncentruje się głównie na zastosowaniach narzędziowych i wdrożeniach punktowych. Różnica ta przekłada się na odmienne oczekiwania wobec kompetencji: perspektywa makro akcentuje rozumienie kontekstu regulacyjnego, etycznego i społecznego, a ujęcie usługowe – biegłość operacyjną i integracyjną.

4) Cechy społeczeństwa informacyjnego: dominacja ujęć technologiczno-funkcjonalnych

Najczęstsze wskazania: „Internet do nauki/pracy/zabawy/komunikacji” – 159; „powszechny dostęp do Internetu” – 151; „Internet jako podstawowe źródło informacji” – 143; „większość spraw/usług da się załatwić online” – 131.

Rzadziej: „Internet ogranicza wykluczenie edukacyjne i kulturalne” – 60; „...wykluczenie społeczne osób z niepełnosprawnościami” – 31.

Interpretacja: Perspektywa inkluzji/wykluczenia jest słabiej obecna, co uzasadnia systematyczne włączanie wątku dostępności (accessible-by-design) i digital inclusion do dydaktyki (HCI/UX, inżynieria oprogramowania, etyka/prawo IT). W praktyce oznacza to konieczność projektowania programów nauczania, które od początku uwzględniają różnorodność użytkowników, bariery technologiczne oraz kontekst społeczny korzystania z systemów cyfrowych.

5) Hierarchia kompetencji: priorytet dla sprawności operacyjno-informacyjnych

Najczęściej: obsługa urządzeń – 171; wyszukiwanie informacji – 169; selekcja i weryfikacja – 152; zasady cyberbezpieczeństwa – 141; korzystanie z usług cyfrowych – 121.

Najrzadziej: oprogramowanie biurowe – 58; programowanie – 39.

Interpretacja: „Kompetencje dla SI” są postrzegane jako powszechne (digital i information literacy), a nie „twórcze” w sensie wytwarzania technologii. Implikacja: łączenie programowania z kontekstem społecznym (sprawczość w automatyzacji, analizie danych, weryfikacji informacji, narzędzia dostępnościowe), aby przełamać wrażenie czysto zawodowego charakteru tej kompetencji.

Rozwinięcie: W dominującym odbiorze kompetencje związane z SI są traktowane jako fundamentarne umiejętności użytkowe — podobne do umiejętności obsługi narzędzi biurowych czy wyszukiwarek — a nie jako przestrzeń twórczej ekspresji, innowacji czy projektowania nowych rozwiązań technologicznych. Taki obraz wzmacnia narracja edukacyjna skupiona na bezpiecznym i efektywnym korzystaniu z narzędzi cyfrowych, a nie na ich krytycznym współtworzeniu.

6) Samooocena kompetencji: silne użytkowe, słabsze bezpieczeństwo i weryfikacja

Średnie (1–5): obsługa urządzeń M=4,23; wyszukiwanie informacji M=4,21; korzystanie z usług cyfrowych M=4,12; oprogramowanie biurowe M=3,88; selekcja i weryfikacja informacji M=3,90; cyberbezpieczeństwo M=3,67.

Interpretacja: Profil typowy dla intensywnych użytkowników – bardzo wysoka sprawność operacyjna i nawigacyjna (szybkie wykonywanie zadań, skuteczne poruszanie się między aplikacjami i usługami, biegłość w konfiguracji ustawień oraz rozwiązywaniu prostych problemów), przy jednocześnie niższej pewności w obszarach wymagających pogłębionej wiedzy proceduralnej, krytycznego myślenia i refleksji (m.in. rozumienie konsekwencji działań, ocena ryzyka, interpretacja polityk prywatności, rozpoznawanie manipulacji, a także właściwe dokumentowanie i utrwalanie procesów).

7) Postrzegane problemy SI: kryzys zaufania, nadmiar informacji, prywatność

Najczęściej: infodemia/nadmiar informacji – 150; prywatność i bezpieczeństwo danych – 147; brak zaufania do źródeł online – 145.

Dalej: niskie kompetencje cyfrowe w otoczeniu – 105; ograniczenia prawne/administracyjne – 89.

Rzadziej: brak szerokopasmowego Internetu/wysokie koszty – 64; brak urządzeń – 48.

Interpretacja: W percepcji studentów dominują bariery jakościowe („post-access divide”), obejmujące m.in. trudności w krytycznej ocenie źródeł, rozumieniu kontekstu informacji, rozpoznawaniu dezinformacji oraz w stosowaniu odpowiednich praktyk bezpieczeństwa cyfrowego. Dostęp techniczny jest w dużej mierze zapewniony, jednak to kompetencje związane z jakością korzystania z informacji decydują o skuteczności i bezpieczeństwie działań w środowisku cyfrowym.

8) Postawy wobec etycznych ograniczeń technologii: umiarkowanie pro-etyczne

Rozkład (1–5): 1: 23; 2: 24; 3: 46; 4: 63; 5: 31.

Interpretacja: Przewaga akceptacji ograniczeń (AI, rozpoznawanie twarzy, profilowanie), lecz obecna ambiwalencja. Jednocześnie widoczna jest potrzeba doprecyzowania granic odpowiedzialności oraz transparentności mechanizmów decyzyjnych, zwłaszcza w kontekstach wysokiego ryzyka i asymetrii władzy informacyjnej. Rosnące oczekiwania wobec zgodności z regulacjami (np. RODO, nadchodzące ramy AI) współlistnieją z presją innowacyjną i efektywnościową, co potęguje dysonans między deklaracjami a praktykami wdrożeniowymi.

6. Dyskusja i wnioski

Analiza uzyskanych wyników potwierdza obraz studentów informatyki jako intensywnych użytkowników o profilu smartfonocentrycznym, ale jednocześnie niejednorodnych pod względem praktyk i nawyków cyfrowych. Zgodnie z ujęciem podziałów cyfrowych drugiego i trzeciego rzędu [6], różnice nie sprowadzają się już do dostępu, lecz do sposobów korzystania i efektów użytkowania. Słabsza samoocena w cyberbezpieczeństwie i w krytycznej weryfikacji informacji koresponduje z wnioskami z badań nad kompetencjami informacyjnymi i medialnymi, które akcentują trudności w ocenie źródeł i odporności na dezinformację [2][1], a jednocześnie wzmacnia tezy przedstawione we Wprowadzeniu dotyczące rozwarstwienia kompetencji cyfrowych wśród młodych dorosłych oraz luki między zaawansowaną biegłością techniczną a kompetencjami krytycznymi i bezpieczeństwa.

Interesujące jest relatywne „zdeprecjonowanie” programowania jako kompetencji społeczeństwa informacyjnego. W świetle ujęcia myślenia komputacyjnego jako meta-umiejętności [7], może to świadczyć o rozbieżności pomiędzy rolami użytkownika i twórcy technologii, ale też wskazuje na potrzebę silniejszego osadzenia nauki programowania w kontekstach sprawczości społecznej (automatyzacja, dane obywatelskie, transparentność algorytmów). Z kolei makroinstytucyjne rozumienie społeczeństwa informacyjnego, obecne u większości badanych, harmonizuje z klasycznymi ujęciami [3], choć marginalizacja perspektywy włączającej sygnalizuje potrzebę dydaktycznego wzmacniania wątków równości i projektowania uniwersalnego.

Implikacje dydaktyczne

- Diagnostyka startowa i adaptacyjne ścieżki dydaktyczne na I roku (zwłaszcza w bezpieczeństwie i weryfikacji informacji).
- Projektowanie zadań „produkcyjnych” i procesowych: praca w repozytoriach, dokumentacja techniczna, analiza danych, konfiguracja środowisk, praktyki DevSecOps w wersji edukacyjnej.
- Włączenie modułów o społecznych konsekwencjach informatyki: datafikacja, platformizacja, algorytmiczne procesy decyzyjne, ekonomia danych, regulacje.
- Systematyczne kształcenie w zakresie cyberbezpieczeństwa użytkownika, prywatności i higieny cyfrowej, w tym uwierzytelniania wieloskładnikowego i podstaw modeli zagrożeń.
- Kształcenie wrażliwości inkluzywnej: accessible-by-design, standardy WCAG, projektowanie dla różnorodności zdolności i kontekstów użycia.
- Łączenie programowania z kontekstami społecznej sprawczości i odpowiedzialności (case studies, projekty service learning, audyty algorytmiczne).

Ograniczenia i kierunki dalszych badań

- Samooocena może przeszacowywać lub niedoszacowywać realne umiejętności.
- Analizy podgrup (płeć, doświadczenia edukacyjne, status społeczno-ekonomiczny) wymagają większych próbek, aby wiarygodnie oszacować różnice efektów.
- Warto rozwinąć wskaźniki „post-access divide” i zoperacjonalizować kompetencje krytyczne (np. scenariusze phishingu, zadania fact-checkingowe).

Podsumowując, badana grupa cyfrowych tubylców wchodzących na kierunki informatyczne cechuje się nie tylko wysoką intensywnością korzystania z Internetu i dominacją smartfonów jako podstawowych terminali dostępu do usług i treści, lecz także wyraźnie ukształtowanym, systemowym – choć w istotnym stopniu nadal usługowym – rozumieniem społeczeństwa informacyjnego, w którym technologie postrzegane są głównie jako narzędzia efektywności, komunikacji i rozrywki.

W obrębie samooceny kompetencji ujawnia się hierarchia umiejętności, w której na czoło wysuwają się sprawności operacyjne (sprawne posługiwanie się aplikacjami, konfiguracją urządzeń, automatyzacją prostych zadań) oraz informacyjne (wyszukiwanie, selekcja, organizacja i podstawowa kategoryzacja zasobów), podczas gdy elementy wymagające głębszej refleksji i praktyk metodycznych – takie jak projektowanie rozwiązań, dokumentowanie procesów czy systematyczna walidacja źródeł – są rzadziej artykułowane i słabiej utrwalone. Relatywnie najsłabiej oceniane pozostają domeny cyberbezpieczeństwa (świadomość zagrożeń, zarządzanie tożsamością i uprawnieniami, higiena haseł, praktyki szyfrowania, rozumienie modelu zagrożeń) oraz krytycznej weryfikacji informacji (analiza wiarygodności źródeł, rozpoznawanie manipulacji, praca z dowodami i metodologią), co wskazuje na lukę między kompetencjami użytkowymi a refleksyjnymi i normatywnymi.

W obszarze postaw przeważa umiarkowana akceptacja dla etycznych ograniczeń technologii: studenci deklarują poparcie dla zasad prywatności, przejrzystości algorytmicznej i odpowiedzialnego wykorzystania danych, lecz jednocześnie wykazują skłonność do kompromisów w sytuacjach, w których ograniczenia te kolidują z wygodą, szybkością działania lub krótkoterminowymi korzyściami.

Z perspektywy dydaktyki I roku kierunków informatycznych zasadne jest zatem równoległe i systematyczne wzmacnianie trzech osi rozwoju: bezpieczeństwa (praktyczne ćwiczenia z modelowania zagrożeń, konfiguracji zabezpieczeń, reagowania na incydenty), krytycznej pracy z informacją (metody oceny jakości źródeł, replikowalność, ścieżki dowodowe, podstawy myślenia statystycznego i probabilistycznego) oraz refleksji etyczno-społecznej (analiza skutków ubocznych technologii, odpowiedzialność projektantów, równość dostępu, zgodność z regulacjami), przy jednoczesnym adresowaniu

zróżnicowania przygotowania startowego poprzez elastyczne ścieżki kształcenia, diagnostykę wejściową, tutoring oraz zadania o rosnącej złożoności, które pozwolą na wyrównywanie braków bez hamowania postępów bardziej zaawansowanych studentów. Warto równocześnie rozważyć, czy o brakujące kompetencje – zwłaszcza w obszarach cyberbezpieczeństwa, krytycznej weryfikacji informacji i refleksji etycznej – nie należy zabiegać już na wcześniejszych etapach edukacji (np. w szkołach średnich), a także czy nie powinny one mieć charakteru powszechnego, wykraczającego poza profil przyszłych „informatyków” i obejmującego szerokie grono uczniów oraz użytkowników technologii

Literatura

1. Bawden, D., & Robinson, L. (2009). *The dark side of information: Overload, anxiety and other paradoxes and pathologies*. Journal of Information Science, 35(2)/2009. DOI: 10.1177/0165551508095781.
2. Bulger, M., & Davison, P. *The Promises, Challenges, and Futures of Media Literacy*. Psychology of Popular Media Culture, 7(2)/2018.
3. Castells, M. *The Rise of the Network Society (2nd ed.)*. Wiley-Blackwell 2010.
4. Floridi, L. & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review. DOI: 10.1162/99608f92.8cd550d1.
5. Hargittai, E. *Second-level digital divide: Differences in people's online skills*. First Monday, 7(4)/2002. DOI: 10.5210/fm.v7i4.942.
6. van Deursen, A. J. A. M., & van Dijk, J. A. G. M. *The digital divide shifts to differences in usage*. Telecommunications Policy, 38(1)/2014.
7. Wing, J. M. *Computational thinking*. Communications of the ACM, 49(3)/2006.