

Sławomir Krzysztof Czubaj¹

Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103304_2

ROLA SZTUCZNEJ INTELIGENCJI W KSZTAŁTOWANIU BEZPIECZEŃSTWA INFORMACYJNEGO INTERNETU JAKO MEDIUM WSPÓŁCZESNEJ CYWILIZACJI

THE ROLE OF ARTIFICIAL INTELLIGENCE IN SHAPING INFORMATION SECURITY ON THE INTERNET AS A MEDIUM OF MODERN CIVILISATION

Streszczenie

Celem pracy jest analiza wpływu sztucznej inteligencji na bezpieczeństwo informacyjne Internetu jako kluczowego medium współczesnej cywilizacji. Rozdział bada transformację Internetu z tradycyjnej infrastruktury komunikacyjnej w złożone środowisko algorytmiczne, w którym systemy generatywne, rekomendacyjne i agentowe aktywnie współuczestniczą w procesach poznawczych, komunikacyjnych i decyzyjnych użytkowników. Przedmiotem analizy są korzyści, zagrożenia oraz wyzwania regulacyjne wynikające z dynamicznego rozwoju technologii AI. W pracy zastosowano metodę przeglądu literatury naukowej i raportów instytucjonalnych z lat 2023-2025, w tym publikacji OECD, UNESCO, Stanford Institute for Human-Centered Artificial Intelligence, Europolu,

¹ <https://orcid.org/0000-0002-7561-2277>, e-mail: s.czubaj@dyd.akademiabialska.pl

DataReportal, Nature Machine Intelligence oraz ACM. Dokonano krytycznej analizy najważniejszych modeli generatywnych i systemów algorytmicznych wpływających na środowisko informacyjne, obejmującej zarówno aspekty technologiczne, jak i społeczne. Uwzględniono również aktualne ramy regulacyjne, takie jak Artificial Intelligence Act UE czy amerykańskie Executive Orders. Analiza ma charakter jakościowy i opiera się na metodzie studiów przypadków (case-based review) oraz analizie porównawczej aktualnych podejść regulacyjnych. Przeprowadzona analiza wykazała, że sztuczna inteligencja stała się jednym z kluczowych mechanizmów współczesnego Internetu, wpływając na sposób organizacji i kontroli informacji. Modele generatywne i systemy rekomendacyjne zwiększają efektywność dostępu do wiedzy, lecz jednocześnie wzmacniają zagrożenia informacyjne, takie jak dezinformacja generatywna, manipulacja poznawcza, nieprzejrzystość algorytmów oraz erozja autonomii poznawczej użytkowników. Stwierdzono również rosnące znaczenie systemów agentowych i „Internetu agentów”, które radykalnie zmieniają strukturę uczestników ekosystemu informacyjnego. Ponadto odnotowano znaczące różnice w tempie i zakresie wdrażania regulacji AI między regionami świata. Sztuczna inteligencja redefiniuje Internet jako środowisko informacyjne, przekształcając go w układ kognitywno-algorytmiczny współtworzony przez ludzi i systemy autonomiczne. Odpowiedzialne wykorzystanie AI wymaga wzmocnienia infrastruktury regulacyjnej, wprowadzenia mechanizmów audytu algorytmicznego, budowania odporności cyfrowej społeczeństwa oraz rozwijania kompetencji krytycznych użytkowników. Internet przyszłości będzie środowiskiem współpracy człowieka i inteligentnych systemów, jednak warunkiem zachowania zaufania społecznego i integralności informacyjnej jest transparentne, etyczne i kontrolowane wdrażanie technologii AI.

Słowa kluczowe: sztuczna inteligencja, bezpieczeństwo informacyjne, Internet, dezinformacja, generatywna AI, algorytmizacja, Internet agentów, odporność cyfrowa

Abstract

The aim of this study is to examine the influence of artificial intelligence on the information security of the Internet as a key medium of contemporary civilisation. The article investigates the transformation of the Internet from a traditional communication infrastructure into a complex algorithmic environment in which generative, recommender, and agent-based systems actively participate in users' cognitive, communicative, and decision-making processes. The study focuses on the benefits, risks, and regulatory challenges arising from the rapid development of AI technologies. The study applies a qualitative literature review of scientific publications and institutional reports from 2023-2025, including sources from OECD, UNESCO, Stanford Institute for Human-Centered Artificial Intelligence, Europol, DataReportal, Europol, DataReportal, Nature Machine Intelligence, and ACM.

A critical analysis of the main generative models and algorithmic systems shaping the contemporary information environment was conducted, encompassing technological, social, and epistemic perspectives. Current regulatory frameworks – such as the EU Artificial Intelligence Act and U.S. Executive Orders – were examined using comparative policy analysis. Additionally, selected case studies were used to identify emerging risks and societal impacts of algorithmic systems. The findings indicate that artificial intelligence has become a central mechanism of the modern Internet, reshaping how information is organised, interpreted, and distributed. Generative models and recommendation systems enhance access to knowledge but simultaneously amplify information security threats, including generative disinformation, cognitive manipulation, algorithmic opacity, and the erosion of users' cognitive autonomy. The analysis also reveals the growing importance of agent-based systems and the emerging “agentic Internet,” which fundamentally alters the structure of participants in the digital ecosystem. Significant regional disparities were identified in the development and enforcement of AI regulations. Artificial intelligence is redefining the Internet as an information environment, transforming it into a cognitive-algorithmic system co-constructed by humans and autonomous technologies. Ensuring responsible AI adoption requires strengthening regulatory infrastructures, implementing algorithmic audit mechanisms, fostering digital resilience, and developing users' critical competencies. The future Internet will increasingly rely on collaboration between humans and intelligent systems; however, maintaining public trust and safeguarding information integrity will depend on transparent, ethical, and accountable AI governance.

Keywords: artificial intelligence, information security, Internet, disinformation, generative AI, algorithmization, agentic Internet, digital resilience

Wstęp

Internet stanowi fundament współczesnego świata, będąc zarówno podstawowym kanałem dystrybucji informacji, jak i narzędziem pracy, edukacji, kultury oraz komunikacji społecznej. Według najnowszych danych Digital Poland 2025 ponad 88% mieszkańców Polski korzysta z Internetu, spędzając średnio ponad sześć godzin dziennie w przestrzeni cyfrowej, w tym ponad dwie godziny w mediach społecznościowych (DataReportal, 2025b). Skala uczestnictwa cyfrowego potwierdzona jest także w danych globalnych, które wskazują na systematyczny wzrost intensywności korzystania z Internetu w ujęciu międzynarodowym (DataReportal, 2025a). Internet staje się zatem nie tylko narzędziem, ale kluczowym

medium funkcjonowania człowieka XXI wieku oraz obszarem o znaczeniu strategicznym dla bezpieczeństwa informacyjnego.

W ostatnich latach obserwujemy jednak fundamentalną transformację tego środowiska. Internet przestaje być wyłącznie przestrzenią treści tworzonych i zarządzanych przez ludzi – coraz większą rolę pełni w nim sztuczna inteligencja, która staje się aktywnym uczestnikiem procesów obiegu informacji. Zmianę tę wzmacniają także trendy technologiczne wskazywane w raportach globalnych, takich jak Ericsson Mobility Report (Ericsson, 2024b), które podkreślają rosnącą integrację systemów komunikacji, danych i sztucznej inteligencji. Współczesne systemy AI:

- generują i przetwarzają treści,
- filtrują i moderują informacje,
- rekomendują zasoby i kształtują ekspozycję informacyjną użytkowników,
- analizują i przewidują zachowania odbiorców,
- automatyzują komunikację i inicjują interakcje,
- współuczestniczą w procesach poznawczych, decyzyjnych i komunikacyjnych.

Modele generatywne, takie jak GPT, Claude, Gemini czy Llama, a także multimodalne systemy obrazu i wideo (DALL-E, Stable Diffusion, Sora) wpływają nie tylko na strukturę Internetu jako zasobu, lecz przede wszystkim na integralność i wiarygodność informacji. Wraz z pojawieniem się autonomicznych architektur agentowych rośnie także znaczenie koncepcji Internetu agentów i Internetu zmysłów (6G + AI), w których systemy sztucznej inteligencji przejmują część funkcji tradycyjnych procesów komunikacji i przetwarzania danych (Sehad i in., 2024).

Równocześnie intensyfikują się wyzwania związane z bezpieczeństwem informacyjnym: manipulacja treściami, dezinformacja generatywna, automatyzacja propagandy, naruszenia prywatności, filtracja algorytmiczna czy ryzyka wynikające z nierównowagi informacyjnej. Rozwija się również zjawisko uzależnienia od systemów algorytmicznych i ograniczania autonomii poznawczej użytkowników.

Rozdział podejmuje analizę tych procesów oraz ich konsekwencji dla funkcjonowania Internetu jako złożonego, inteligentnego medium współczesnej cywilizacji, ze szczególnym uwzględnieniem roli sztucznej inteligencji w kształtowaniu bezpieczeństwa informacyjnego i integralności przestrzeni cyfrowej.

Czym jest Internet we współczesnej cywilizacji

Internet należy do kluczowych osiągnięć cywilizacji informacyjnej i stanowi fundamentalną infrastrukturę społeczeństwa wiedzy. Od momentu powstania pełni funkcję globalnego medium komunikacyjnego, umożliwiającego transfer informacji, wymianę danych, rozwój nauki, gospodarki i kultury oraz kształtowanie relacji społecznych. Jego istota wykracza jednak poza rolę kanału komunikacyjnego – Internet stał się środowiskiem życia społecznego, ekonomicznego i edukacyjnego, a obecnie, za sprawą sztucznej inteligencji, również obszarem o kluczowym znaczeniu dla bezpieczeństwa informacyjnego.

Zgodnie z najnowszymi danymi dotyczącymi użytkowania Internetu, w Polsce 88,4% mieszkańców korzysta z sieci, a średni dzienny czas aktywności online wynosi ponad 6 godzin (DataReportal, 2025b). Globalne raporty potwierdzają systematyczny wzrost intensywności uczestnictwa cyfrowego oraz rosnącą zależność społeczeństw i gospodarek od infrastruktury internetowej (DataReportal, 2025a). Jednocześnie analizy *Ericsson Mobility Report* wskazują, że zwiększa się zapotrzebowanie na transmisję danych oraz integrację systemów sieciowych z technologiami sztucznej inteligencji, co wpływa na odporność i stabilność cyfrowego ekosystemu informacyjnego (Ericsson, 2024b; Ericsson, 2024a).

Wraz z rozwojem technologii informacyjnych Internet przekształcił się z pasywnego repozytorium danych w środowisko interaktywne, a następnie – dzięki dynamicznie rozwijającym się modelom AI – w przestrzeń współtworzoną przez systemy inteligentne. Zjawisko to jest szeroko opisywane we współczesnych pracach poświęconych cyfryzacji i społeczeństwu sieci, które wskazują na przejście od Internetu komunikacyjnego do Internetu algorytmicznego, w którym przetwarzanie danych staje się integralnym elementem struktury społecznej (van Dijck i in., 2025; Perriam, Carter, 2022). W literaturze opisuje się współczesny Internet jako układ hybrydowy, w którym współdziałają:

- użytkownicy,
- instytucje i organizacje,
- infrastruktura sieciowa i obliczeniowa,
- algorytmy decyzyjne,
- systemy generatywne i agentowe.

Takie ujęcie jest zgodne z koncepcjami nowoczesnych społeczeństw cyfrowych, które wskazują na coraz bardziej współzależny charakter relacji między człowiekiem a infrastrukturą technologiczną (Camarinha-Matos i in., 2022). Jednocześnie rozwój narzędzi sztucznej inteligencji wywołuje redefinicję klasycznego modelu komunikacji – algorytmy zaczynają pełnić funkcję współuczestników procesów informacyjnych, a nie tylko narzędzi przesyłu treści.

Trend ten znajduje potwierdzenie w globalnych raportach dotyczących SI, które opisują gwałtowne zwiększenie roli modeli generatywnych, systemów rekomendacyjnych i architektur agentowych w kształtowaniu przepływu informacji oraz organizacji wiedzy w Internecie (Stanford HAI, 2025). Wraz z tym procesem Internet przechodzi od modelu transmisji danych do modelu poznawczo-algorytmicznego, w którym technologie AI interpretują, filtrują i generują treści, przyczyniając się zarówno do wzrostu efektywności komunikacyjnej, jak i nowych wyzwań dotyczących integralności informacyjnej. Zjawisko to prowadzi do szeregu implikacji:

- redefinicji pojęcia autorytetu informacyjnego,
- transformacji modelu wyszukiwania wiedzy – od indeksacji do generatywnych odpowiedzi AI,
- algorytmicznego kształtowania opinii publicznej,
- automatyzacji interakcji społecznych i komunikacji,
- przekształcenia modeli gospodarczych i edukacyjnych,
- wzrostu podatności na manipulację informacyjną i dezinformację generowaną przez modele AI.

Wraz z ekspansją sztucznej inteligencji Internet przestaje być neutralną infrastrukturą odbicia rzeczywistości społecznej – staje się środowiskiem współtworzącym tę rzeczywistość, wpływającym na percepcję, decyzje i zachowania użytkowników. W tym sensie Internet nie jest już jedynie technologią pomocniczą, lecz strukturą poznawczą współczesnej cywilizacji, w której bezpieczeństwo informacyjne odgrywa rolę fundamentalną.

Sztuczna inteligencja jako mechanizm Internetu

Rozwój sztucznej inteligencji w ostatnich latach doprowadził do fundamentalnej transformacji Internetu. Współcześnie nie jest on jedynie przestrzenią

gromadzenia i dystrybucji informacji, lecz staje się środowiskiem poznawczym, w którym algorytmy pełnią funkcję filtrów, moderatorów, a coraz częściej także generatorów treści oraz autonomicznych uczestników ekosystemu informacyjnego. Najnowsze analizy globalne, m.in. *Artificial Intelligence Index Report* (Stanford HAI, 2025) wskazują, że systemy oparte na uczeniu maszynowym i modelach generatywnych stają się kluczowym elementem przetwarzania danych w sieci.

Postęp technologiczny w obszarze uczenia głębokiego, transformatorów oraz multimodalnych sieci neuronowych doprowadził do powstania systemów zdolnych do rozumienia kontekstu, analizy semantycznej, przewidywania zachowań użytkowników oraz generowania treści tekstowych, graficznych i dźwiękowych zgodnych z ludzkimi wzorcami kulturowymi. Rozwiązania te są integrowane praktycznie we wszystkich sektorach funkcjonowania Internetu – od wyszukiwarek i mediów społecznościowych, przez edukację i finanse, aż po sektor zdrowia i administrację publiczną. Tendencja ta wpisuje się w globalną koncepcję Internetu zmysłów (Internet of Senses), w której generatywna AI umożliwia coraz bardziej immersyjne formy komunikacji (Sehad i in., 2024).

W początkowej fazie Internet opierał się na algorytmach statycznych, które indeksowały zasoby i porządkowały treści według słów kluczowych. Wprowadzenie uczenia maszynowego doprowadziło do powstania modelu dynamicznego, w którym dostęp do informacji jest kształtowany przez personalizację i predykcyjne modelowanie zachowań użytkowników. Współczesne mechanizmy wyszukiwawcze interpretują zapytania semantycznie, filtrują treści, rekomendują zasoby, moderują komunikację, automatyzują przepływy pracy i generują odpowiedzi zamiast jedynie wskazywać źródła. Zmiana ta prowadzi do stopniowego przejścia od klasycznej wyszukiwarki (search engine) do tzw. silnika odpowiedzi (answer engine), co jest obserwowane m.in. w badaniach nad ruchem internetowym w kontekście generatywnego Google AI Overviews (Scire, 2025).

Modele generatywne zmieniają epistemologię Internetu – wiedza nie musi być już samodzielnie wyszukiwana, ponieważ jest wytwarzana i syntetyzowana przez systemy AI w odpowiedzi na potrzeby użytkownika. Systemy te potrafią generować tekst, kod, obrazy, wideo, a także personalizować narracje w czasie rzeczywistym. Najnowsze przeglądy literatury wskazują, że technologie generatywne zaczynają pełnić funkcję współtwórców wiedzy i informacji cyfrowej, a ich wpływ na społeczeństwo będzie narastał (Musiol, 2024).

Kolejnym istotnym etapem rozwoju Internetu jest popularyzacja systemów agentowych. Agenci AI są zdolni do autonomicznego działania w środowisku cyfrowym – planują i wykonują operacje wieloetapowe, komunikują się z innymi systemami oraz API usług internetowych, a także automatyzują procesy społeczne i gospodarcze. Najnowsze opracowania opisują rodzącą się koncepcję Agentic Web – ekosystemu, w którym głównymi uczestnikami komunikacji są nie tylko ludzie, lecz także autonomiczne systemy AI współdziałające ze sobą (Caetano i in., 2025). Internet staje się w ten sposób przestrzenią koegzystencji ludzi i cyfrowych bytów zdolnych do podejmowania decyzji i zarządzania informacją. Współczesny Internet można zatem opisać jako system złożony z trzech współzależnych warstw:

- warstwy ludzkiej (użytkownicy, instytucje, twórcy treści),
- warstwy infrastrukturalnej (sieci, centra danych, chmura, urządzenia mobilne),
- warstwy algorytmiczno-kognitywnej (systemy predykcyjne, modele generatywne, filtry informacyjne, agenci AI).

Integracja tych warstw prowadzi do powstania symbiotycznego ekosystemu poznawczego, w którym informacja nie jest wyłącznie gromadzona i przesyłana, lecz jest aktywnie interpretowana, modulowana i generowana. To właśnie w tej warstwie algorytmicznej rozstrzygają się współcześnie kwestie bezpieczeństwa informacyjnego – takie jak integralność treści, autentyczność przekazów, odporność na manipulację czy kontrola nad przepływem informacji.

Współczesne społeczeństwo informacyjne w epoce sztucznej inteligencji

Spółeczeństwo informacyjne, którego fundamentalnym zasobem jest informacja, ulega obecnie kolejnemu etapowi transformacji – przejściu do społeczeństwa algorytmicznego. W strukturze społecznej coraz większą rolę odgrywają dane, modele predykcyjne oraz inteligentne systemy informacyjne, które w coraz większym stopniu wpływają na procesy poznawcze, decyzyjne i komunikacyjne. Raporty OECD (2023a) oraz UNESCO (2023) podkreślają, że w erze sztucznej inteligencji informacja przestaje być kategorią bierną – staje się dynamicznie modelowaną strukturą, której interpretacja i dystrybucja zależą od działania algorytmów.

Internet stanowi podstawową przestrzeń pracy, edukacji, komunikacji i rozrywki współczesnego człowieka, a jego rola w procesie socjalizacji młodego pokolenia jest szczególnie znacząca. Badania pokazują, że dzieci i młodzież należą do grup najbardziej intensywnie korzystających z technologii cyfrowych, co sprawia, że środowisko online pełni funkcję zarówno narzędzia edukacyjnego, jak i platformy formowania tożsamości cyfrowej oraz kompetencji społecznych (OECD, 2023b; UNESCO, 2023). Współczesna młodzież funkcjonuje w warunkach stałej ekspozycji na systemy algorytmiczne i traktuje Internet jako naturalne środowisko nauki, rozwoju i komunikacji, jednocześnie będąc odbiorcą treści modelowanych przez mechanizmy personalizacji. Najnowsze przeglądy badań potwierdzają, że personalizacja może prowadzić do ograniczenia różnorodności informacyjnej, powstawania baniek filtrujących oraz kształtowania opinii na podstawie zawężonego zestawu treści (Ahmmed i in., 2025; Ludwig i in., 2025). Jednocześnie rozwój modeli generatywnych prowadzi do pojawienia się zjawiska automatyzowanej komunikacji społecznej, w której użytkownik wchodzi w interakcję nie tylko z innymi ludźmi, lecz także z systemami AI, często nieświadomie, ponieważ treści generowane przez algorytmy nie zawsze są odróżnialne od treści tworzonych przez człowieka (Musiol, 2024).

Rozszerzenie funkcji Internetu oraz intensywna personalizacja doprowadziły także do nasilenia zjawiska uzależnienia cyfrowego. Mechanizmy natychmiastowej gratyfikacji, algorytmiczne wzmacnianie zaangażowania oraz projektowanie bodźców opartych na zmiennej nagrodzie sprzyjają kompulsywnemu korzystaniu z technologii, co znajduje potwierdzenie w najnowszych metaanalizach (Lu i in., 2025). Wraz z rozwojem sztucznej inteligencji pojawia się również nowa forma zależności poznawczej – uzależnienie od systemów wspomagania myślenia i decyzji. Narzędzia generatywne, takie jak modele językowe, ułatwiają tworzenie treści, wyszukiwanie informacji i rozwiązywanie problemów, lecz jednocześnie mogą ograniczać potrzebę samodzielnej refleksji, redukować kompetencje krytyczne oraz prowadzić do delegowania procesów poznawczych na algorytmy (UNESCO, 2023). Zjawisko to określa się mianem algorytmicznego ubezwłasnowolnienia poznawczego, gdy jednostka zaczyna polegać na systemach AI w zakresie uczenia się i podejmowania decyzji, jednocześnie tracąc część autonomii intelektualnej.

W obszarze edukacji sztuczna inteligencja wymusza głęboką przebudowę klasycznego modelu nauczania. Raporty UNESCO (2023) oraz OECD (2023c) wskazują, że edukacja XXI wieku powinna koncentrować się na rozwijaniu kompetencji krytycznych, metapoznawczych oraz umiejętności oceny wiarygodności źródeł. Równocześnie konieczne jest wprowadzanie edukacji dotyczącej etyki technologicznej, bezpieczeństwa cyfrowego oraz zasad odpowiedzialnego korzystania z AI. W literaturze podkreśla się, że narzędzia oparte na sztucznej inteligencji powinny pełnić funkcję wspierającą, a nie zastępującą proces dydaktyczny, a kluczową rolę odgrywa rozwój kompetencji algorytmicznych – czyli podstawowej świadomości dotyczącej sposobu działania i ograniczeń systemów AI (OECD, 2023c).

W rezultacie społeczeństwo informacyjne wchodzi w fazę, w której relacje między człowiekiem a technologią ulegają złożonym przekształceniom. Internet nie jest już przestrzenią neutralną ani bierną, lecz środowiskiem aktywnie współtworzonym przez algorytmy. Sztuczna inteligencja staje się integralnym elementem procesów społecznych, poznawczych i edukacyjnych, prowadząc do powstania nowego modelu organizacji życia społecznego – społeczeństwa algorytmicznego, w którym bezpieczeństwo informacyjne i autonomia poznawcza stają się kluczowymi wyzwaniami współczesnej cywilizacji.

Zagrożenia, regulacje i wyzwania etyczne w erze sztucznej inteligencji

Rozwój sztucznej inteligencji w środowisku internetowym generuje nie tylko nowe możliwości, lecz także zagrożenia o charakterze społecznym, gospodarczym, politycznym i poznawczym. Wraz ze wzrostem złożoności modeli algorytmicznych zwiększa się ich wpływ na życie publiczne, co rodzi konieczność analizy kwestii bezpieczeństwa, przejrzystości, odpowiedzialności i ochrony praw jednostki. Najnowsze raporty OECD (2024) oraz Europol Innovation Lab (2024) wskazują, że technologie generatywne radykalnie przekształcają krajobraz komunikacji cyfrowej i wymagają systemowego podejścia regulacyjnego.

Jednym z najbardziej dynamicznie rozwijających się zagrożeń jest dezinformacja generatywna i manipulacja informacyjna. Modele tworzą realistyczne teksty, obrazy, materiały audio i wideo, często niemożliwe do odróżnienia od treści rzeczywistych. Ułatwia to powstawanie syntetycznych wiadomości, deepfake'ów,

automatycznych profili, kampanii wpływu oraz narzędzi propagandowych opartych na modelach językowych. Badania ACM Computing Surveys podkreślają, że deepfake'i stały się kluczowym wyzwaniem dla bezpieczeństwa informacyjnego i zaufania społecznego (Wang i in., 2024). Zjawisko to ma wymiar polityczny i kulturowy – generatywna AI staje się narzędziem formowania opinii publicznej, wpływając na procesy demokratyczne oraz integralność informacyjną (OECD, 2024; Negreiro, 2025).

Równolegle rośnie znaczenie zagrożeń związanych z prywatnością, danymi osobowymi i bezpieczeństwem cyfrowym. Sztuczna inteligencja opiera się na analizie ogromnych zbiorów danych, co rodzi napięcie pomiędzy postępem technologicznym a prawem jednostki do prywatności. Kluczowe problemy obejmują masowe profilowanie użytkowników, predykcyjne modelowanie ich zachowań, wykorzystywanie danych biometrycznych oraz ryzyko cyberataków na infrastrukturę zasilającą modele AI. Report UE *Facing Reality?* (Europol Innovation Lab, 2024) podkreśla dodatkowo nieprzejrzystość algorytmów, która utrudnia audyt, ocenę zagrożeń oraz przypisanie odpowiedzialności za decyzje podejmowane przez modele.

Istotne wyzwania pojawiają się również w obszarze prawa autorskiego i własności treści generowanych przez sztuczną inteligencję. Rozwój modeli generatywnych prowadzi do debat dotyczących praw własności do treści wytwarzanej przez SI, legalności wykorzystywania danych treningowych, ryzyka naruszania praw twórców oraz odpowiedzialności za nieprawdziwe lub szkodliwe treści. Dyskusje te potwierdzają, że dotychczasowe koncepcje autorstwa, kreatywności i własności intelektualnej stają się niewystarczające wobec twórczości algorytmicznej.

W odpowiedzi na te wyzwania rządy oraz organizacje międzynarodowe opracowują systemy regulacji i nadzoru nad rozwojem sztucznej inteligencji. Unia Europejska przyjęła w 2024 r. przełomowy *Artificial Intelligence Act* – pierwszy kompleksowy system klasyfikacji ryzyka i nadzoru nad AI, obejmujący wymogi transparentności, obowiązki audytowe oraz regulacje dotyczące modeli wysokiego ryzyka (European Union, 2024). W Stanach Zjednoczonych administracja federalna wydała *Executive Order 14110* dotyczący zgodności, bezpieczeństwa i ochrony danych (Federal Register, 2023), choć część jego przepisów została w 2025 r. uchylona przez nową administrację (Reuters, 2025; The White House, 2025). Debaty regulacyjne dotyczą również wpływu silników odpowiedzi

(answer engines) – według analiz (Deck, 2025; Kint, 2025) i Reutersa (2025), generatywne systemy wyszukiwania wpływają na rynek informacji, ruch wydawców oraz konstrukcję ekosystemu medialnego.

Nadrzędnym wyzwaniem pozostają etyka algorytmiczna i odpowiedzialność technologiczna. Nowoczesne systemy Ai muszą być rozwijane w sposób zgodny z wartościami demokratycznymi, zasadami sprawiedliwości oraz ochroną praw człowieka. Kluczowe zagadnienia obejmują przejrzystość modeli, zapobieganie dyskryminacji algorytmicznej, określanie odpowiedzialności za skutki działania systemów autonomicznych oraz wprowadzanie mechanizmów nadzoru i kontroli. W centrum dyskusji znajduje się koncepcja odpowiedzialności technologicznej, zakładająca, że rozwój sztucznej inteligencji musi być nierozzerwalnie związany z oceną jej konsekwencji społecznych i ochroną jednostki przed nadużyciami.

Podsumowanie

Rzeczywisty rozwój sztucznej inteligencji stał się jednym z najważniejszych czynników redefiniujących współczesny Internet oraz architekturę globalnej cywilizacji informacyjnej. Internet, który pierwotnie pełnił funkcję infrastruktury komunikacyjnej i informacyjnej, przekształcił się w złożone środowisko kognitywno-algorytmiczne, w którym systemy AI nie tylko wspierają procesy poznawcze, lecz także współuczestniczą w ich przebiegu. Generatywne modele językowe, systemy rekomendacyjne i agentowe modele działania zmieniły sposób pozyskiwania, interpretowania oraz dystrybucji informacji, czyniąc z AI jeden z kluczowych mechanizmów współczesnego Internetu.

Transformacja ta niesie zarówno wymierne korzyści, jak i istotne zagrożenia. Z jednej strony sztuczna inteligencja zwiększa dostępność wiedzy, usprawnia analizę danych, automatyzuje procesy komunikacji i tworzenia treści oraz wspiera rozwój gospodarczy i naukowy. Z drugiej strony prowadzi do nowych wyzwań dotyczących bezpieczeństwa informacyjnego, odporności społecznej, integralności treści cyfrowych oraz autonomii poznawczej użytkowników. Wraz z ekspansją systemów generatywnych rośnie ryzyko dezinformacji, manipulacji, uprzedzeń algorytmicznych, naruszeń prywatności oraz koncentracji władzy informacyjnej w rękach podmiotów kontrolujących infrastrukturę AI. Jednocześnie niejasność

autorstwa, przejrzystości modeli i odpowiedzialności za działania systemów autonomicznych staje się jednym z kluczowych dylematów współczesnej polityki technologicznej.

Wobec tych wyzwań konieczne jest całościowe podejście do rozwoju sztucznej inteligencji, obejmujące regulacje prawne, mechanizmy audytu algorytmicznego oraz rozwój kompetencji społecznych. Dokumenty prawne, takie jak europejski Artificial Intelligence Act czy amerykańskie regulacje federalne, potwierdzają, że AI wymaga nadzoru instytucjonalnego i normatywnego. Jednak równie istotnym elementem jest edukacja – kształtowanie kompetencji cyfrowych, świadomości algorytmicznej, umiejętności krytycznej analizy treści oraz zdolności do świadomego korzystania z zaawansowanych systemów informacyjnych.

Najbliższe lata przyniosą konieczność wypracowania równowagi między innowacyjnością technologii a ochroną wartości demokratycznych i humanistycznych. Internet przyszłości będzie środowiskiem współpracy człowieka i inteligentnych systemów, w którym rola człowieka nie powinna zostać zredukowana, lecz wzmocniona poprzez odpowiednią refleksję, kompetencje i narzędzia. Odpowiedzialne, transparentne i etyczne wykorzystanie sztucznej inteligencji stanowi fundament zrównoważonego rozwoju społeczeństwa cyfrowego oraz warunków bezpiecznej ewolucji Internetu jako medium kluczowego dla funkcjonowania współczesnej cywilizacji.

Literatura

1. Ahmmad, M., Shahzad, K., Iqbal, A., Latif, M. (2025). Trap of social media algorithms: A systematic review of filter bubbles and echo chambers and their impact on youth. *Societies*, 15(11), 301. <https://doi.org/10.3390/soc15110301>
2. Caetano, A., Verma, K., Taheri, A., Kumaran, R., Chen, Z., Chen, J., Höllerer, T., Sra, M. (2025). *Agentic workflows for conversational human-AI interaction design* (preprint). arXiv. <https://doi.org/10.48550/arXiv.2501.18002>
3. Camarinha-Matos, L. M., Ortiz, A., Boucher, X., Osório, A. L. (Eds.). (2022). *Collaborative Networks in Digitalization and Society 5.0: 23rd IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2022, Lisbon, Portugal, September 19-21, 2022, Proceedings* (IFIP Advances in Information and Communication Technology, Vol. 662). Springer Cham. <https://doi.org/10.1007/978-3-031-14844-6>

4. Europol Innovation Lab. (2024, March 4). *Facing reality? Law enforcement and the challenge of deepfakes: An observatory report from the Europol Innovation Lab*. Publications Office of the European Union.
5. Federal Register. (2023, November 1). *Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (88 Fed. Reg. 76,403).
6. Ludwig, K., Müller, P., Nikolajevic, N., Grote, A. (2025). Putting ‘filter bubble’ effects to the test: Evidence on the polarizing impact of ideology-based news recommendation from two experiments in Germany and the U.S. *Information, Communication & Society*, 1-20. Advance online publication. <https://doi.org/10.1080/1369118X.2024.2435998>
7. Lu, P., Qiu, J., Huang, S., Wang, X., Han, S., Zhu, S., Ning, Y., Zeng, F.-F., Yuan, Y. (2025). Interventions for digital addiction: Umbrella review of meta-analyses. *Journal of Medical Internet Research*, 27, e59656. <https://doi.org/10.2196/59656>
8. Musiol, M. (2024). *Generative AI: Navigating the course to the artificial general intelligence future* (ISBN 978-1-394-20591-2). Wiley.
9. OECD. (2023a). *AI and the future of skills: Volume 2*. OECD Publishing. <https://doi.org/10.1787/ae96ca6c-en>
10. OECD. (2023b). *Employment outlook 2023: Skill needs in the age of AI*. OECD Publishing. <https://doi.org/10.1787/7c5219e7-en>
11. OECD. (2023c). *Artificial intelligence and the future of skills: Project overview*. OECD Publishing. <https://doi.org/10.1787/11f00efb-en>
12. OECD. (2024). *Facts not fakes: Tackling disinformation, strengthening information integrity*. OECD Publishing. <https://doi.org/10.1787/8055b8f6-en>
13. Perriam, J., Carter, S. (Eds.). (2021). *Understanding Digital Societies*. SAGE Publications Ltd.
14. Sehad, N., Bariah, L., Hamidouche, W., Hellaoui, H., Jäntti, R., Debbah, M. (2025). Generative AI for immersive communication: The next frontier in Internet-of-Senses through 6G. *IEEE Communications Magazine*, 63(2), 31-43. <https://doi.org/10.1109/MCOM.001.2400199>
15. Sehad, N., Bariah, L., Hamidouche, W., Hellaoui, H., Jäntti, R., Debbah, M. (2024). *Generative AI for immersive communication: The next frontier in Internet-of-Senses through 6G* (preprint). arXiv. <https://doi.org/10.48550/arXiv.2404.01713>
16. van Dijck, J., van Es, K., Helmond, A., van der Vlist, F. (Eds.). (2025). *Governing the digital society: Platforms, artificial intelligence, and public values*. Amsterdam University Press. <https://doi.org/10.5117/9789048562718>

17. Wang, T., Liao, X., Chow, K. P., Lin, X., Wang, Y. (2024). *Deepfake detection: A comprehensive survey from the reliability perspective*. *ACM Computing Surveys*, 57(3), 1-35. <https://doi.org/10.1145/3699710>

Netografia

1. DataReportal. (2025a). *Digital 2025: Global Overview Report*. DataReportal – Global Digital Insights. Pobrane z: <https://datareportal.com/reports/digital-2025-global-overview-report> (dostęp: 06.11.2025).
2. DataReportal. (2025b). *Digital in Poland 2025*. DataReportal – Global Digital Insights. Pobrane z: <https://datareportal.com/reports/digital-2025-poland> (dostęp: 06.11.2025).
3. Deck, A. (2025, May 5). *Google is using content from publishers who “opt out” of other AI training to power AI Overviews*. Nieman Journalism Lab. Pobrane z: <https://www.niemanlab.org/2025/05/google-is-using-content-from-publishers-who-opt-out-of-other-ai-training-to-power-ai-overviews/> (dostęp: 06.11.2025).
4. Ericsson. (2024a, November). *Ericsson mobility report: November 2024*. Ericsson. Pobrane z: <https://www.ericsson.com/en/reports-and-papers/mobility-report> (dostęp: 06.11.2025).
5. Ericsson. (2024b, June). *Ericsson mobility report: June 2024* (PDF). Ericsson. Pobrane z: <https://www.ericsson.com/en/reports-and-papers/mobility-report> (dostęp: 06.11.2025).
6. European Union. (2024, July 12). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence*. Official Journal of the European Union L 273, 1-175. Pobrane z: <https://data.europa.eu/eli/reg/2024/1689/oj> (dostęp: 06.11.2025).
7. Kint, J. (2025, August 14). *Facts: Google’s push to AI hurts publisher traffic*. Digital Content Next. Pobrane z: <https://digitalcontentnext.org/blog/2025/08/14/facts-googles-push-to-ai-hurts-publisher-traffic/> (dostęp: 06.11.2025).
8. Negreiro Achiaga, M. D. M. (2025, July 3). *Children and deepfakes* (Briefing). European Parliamentary Research Service, European Parliament. Pobrane z: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf) (dostęp: 06.11.2025).
9. Reuters. (2025, January 21). *Trump revokes Biden executive order addressing AI risks*. Reuters. Pobrane z: <https://www.reuters.com/world/us/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/> (dostęp: 06.11.2025).

10. Reuters. (2025, July 4). *EU antitrust complaint vs. Google AI Overviews*. Reuters. Pobrane z: <https://www.reuters.com/world/europe/eu-antitrust-complaint-vs-google-ai-overviews-2025-07-04/> (dostęp: 06.11.2025).
11. Scire, S. (2025). *Google referrals are steady, but social and direct are down, according to new Chartbeat data*. Nieman Journalism Lab. Pobrane z: <https://www.niemanlab.org/reading/google-referrals-are-steady-but-social-and-direct-are-down-according-to-new-chartbeat-data/> (dostęp: 06.11.2025).
12. Stanford Institute for Human-Centered Artificial Intelligence. (2025). *Artificial Intelligence Index Report 2025*. Stanford University. Pobrane z: <https://aiindex.stanford.edu/report/> (dostęp: 06.11.2025).
13. Ten Teije, S. (2025, August 11). *Google's AI Overview is not yet harming traffic, but publishers should remain alert*. INMA. Pobrane z: <https://www.inma.org/blogs/big-data-for-news-publishers/post.cfm/google-s-ai-overview-is-not-yet-harming-traffic-but-publishers-should-remain-alert> (dostęp: 06.11.2025).
14. The White House. (2025, January 23). *Removing barriers to American leadership in AI*. Pobrane z: <https://www.whitehouse.gov/briefing-room/presidential-actions/2025/01/23/removing-barriers-to-american-leadership-in-ai/> (dostęp: 06.11.2025).
15. UNESCO. (2023). *Guidance for generative AI in education and research*. UNESCO Publishing. Pobrane z: <https://unesdoc.unesco.org/ark:/48223/pf0000386081> (dostęp: 06.11.2025).