Roczniki Kulturoznawcze
Tom XVI, numer 4 – 2025
https://doi.org/10.18290/rkult25164.15

DOMINIKA SKOCZYLAS

„CYBERBEZPIECZNA" KOMUNIKACJA SPOŁECZNA W DOBIE DEZINFORMACJI I SZTUCZNEJ INTELIGENCJI

1. PRAWO DO WOLNOŚCI WYPOWIEDZI I DOSTĘPU DO INFORMACJI A WSPÓŁCZESNY MODEL KOMUNIKACJI SPOŁECZNEJ – ZAGADNIENIA WPROWADZAJĄCE

Za jedne z najważniejszych czynników wspierających działania w zakresie ułatwienia dostępu do informacji należy uznać cyfryzację usług oraz informatyzację administracji publicznej. Odkąd idea transformacji cyfrowej stała się podstawą koncepcji, planów i strategii, których celem było zapewnienie rozwoju społeczno-gospodarczego, wzrosło również zainteresowanie tzw. komunikacją, stricte e-komunikacją społeczną[1]. Można powiedzieć, że środki komunikacji elektronicznej[2] zrewolucjonizowały dotychczasowe podejście do kontaktów międzyludzkich, ale także przyczyniły się do wzrostu wiedzy i umiejętności oraz zaangażowania w procesy demokratyczne (e-demokratyczne) obywateli. To właśnie potrzeby społeczeństwa informacyjnego, którymi są nieprzerwany dostęp, przetwarzanie i wykorzystywanie informacji, w dużym stopniu wpłynęły na

Dr Dominika Skoczylas – Uniwersytet Szczeciński; adres do korespondencji: ul. Narutowicza 17a, 70-240 Szczecin; e-mail: dominika.skoczylas@usz.edu.pl; ORCID: https://orcid.org/0000-0003-1231-8078.

[1] Lidia Jaskuła wskazuje, że „swoboda uzewnętrzniania i rozpowszechniania wobec innych własnych poglądów i informacji" możliwa jest „za pośrednictwem wszelkich środków społecznego przekazu". Zob. Lidia Jaskuła, „Prawo prasowe w poszukiwaniu prawdy", w: *Prawo w poszukiwaniu prawdy, dobra i piękna. Księga Jubileuszowa ks. prof. Sławomira Fundowicza*, red. Paweł Świtał, Bartosz Kuś i Emilia Gulińska (Radom: Sieć Badawcza Łukasiewicz – Instytut Technologii Eksploatacji, 2024), 252.

[2] Zgodnie z art. 2 pkt 5 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2024 r. poz. 1513), środki komunikacji elektronicznej to rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną.

zmiany tradycyjnego sposobu komunikacji[3]. W tym miejscu należałoby jednak wskazać, dlaczego przedstawiciele społeczeństwa informacyjnego tak bardzo upodobali sobie komunikację za pośrednictwem nowych technologii. Nie jest chyba szczególnie zaskakujące to, że doceniono przede wszystkim walory związane z automatyzacją, jakością i szybkością (brak ograniczeń czasu i miejsca) przekazywania informacji. Faktycznie informacja stała się produktem, *social media* głównym źródłem dostępu do niej, a anonimowość (pozorna) pozwoliła na wyeliminowanie barier komunikacyjnych, które istnieją w świecie rzeczywistym. Swoboda wypowiedzi może być rozumiana zarówno w aspekcie pozytywnym (wyrażenie konstruktywnej opinii), jak i negatywnym (agresja w wypowiedziach czy działania dezinformacyjne)[4]. Współczesny model komunikacji społecznej jest (co trzeba bezspornie przyznać) kreowany przez mass media, a ściślej ich użytkowników (administratorów platform internetowych, grupy społecznościowe posiadające różne cele i motywy działania). Tym samym obok gwarancji wolności wypowiedzi w internecie pojawia się kolejne wyzwanie związane z selekcją nadmiaru informacji i ochroną prawdy informacyjnej (przeciwdziałanie dezinformacji). Komunikacja społeczna, czy raczej „społeczne zachowania powodowane są kulturą nadmiaru wynikającą z niepoliczalnej i niekonsumowalnej ilości treści, a zwłaszcza dynamicznymi zmianami w obrębie technologii cyfrowych”[5]. Niepoliczalny i niekontrolowany transfer informacji w połączeniu z negatywnym kontekstem (narracją) komunikatu sprzyja celom propagandowym. Ponadto uniemożliwia dostęp do wiarygodnej i rzetelnej informacji oraz kształtuje (celowo) określone wzorce postępowania.

Zrozumienie i wykorzystanie zasobów informacyjnych jest kwestią indywidualną i zależy od możliwości percepcyjnych użytkownika, tj. wiedzy, umiejętności i tzw. kompetencji miękkich (praktycznego zastosowania danych). Paweł Kłos wskazuje, że „swobodny dostęp do internetu wraz ze stopniową eliminacją wykluczenia cyfrowego i […] ochroną prywatności i wolności słowa”[6], należy uznać za podstawowe prawa przedstawicieli społeczeństwa informacyjnego. Trudno się z tym stwierdzeniem nie zgodzić. Co więcej, należy podkreślić, że środki komunikacji elektronicznej stały się gwarantem realizacji konstytucyjnych

[3] Tomasz Warchoł, „Edukacja pozaformalna wsparciem edukacji w społeczeństwie informacyjnym”, *Polityka i Społeczeństwo* 2, nr 21 (2023):259, DOI:10.15584/polispol.2023.2.17.

[4] Robert Grochowski, „Ekspansywny wpływ cyberprzestrzeni na tożsamość człowieka”, *Fides, Ratio et Patria. Studia Toruńskie* 9 (2018):52-54, DOI:10.56583/frp.1551.

[5] Sławomir Rogowski, „Pojęcie społeczeństwa kontentowego a problematyka kultury nadmiaru”, *Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie* 53 (2024):102, DOI:10.17512/znpcz.2024.1.08.

[6] Paweł Kłos, „Cywilizacja informacyjna a prawo – preliminaria”, w: *Horyzonty Informacji 5* , red. Paloma Korycińska (Kraków: Uniwersytet Jagielloński, Biblioteka Jagiellońska, 2023), 32.

praw i wolności, takich jak wolność wyrażania swoich poglądów, pozyskiwania i rozpowszechniania informacji[7] oraz dostęp do informacji publicznej[8].

Elektroniczny model wymiany informacji umożliwia interaktywną komunikację społeczną o masowym charakterze. Interaktywność natomiast wyraża się w kontekście oddziaływania przekazu medialnego na jego odbiorcę. Innymi słowy, „między użytkownikami lub między użytkownikami a informacjami zachodzi sprzężenie zwrotne"[9], co uwydatnia konieczność przeprowadzenia pogłębionej analizy, interpretacji kontekstu oraz ustalenia źródła pochodzenia danych. Nie można zapomnieć o tym, że środowisko online jest miejscem wzmożonej interakcji, integracji i wymiany poglądów, co sprzyja kreowaniu określonych informacji, również tych nieprawdziwych. Tworzenie tzw. *fake newsów* jest w rzeczywistości zabiegiem socjotechnicznym, stosownym w celu wprowadzenia w błąd nadmiernie ufnego odbiorcy komunikatu[10]. Manipulowanie informacją, szczególnie w dobie sztucznej inteligencji, stało się praktycznie niezauważalne, co czyni jeszcze trudniejszym wyodrębnienie informacji prawdziwych od tych, które nie posiadają takiego atrybutu. Wyzwaniem dla zapewnienia bezpieczeństwa komunikacji społecznej w sieci są tzw. cyberzagrożenia[11], które nie tylko zagrażają autentyczności i dostępności informacji, ale również zachowaniu integralności i poufności danych osobowych. Powyższe rozważania skłaniają do refleksji nad stanem cyberbezpieczeństwa komunikacji społecznej.

---

[7] Zob. art. 54 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483, ze zm.).

[8] Zgodnie z art. 61 ust. 1 Konstytucji RP, obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej, osób pełniących funkcje publiczne, organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Szczegółowy zakres dostępu do informacji określa Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902).

[9] Andrzej Adamski, *Media w analogowym i cyfrowym świecie. Wpływ cyfrowej rewolucji na rekonfigurację komunikacji społecznej* (Warszawa: Dom Wydawniczy Elipsa, 2012), 90.

[10] Sandra Omieczyńska, „Komunikacja w cyberprzestrzeni – wyzwania, bariery i korzyści", w: *Communication as a factor of transparency of social interaction: psychological, historical, legal, economic and political dimensions*, red. Jacek Mrozek, Oksana Koval i Krystyna Ziółkowska (Ełk: Centrum Badań Europy Wschodniej UWM w Olsztynie, 2022), 401-402.

[11] Za cyberzagrożenie uznaje się wszelkie potencjalne okoliczności (zdarzenie lub działanie), które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób. Zob. art. 2 pkt 8 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz.UE.L 2019 Nr 151, str. 15).

2. KOMUNIKACJA SPOŁECZNA W DOBIE DEZINFORMACJI I SZTUCZNEJ INTELIGENCJI

Cyberprzestrzeń jest dość specyficznym środowiskiem komunikacji, albowiem z jednej strony zapewnia szybki i nieograniczony sposób kontaktu na odległość, z drugiej zaś stanowi obszar wielu nadużyć, tj. incydentów, cyberprzestępstw czy działań natury dezinformacyjnej. Środki komunikacji elektronicznej stanowią obecnie podstawowy sposób przekazu informacji. Dostępność, interaktywność, możliwość personalizacji informacji czy usług – to tylko niektóre z walorów nowych technologii. Nie dziwi zatem ich popularność w sektorze publicznym i prywatnym, wśród placówek oświatowych, instytucji finansowych, partii politycznych, a przede wszystkim w kręgu influencer*ów*. Zresztą ci ostatni doskonale wykorzystują swój wizerunek do działań marketingowych, a dzięki nawiązaniu relacji ze swoim obserwatorami są w stanie kreować określone wzorce postępowania i wpływać na ich decyzje – nie tylko te o charakterze *stricte* konsumpcyjnym[12]. Nowe technologie, co oczywiste, wspierają działania człowieka, jego aktywność zawodową i aktywizują różne sfery życia prywatnego. Niemniej jednak coraz częściej zauważa się negatywne skutki, takie jak wykluczenie cyfrowe, polaryzacja społeczeństwa, mowa nienawiści, propaganda dezinformacyjna (*fake newsy*), dyskredytowanie określonych wartości czy nawet cyberinwigilacja[13]. Należy zgodzić się z tym, że „bogactwo przekazu medialnego powoduje […] zaangażowanie zmysłowe odbiorcy oraz większe zainteresowanie”[14]. Użytkownicy środków komunikacji elektronicznej powinni jednak charakteryzować się szczególną ostrożnością w zakresie przetwarzania informacji w cyberprzestrzeni. Ma to związek przede wszystkim z tzw. chaosem informacyjnym. Obecnie celom dezinformacyjnym sprzyja algorytmizacja usług. Można zatem stwierdzić, że to dezinformację i powszechne wykorzystywanie systemów sztucznej inteligencji należy uznać za potencjalne cyberzagrożenia dla autentycznej, bezpiecznej i efektywnej komunikacji społecznej w XXI wieku.

Stosowanie innowacyjnych, nowoczesnych rozwiązań teleinformatycznych pozytywnie wpływa na dostępność oraz jakość przepływu informacji na odległość, w ramach elektronicznej (cyfrowej) komunikacji społecznej. Warto podkreślić, że o ile wolność wypowiedzi i prawo dostępu do informacji mogą

[12] Dominika Marzec, „Znaczenie influencer marketingu w kształtowaniu decyzji współczesnych konsumentów”, *Media i Społeczeństwo* 16 (2022):162-163, DOI:10.53052/MiS.2022.16.10.

[13] Łukasz Flak, „Między demonizacją a apoteozą – krytyczny przegląd naukowy odnośnie mediów cyfrowych”, *Kultura – Media – Teologia* 4, nr 48 (2021):121, DOI:10.21697/kmt.48.5.

[14] Katarzyna Garwol i Krystian Bieś, „Seniorzy w świecie mediów XXI wieku”, *Dydaktyka Informatyki* 17 (2022):24, DOI:10.15584/di.2022.17.3.

być realizowane za pośrednictwem nowych technologii, o tyle wzrasta potrzeba ochrony tych praw przed potencjalnymi cyberzagrożeniami. Cyberataki typu *phishing*, *spyware*, złośliwe oprogramowania (*malware*), wirusy, działania o charakterze cyberprzestępczym czy cyberterrorystycznym, mogą bowiem wyrządzić szkodę w sensie technologicznym (przerwanie świadczenia usługi, naruszenie bezpieczeństwa systemowego), ale przede wszystkim mogą być niebezpieczne dla użytkowników e-usług[15]. Niestety, użytkownicy internetu bardzo często są nieświadomi tego, że stali się ofiarami cyberataku. Wskazuje się, że to m.in. „zdenerwowanie, pośpiech, niedokładne czytanie otrzymanej wiadomości, niezwracanie szczególnej uwagi na błędy w treści korespondencji"[16] wzmacnia skuteczność cyberataków. Oczywiście cyberzagrożenie w znaczeniu technicznym, którego efektem jest np. awaria sprzętu bądź niedostępność aplikacji, jest bardziej czytelne niż to, które polega na stworzeniu nieprawdziwej narracji, czego skutkiem jest wywołanie tzw. szumu informacyjnego.

W kontekście bezpiecznej i dostępnej dla każdego komunikacji społecznej należy uwzględnić trzy aspekty: prawdę informacyjną, innowacyjne technologie i e-partycypację użytkowników w zakresie dostępu do informacji, wolności wypowiedzi, ale również wyboru mediów, kanałów źródłowych (platform internetowych), z których będą czerpać wiedzę. Niewątpliwie elektroniczna komunikacja społeczna (szerzej: nowe technologie) narażona jest na działania związane z „brakiem transparentności oraz ich niekontrolowaną komercjalizacją, w tym danych osobowych użytkowników (…) rozprzestrzenianiem dezinformacji i propagandy w mediach społecznościowych"[17]. Dezinformacja stanowi poważne zagrożenie dla tzw. prawdy informacyjnej. Co ważne, dezinformacja jest informacją, niemniej jednak jej intencją jest celowe wprowadzenie w błąd, aby skłonić jej adresata do odpowiedniego zachowania się. Innymi słowy, nadprodukcja informacji (konglomerat danych) powoduje, oprócz pewnego rodzaju chaosu informacyjnego, problem odróżnienia informacji prawdziwych od tych, którym taka właściwość nie przysługuje. Dodatkowo kreowanie fałszywych treści według preferencji odbiorcy komunikatu (personalizacja) pozwala na ugruntowanie jego poglądu (przekonań) i uznania

[15] Dominika Skoczylas, „Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe", *Prawo w Działaniu. Sprawy karne* 53 (2023):101-102, DOI:10.32041/pwd.5306.

[16] Anita Połowin, „Cyberzagrożenia w internecie – analiza przypadków", *Cybersecurity and Law* 2, nr 12 (2024):129, DOI:10.35467/cal/188563.

[17] Alicja Jaskiernia, „Pluralizm, transparentność i odpowiedzialność. Nowe regulacje Unii Europejskiej w obszarze mediów i technologii cyfrowych", *Studia Medioznawcze*, 25, nr 1/96 (2024):20.

informacji za prawdziwą[18]. Wzmacnianie nieprawdziwego wizerunku i dyskredytowanie określonych wartości (szczególnie tych tradycyjnych) potęguje poczucie destabilizacji w komunikacji społecznej. Cele propagandy dezinformacyjnej realizują tzw. trolle czy boty społecznościowe, które w skoordynowany sposób rozpowszechniają *fake newsy*. Ich skuteczność wynika z tego, że „działają w grupie i nawzajem udostępniają i lajkują swoje posty, co przekłada się na (…) popularność zamieszczanych przez nie treści"[19]. Dezinformacja wpływa na sferę emocjonalną i psychiczną, może wzbudzać niepokój, skrajne emocje, a nawet agresję. Stanowi formę manipulacji ludźmi, w szczególności wrażliwymi członkami społeczeństwa. Jest elementem wojny hybrydowej na poziomie międzynarodowym, państwowym, społecznym, politycznym czy gospodarczym. Kazuistycznie dezinformacja stała się elementem kryzysu migracyjnego na granicy polsko-białoruskiej w 2021 roku. Pokłosiem tej sytuacji było m.in. powstanie filmu „Zielona Granica"[20]. W literaturze wskazuje się, że działania dezinformacyjne w tym przypadku przyczyniły się do „podziału społeczeństwa polskiego, do podważenia autorytetu służb granicznych w obliczu zagrożenia, jakim był kryzys migracyjny, ćwiczenia wojskowe Federacji Rosyjskiej i Białorusi ZAPAD 2021, które mogły destabilizować państwo"[21]. Niewątpliwie wojna hybrydowa oparta w dużej mierze na działaniach pozamilitarnych sprzyja kształtowaniu nieprawdziwej narracji na płaszczyźnie ekonomicznej, gospodarczej, społecznej, politycznej czy prawnej. Tym samym na znaczeniu zyskuje wzmocnienie kompetencji cyfrowych użytkowników sieci, rozumiane nie tylko przez pryzmat umiejętności technicznych, ale również jako czynności analityczne, polegające na pogłębianiu wiedzy na temat potencjalnych cyberzagrożeń. Należy się zatem zgodzić z Agnieszką Szczygielską, która wskazuje, że „świadomość istnienia różnego rodzaju zagrożeń (…), możliwości reakcji na nie i rozeznania w obecnej sytuacji powodują wzrost racjonalnego postępowania i działania (…)"[22]. Ponadto dezinformacja może być jednym z komponentów cyberinwigilacji, formą kontroli nad przetwarzaniem

[18] Grażyna Szpor, „Dezinformacja", w: *Wielka Encyklopedia Prawa. Tom XXII – Prawo informatyczne*, red. Brunon Hołyst (Warszawa: Fundacja „Ubi societas, ibi ius", 2021), 109-110.

[19] Agnieszka Łukasik-Turecka, „Boty w służbie dezinformacji", *Polityka i Społeczeństwo* 4, nr 22 (2024):141, DOI:10.15584/polispol.2024.4.9.

[20] „Zielona Granica" – film Agnieszki Holland z 2023 roku. Zob. Maciej Pieczyński, „Zielona granica propagandy", dostęp: 05.04.2025, https://dorzeczy.pl/opinie/486645/pieczynski-zielona-granica-propagandy.html.

[21] Agnieszka Zaręba, „Dezinformacja jako zagrożenie hybrydowe cyberbezpieczeństwa społecznego (social cyberseciurity)", *Cybersecurity and Law* 1, nr 13 (2025):103-104.

[22] Agnieszka Szczygielska, „Konflikt hybrydowy – analiza porównawcza źródeł wiedzy o zjawisku", *Roczniki Nauk Społecznych* 15/51, nr 2 (2023):32, DOI:10.18290/rns2023.002232.

i wymianą informacji. W komunikacji społecznej jest to szczególnie niebezpieczne, ponieważ podaje w wątpliwość wiarygodność danych, a także wpływa na zniekształcenie form i sposobów komunikacji. W skrajnym przypadku, może być formą kontroli i manipulacji użytkowników sieci[23].

W poszukiwaniu odpowiedzi na pytanie o czynniki, które mogą wzmacniać poczucie chaosu informacyjnego, należy jeszcze wspomnieć o sztucznej inteligencji. Oczywiście, algorytmizacja posiada wiele walorów, do których należą m.in. innowacyjność oraz personalizacja usług, automatyzacja procesów, szybkość i transparentność działania. Zresztą zastosowanie systemów sztucznej inteligencji ma pozytywny wpływ na rozwój społeczno-gospodarczy, jednocześnie wspiera działalność człowieka w kluczowych sektorach[24]. Z drugiej strony może być także narzędziem wykorzystywanym w celu zdeformowania procesów komunikacyjnych, tj. tworzenia *fake newsów* czy szerzenia propagandy dezinformacyjnej. Dlatego też coraz częściej zwraca się uwagę na kontekst ochrony praw człowieka przed działaniami sztucznej inteligencji, także w sferze dostępu do informacji, a przede wszystkim cyberinwigilacji[25]. Jednakże w literaturze przedmiotu wskazuje się, że sztuczna inteligencja może być wykorzystana także do walki z dezinformacją. Tomasz Wróblewski podkreśla, że umożliwia ona „szybką i skuteczną identyfikację oraz neutralizację fałszywych informacji". Jednocześnie zaznacza, że „algorytmy uczenia maszynowego są w stanie analizować ogromne ilości danych, identyfikując wzorce charakterystyczne dla dezinformacji"[26]. Można zatem pokusić się o stwierdzenie, że od użytkownika sztucznej inteligencji będzie zależało to, w jakim celu oraz w jaki sposób ją wykorzysta. Co więcej, kazus wojny na Ukrainie wskazuje, że algorytmy stały się komponentem wojny hybrydowej, albowiem „niektóre operacje informacyjne (…) promowały narracje faworyzowane przez Rosję i miały skutki psychologiczne"[27]. *De facto* stanowiły narzędzie kampanii dezinformacyjnej. Dlatego też w procesie komunikacji społecznej należy zastanowić się nad wdrożeniem standardów

---

[23] Konrad Snopkiewicz, „Przegląd zagrożeń w cyberprzestrzeni", *Studia Administracji i Bezpieczeństwa* 9 (2020):35.

[24] Dominika Skoczylas, „Sztuczna inteligencja a dobrostan człowieka i ochrona praw podstawowych – rozważania na gruncie aktu w sprawie sztucznej inteligencji", *Studia Prawnoustrojowe* 67 (2025):356, DOI:10.31648/sp.10403.

[25] Jarosław Bugajski, „Sztuczna inteligencja – zagrożenie czy bezpieczeństwo?", *Zbliżenia Cywilizacyjne* 19, nr 3 (2023):33, DOI:10.21784/ZC.2023.015.

[26] Tomasz Wróblewski, „Sztuczna inteligencja jako narzędzie do walki z dezinformacją", *International Journal of Legal Studies* 1, nr 17 (2024):163, DOI:10.5604/01.3001.0054.6967.

[27] Agnieszka Gryszczyńska, „Wykorzystanie sztucznej inteligencji w cyberatakach", w: *Internet. Hacking*, red. Agnieszka Gryszczyńska, Grażyna Szpor i Wojciech R. Wiewiórowski (Warszawa: C.H. Beck, 2023), 215.

cyberbezpieczeństwa w związku z wykorzystywaniem sztucznej inteligencji. Na pewno zarówno na etapie projektowania, jak i użytkowania algorytmów należy uwzględnić zasadę praworządności, ochronę prawa oraz wolności człowieka i obywatela, uczciwość, dostępność i wiarygodność treści informacyjnych[28]. Sprzyja to budowaniu zaufania do komunikacji społecznej w trybie online.

3. STANDARDY CYBERBEZPIECZEŃSTWA W RAMACH KOMUNIKACJI SPOŁECZNEJ

Biorąc pod uwagę podstawowe założenia komunikacji społecznej, należy przyznać, że technologie informacyjno-komunikacyjne doskonale realizują postulaty dostępności, szybkości oraz transgraniczności przetwarzania informacji. Niemniej jednak nie można zignorować działań, które mogą w istotny sposób ograniczyć prawo dostępu do informacji, wolność wypowiedzi czy pluralizm mediów. Bezpieczeństwo komunikacji (e-komunikacji) wymaga zatem przyjęcia określonych rozwiązań natury prawno-technologicznej zapewniających ochronę: danych osobowych, prawdy informacyjnej (przeciwdziałanie dezinformacji) oraz przed zagrożeniami o cyberprzestępczym czy cyberterrorystycznym charakterze. Na znaczeniu zyskują zatem tzw. standardy cyberbezpieczeństwa, które zgodnie z definicją przedmiotowego pojęcia określa się poprzez zapewnienie odporności systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[29]. Zasadniczo kluczowe miejsce w politykach cyberbezpieczeństwa powinny również zająć zasady wykorzystania sztucznej inteligencji oraz wzmacnianie kompetencji cyfrowych użytkowników internetu (cyberhigiena). Zresztą należy podjąć wszystkie możliwe kroki, aby ograniczyć (najlepiej wyeliminować) informacje nieprawdziwe, co niewątpliwie może przyczynić się do szerzenia prawdy informacyjnej i ochrony przed manipulacją (propagandą dezinformacyjną). Nie można zapomnieć, że współcześnie warunkiem *sine qua non* cyberbezpieczeństwa komunikacji społecznej jest „transparentność działania algorytmów mechanizmów sztucznej inteligencji (…)"[30], co determinuje

[28] Aleksandra Igielska, „Wielki Brat patrzy. Sztuczna inteligencja w obliczu ochrony praw człowieka", w: *Dialog sądowy w sferze praw człowieka*, red. Bartłomiej Oręziak (Warszawa: Wydawnictwo Naukowe Uniwersytetu Kardynała Stefana Wyszyńskiego, 2022), 84-85.

[29] Zob. art. 2 pkt 4 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077, 1222).

[30] Dominik Lubasz, „Zasady legalności, przejrzystości i minimalizacji danych w ogólnym rozporządzeniu o ochronie danych osobowych w kontekście sztucznej inteligencji", w: *Prawo sztucznej inteligencji*, red. Luigi Lai i Marek Świerczyński (Warszawa: C.H. Beck, 2020), 173.

konieczność aktualizacji dotychczas przyjętych standardów cyberbezpieczeństwa w e-komunikacji.

Kluczowym aspektem w ramach konstruowania standardów cyberbezpieczeństwa komunikacji społecznej będzie zapewnienie kompatybilności działań w trzech obszarach: prawdy informacyjnej (wiarygodność informacji), innowacyjności (dostępność usług za pomocą różnorodnych narzędzi komunikacyjnych), e-partycypacji (aktywne uczestnictwo użytkowników sieci w procesach związanych z przetwarzaniem informacji). Niewątpliwie dzisiaj w związku z takimi zabiegami, jak nadprodukcja czy pomijanie informacji istotnych, mamy do czynienia z szumem informacyjnym. W efekcie trudno odróżnić informacje prawdziwe od nieprawdziwych, co dodatkowo potęguje intensyfikacja działań tzw. trolli czy botów społecznościowych. Co więcej, środki komunikacji elektronicznej stały się czynnikiem zmiany kultury administrowania i korzystania z informacji. Zaufanie do nowych technologii, w wyniku wzrostu działalności dezinformacyjnej, powinno ulec obniżeniu, *de facto* jednak służy wzmocnieniu polaryzacji społeczeństwa, manipulacji określonymi grupami społecznymi, wpływa na procesy decyzyjne i zachowania. Brak umiejętności krytycznego myślenia i selekcji danych oraz „wielość źródeł informacji nie idzie w parze ze wzrostem mechanizmów weryfikowania ich wiarygodności"[31].

Działania na rzecz cyfryzacji usług, informatyzacji zadań i wykorzystania innowacyjnych rozwiązań technologicznych stały się obiektem zainteresowań w Unii Europejskiej. W przypadku cyberbezpieczeństwa za podstawowe akty prawne uznaje się dyrektywę NIS2[32] czy akt o cyberbezpieczeństwie[33]. Ochronę danych osobowych reguluje RODO[34], z kolei ramy prawne dotyczące sztucznej inteligencji przedstawiono w akcie w sprawie sztucznej

[31] Karol Dobrzeniecki, „Post-prawda jako zagrożenie dla podstaw etycznych społeczeństwa informacyjnego", w: *Internet. Strategie bezpieczeństwa*, red. Agnieszka Gryszczyńska i Grażyna Szpor (Warszawa: C.H. Beck, 2017), 182.

[32] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.Urz.UE.L. 2022 Nr 333, s. 80).

[33] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz.UE.L. 151 z 7.6.2019 r., s. 15).

[34] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE.L. 2016 Nr 119, str. 1).

inteligencji[35]. W kontekście cyberbezpiecznej komunikacji społecznej kluczowe znaczenie należy przypisać aktowi o usługach cyfrowych[36]. Należy podkreślić, że celem Unii Europejskiej jest zapewnienie użytkownikom bezpiecznej przestrzeni cyfrowej przy jednoczesnym zagwarantowaniu poszanowania praw podstawowych. Z uwagi na powyższe nałożono na dostawców usług pośrednich obowiązki zapobiegania rozpowszechnianiu nielegalnych treści w internecie, w szczególności pod kątem przeciwdziałania dezinformacji, uregulowano również politykę moderowania treści, w tym funkcjonowanie niezawodnego i bezpiecznego systemu wymiany informacji, tzw. systemu AGORA[37]. Korzyści z wprowadzenia aktu o usługach cyfrowych można wyliczyć na przysłowiowych palcach jednej ręki – związane są one z „moderowaniem treści, transparentnością (w tym reklam), zwalczaniem cyberprzemocy, mechanizmami składania skarg oraz sprawozdawczością"[38]. Niewątpliwie, zważywszy na aktualność problemu, jakim jest szerzenie propagandy dezinformacyjnej w cyberprzestrzeni i jej wpływu na komunikację (e-komunikację) społeczną, należy rozważyć aktualizację procedur cyberbezpieczeństwa stron i platform internetowych.

Polityka cyberbezpieczeństwa komunikacji elektronicznej powinna uwzględniać kilka istotnych aspektów, które z uwagi na dziedzinę spraw można skategoryzować jako działania natury prawno-organizacyjnej, technologicznej i społecznej. Istotne będzie zatem zapewnienie bezpiecznego przetwarzania danych osobowych i dostępu do informacji (*a contrario* ochrony przed dezinformacją), przy jednoczesnym zachowaniu wolności prawa do wypowiedzi i pluralizmu mediów. To będzie możliwe w przypadku wdrożenia środków umożliwiających nadzór i monitoring nad treściami udostępnianymi w sieci, ale również z uwagi na inwestycje w innowacyjne rozwiązania (sztuczną inteligencję) i wzrost kompetencji cyfrowych użytkowników (cyberhigienę). Przy czym konieczna jest także

[35] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.Urz.UE.L. z 2024 r. s. 1689).

[36] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.Urz.UE.L. 2022 Nr 277, str. 1).

[37] Zob. motyw 1 i 2 preambuły rozporządzenia wykonawczego Komisji (UE) 2024/607 z dnia 15 lutego 2024 r. w sprawie ustaleń praktycznych i operacyjnych na potrzeby funkcjonowania systemu wymiany informacji na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 (akt o usługach cyfrowych) (Dz.Urz.UE.L. 2024 Nr 33, str. 607).

[38] Jaskiernia, „Pluralizm, transparentność i odpowiedzialność", 15.

zmiana społeczna, ponieważ to, czy propaganda dezinformacyjna będzie skuteczna, zależy od interpretacji, a następnie przyswojenia i uznania informacji za prawdziwą. Można powiedzieć, że „stworzenie przez odbiorcę filtra informacyjnego powoduje, że zaczyna on funkcjonować w swoistej bańce informacyjnej"[39]. Zatem te informacje, które są zgodne z jego przekonaniami, światopoglądem, uznaje za prawdziwe, nie zważając na ich wątpliwą wartość informacyjną.

Aktualnie trwają prace nad implementacją unijnego aktu o usługach cyfrowych. Równocześnie w przestrzeni publicznej pojawiają się zarzuty dotyczące nadmiernej inwigilacji oraz cenzury treści w internecie. Ministerstwo Cyfryzacji odpiera je, wskazując na konieczność przyjęcia restrykcyjnych rozwiązań z uwagi na wypracowanie mechanizmów blokowania dostępu do nielegalnych treści i zwiększenia transparentności działania platform internetowych[40]. Jest to dość ciekawe zagadnienie, ponieważ wydawałoby się, że nic tak nie gwarantuje przestrzegania zasady pluralizmu i dostępności do e-informacji, jak działalność mediów elektronicznych. Coraz częściej w dyskursie pojawia się problematyka ograniczenia wolności słowa w internecie z uwagi na przeciwdziałanie zagrożeniom czy dbałość o przejrzystość udostępnianych treści. Takie działanie oczywiście należy ocenić pozytywnie, jednakże pewne wątpliwości może powodować kontekst zastosowania tej cenzury, w szczególności taki, który będzie nosił znamiona ograniczenia wolności wypowiedzi ze względu na kwestie światopoglądowe. Krytyczne stanowisko wobec projektu ustawy wdrażającej akt o usługach cyfrowych w Rzeczypospolitej Polskiej wyraziła Krajowa Rada Radiofonii i Telewizji. Zdaniem organu zapowiedziane zmiany stanowią rażące naruszenie konstytucyjnych gwarancji wolności słowa, zapisanych w art. 54 Konstytucji Rzeczypospolitej Polskiej. Ograniczeniem prawa do informacji i wolności słowa może być reglamentowanie dostępu do platform internetowych, w tym blokowanie treści (również z uwagi na kontekst światopoglądowy), co rodzi obawę dużego pola do nadużyć i cenzury. Ponadto podaje się w wątpliwość brak nadzoru sądowego (subiektywna, arbitralna ocena treści) i gwarancji proceduralnych[41].

---

[39] Tomasz Aleksandrowicz, „Mechanizmy ataku informacyjnego. Skuteczność przeciwdziałania", w: *Dezinformacja – inspiracja – społeczeństwo. Social cybersecurity*, red. Daniel Boćkowski, Ewa Dąbrowska-Prokopowska, Patrycja Goryń i Kamil Goryń (Białystok: Wydawnictwo Uniwersytetu w Białymstoku, 2022), 14.

[40] „Prace nad ochroną użytkowników internetu – implementacja unijnego Aktu o usługach cyfrowych (DSA)", dostęp 07.04.2025, https://www.gov.pl/web/cyfryzacja/prace-nad-ochrona-uzytkownikow-internetu--implementacja-unijnego-aktu-o-uslugach-cyfrowych-dsa.

[41] „Stanowisko KRRiT w sprawie projektu ustawy wdrażającej unijne rozporządzenie, Akt o Usługach Cyfrowych (DSA), przedstawionego przez Ministerstwo Cyfryzacji (plan wprowadzenia cenzury w internecie)", dostęp 08.04.2025, https://www.gov.pl/web/krrit/stanowisko-krrit-w-sprawie-projektu-ustawy-wdrazajacej-unijne-rozporzadzenie-akt-o-uslugach-cy-

Powyższe rozważania wskazują, jak ważne jest zatem wypracowanie spójnych i transparentnych rozwiązań w zakresie ochrony przed dezinformacją i negatywnym oddziaływaniem sztucznej inteligencji na sferę komunikacji społecznej w cyberprzestrzeni. Nie zmienia to jednak faktu, że jest ono niezwykle skomplikowane z uwagi na konieczność zapewnienia ochrony praw podstawowych jednostki obejmujących prawo do informacji publicznej i wolność wypowiedzi oraz zachowania zasady pluralizmu mediów.

PODSUMOWANIE

Konkludując, nie ulega wątpliwości, że technologie informacyjno-komunikacyjne mają istotne znaczenie w obszarze komunikacji (e-komunikacji) społecznej. W dobie cyfryzacji charakteryzuje się ona dostępnością, personalizacją oraz szybkością przetwarzania treści. Ponadto interoperacyjność usług elektronicznych sprzyja zainteresowaniu społeczeństwa korzystaniem z takiej formy przetwarzania danych. Niemniej jednak oprócz niewątpliwie szczególnych walorów e-komunikacji, należy również zwrócić uwagę na potencjalne cyberzagrożenia w zakresie dostępu do informacji, wolności słowa czy pluralizmu mediów. Cyberzagrożenia procesów komunikacji społecznej mogą przybierać różne formy, takie jak m.in. *phishing* czy *spyware*, i w rezultacie wpływać na autentyczność oraz transparentność przekazywanych informacji. W ostatnich latach zauważa się ponadprzeciętną intensyfikację działań dezinformacyjnych, co w połączeniu z algorytmizacją usług utrudnia dostęp do wiarygodnej i rzetelnej informacji, powoduje chaos informacyjny. W tym kontekście kluczowym zagadnieniem jest określenie zasad cyberbezpieczeństwa komunikacji społecznej.

Warunkiem *sine qua non* bezpiecznej komunikacji społecznej w świecie cyfrowym jest zatem stworzenie optymalnych rozwiązań natury prawno-technologicznej, których celem będzie ochrona prawdy informacyjnej i wolności słowa w internecie. Nie można zapomnieć o tym, że polityka cyberbezpieczeństwa *per se* nie uchroni użytkowników przed dezinformacją. Jak pisze Rafał Ziemkiewicz, algorytm „to tylko potężny wzmacniacz, podchwytujący oczekiwania poddanych cyberprzestrzennego królestwa (…)”[42]. Dlatego też warto postulować wzmocnienie kompetencji cyfrowych użytkowników cyberprzestrzeni w kwestii analizy, interpretacji i ustalenia wartości informacyjnej przekazu online. Z kolei

frowych-dsa-przedstawionego-przez-ministerstwo-cyfryzacji-plan-wprowadzenia-cenzury-w-internecie.

[42] Rafał Ziemkiewicz, *Strollowana rewolucja* (Lublin–Warszawa: Wydawnictwo Fabryka Słów, 2021), 79.

w związku z wprowadzaniem nowych rozwiązań prawnych, w tym implementacji unijnego aktu o usługach cyfrowych do porządku krajowego, należy zachować harmonizację działań pomiędzy stosowaniem mechanizmów blokowania dostępu do nielegalnych czy nieprawdziwych treści a zapewnieniem wolności wypowiedzi i pluralizmu mediów. Reasumując, istnieje dość cienka granica pomiędzy prawem dostępu do informacji a reglamentacją treści w internecie, ochroną przed dezinformacją a cenzurą. Z tego względu przepisy muszą w sposób konkretny i kompleksowy określać warunki, cele i sposoby zapewnienia cyberbezpiecznej komunikacji społecznej w dobie dezinformacji i sztucznej inteligencji.

BIBLIOGRAFIA

Adamski, Andrzej. *Media w analogowym i cyfrowym świecie. Wpływ cyfrowej rewolucji na rekonfigurację komunikacji społecznej*. Warszawa: Dom Wydawniczy Elipsa, 2012.

Aleksandrowicz, Tomasz. „Mechanizmy ataku informacyjnego. Skuteczność przeciwdziałania". W: *Dezinformacja – inspiracja – społeczeństwo. Social cybersecurity*, red. Daniel Boćkowski, Ewa Dąbrowska-Prokopowska, Patrycja Goryń i Kamil Goryń, 11-33. Białystok: Wydawnictwo Uniwersytetu w Białymstoku, 2022.

Bugajski, Jarosław. „Sztuczna inteligencja – zagrożenie czy bezpieczeństwo?". *Zbliżenia Cywilizacyjne* 19, nr 3 (2023):31-59. DOI:10.21784/ZC.2023.015.

Dobrzeniecki, Karol. „Post-prawda jako zagrożenie dla podstaw etycznych społeczeństwa informacyjnego". W: *Internet. Strategie bezpieczeństwa*, red. Agnieszka Gryszczyńska i Grażyna Szpor, 175-184. Warszawa: C.H. Beck, 2017.

Flak, Łukasz. „Między demonizacją a apoteozą – krytyczny przegląd naukowy odnośnie mediów cyfrowych". *Kultura – Media – Teologia* 4, nr 48 (2021):102-126. DOI:10.21697/kmt.48.5.

Garwol, Katarzyna i Krystian Bieś. „Seniorzy w świecie mediów XXI wieku". *Dydaktyka Informatyki* 17 (2022):19-32. DOI:10.15584/di.2022.17.3.

Grochowski, Robert. „Ekspansywny wpływ cyberprzestrzeni na tożsamość człowieka". *Fides, Ratio et Patria. Studia Toruńskie* 9 (2018):51-64. DOI:10.56583/frp.1551.

Gryszczyńska, Agnieszka. „Wykorzystanie sztucznej inteligencji w cyberatakach". W: *Internet. Hacking*, red. Agnieszka Gryszczyńska, Grażyna Szpor i Wojciech R. Wiewiórowski, 211-220. Warszawa: C.H. Beck, 2023.

Igielska, Aleksandra. „Wielki Brat patrzy. Sztuczna inteligencja w obliczu ochrony praw człowieka". W: *Dialog sądowy w sferze praw człowieka*, red. Bartłomiej Oręziak, 67-89. Warszawa: Wydawnictwo Naukowe Uniwersytetu Kardynała Stefana Wyszyńskiego, 2022.

Jaskiernia, Alicja. „Pluralizm, transparentność i odpowiedzialność. Nowe regulacje Unii Europejskiej w obszarze mediów i technologii cyfrowych". *Studia Medioznawcze* 25, nr 1/96 (2024):13-23.

Jaskuła, Lidia. „Prawo prasowe w poszukiwaniu prawdy". W: *Prawo w poszukiwaniu prawdy, dobra i piękna. Księga Jubileuszowa ks. prof. Sławomira Fundowicza*, red. Paweł Świtał, Bartosz Kuś i Emilia Gulińska, 249-262. Radom: Sieć Badawcza Łukasiewicz – Instytut Technologii Eksploatacji, 2024.

Kłos, Paweł. „Cywilizacja informacyjna a prawo – preliminaria". W: *Horyzonty Informacji 5*, red. Paloma Korycińska, 27-37. Kraków: Uniwersytet Jagielloński, Biblioteka Jagiellońska, 2023.

Lubasz, Dominik. „Zasady legalności, przejrzystości i minimalizacji danych w ogólnym rozporządzeniu o ochronie danych osobowych w kontekście sztucznej inteligencji". W: *Prawo sztucznej inteligencji*, red. Luigi Lai i Marek Świerczyński, 173-186. Warszawa: C.H. Beck, 2020.

Łukasik-Turecka, Agnieszka. „Boty w służbie dezinformacji". *Polityka i Społeczeństwo* 4, nr 22 (2024):136-146. DOI:10.15584/polispol.2024.4.9.

Marzec, Dominika. „Znaczenie influencer marketingu w kształtowaniu decyzji współczesnych konsumentów". *Media i Społeczeństwo* 16 (2022):154-174. DOI:10.53052/MiS.2022.16.10.

Omieczyńska, Sandra. „Komunikacja w cyberprzestrzeni – wyzwania, bariery i korzyści". W: *Communication as a factor of transparency of social interaction: psychological, historical, legal, economic and political dimensions*, red. Jacek Mrozek, Oksana Koval i Krystyna Ziółkowska, 399-410. Ełk: Centrum Badań Europy Wschodniej UWM w Olsztynie, 2022.

Pieczyński, Maciej. „Zielona granica propagandy". Dostęp: 05.04.2025. https://dorzeczy.pl/opinie/486645/pieczynski-zielona-granica-propagandy.html.

Połowin, Anita. „Cyberzagrożenia w internecie – analiza przypadków". *Cybersecurity and Law* 2, nr 12 (2024):117-130. DOI:10.35467/cal/188563.

„Prace nad ochroną użytkowników internetu – implementacja unijnego Aktu o usługach cyfrowych (DSA)". Dostęp 07.04.2025. https://www.gov.pl/web/cyfryzacja/prace-nad-ochrona-uzytkownikow-internetu--implementacja-unijnego-aktu-o-uslugach-cyfrowych-dsa.

Rogowski, Sławomir. „Pojęcie społeczeństwa kontentowego a problematyka kultury nadmiaru". *Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie* 53 (2024):93-103. DOI:10.17512/znpcz.2024.1.08.

Skoczylas, Dominika. „Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe". *Prawo w Działaniu. Sprawy karne* 53 (2023):97-113. DOI:10.32041/pwd.5306.

Skoczylas, Dominika. „Sztuczna inteligencja a dobrostan człowieka i ochrona praw podstawowych – rozważania na gruncie aktu w sprawie sztucznej inteligencji". *Studia Prawnoustrojowe* 67 (2025):353-367. DOI:10.31648/sp.10403.

Snopkiewicz, Konrad. „Przegląd zagrożeń w cyberprzestrzeni". *Studia Administracji i Bezpieczeństwa* 9 (2020):29-41.

„Stanowisko KRRiT w sprawie projektu ustawy wdrażającej unijne rozporządzenie, Akt o Usługach Cyfrowych (DSA), przedstawionego przez Ministerstwo Cyfryzacji (plan wprowadzenia cenzury

w internecie)". Dostęp 08.04.2025. https://www.gov.pl/web/krrit/stanowisko-krrit-w-sprawie-projektu-ustawy-wdrazajacej-unijne-rozporzadzenie-akt-o-uslugach-cyfrowych-dsa-przedstawionego-przez-ministerstwo-cyfryzacji-plan-wprowadzenia-cenzury-w-internecie.

Szczygielska, Agnieszka. „Konflikt hybrydowy – analiza porównawcza źródeł wiedzy o zjawisku". *Roczniki Nauk Społecznych* 15/51, nr 2 (2023):31-48. DOI:10.18290/rns2023.002232.

Szpor, Grażyna. „Dezinformacja". W: *Wielka Encyklopedia Prawa. Tom XXII – Prawo informatyczne*, red. Brunon Hołyst, 109-110. Warszawa: Fundacja „Ubi societas, ibi ius", 2021.

Warchoł, Tomasz. „Edukacja pozaformalna wsparciem edukacji w społeczeństwie informacyjnym". *Polityka i Społeczeństwo* 2, nr 21 (2023):257-269. DOI:10.15584/polispol.2023.2.17.

Wróblewski, Tomasz. „Sztuczna inteligencja jako narzędzie do walki z dezinformacją". *International Journal of Legal Studies* 1, nr 17 (2024):149-166. DOI10.5604/01.3001.0054.6967.

Zaręba, Agnieszka. „Dezinformacja jako zagrożenie hybrydowe cyberbezpieczeństwa społecznego (social cyberseciurity)". *Cybersecurity and Law* 1/13 (2025):95-107.

Ziemkiewicz, Rafał. *Strollowana rewolucja*. Lublin–Warszawa: Wydawnictwo Fabryka Słów, 2021.

„CYBERBEZPIECZNA" KOMUNIKACJA SPOŁECZNA W DOBIE DEZINFORMACJI I SZTUCZNEJ INTELIGENCJI

Streszczenie

Celem artykułu jest wskazanie roli, jaką pełnią technologie informacyjno-komunikacyjne w obszarze komunikacji społecznej. Uznając szczególne walory innowacyjnych rozwiązań teleinformatycznych, należy dokonać analizy potencjalnych cyberzagrożeń dla bezpieczeństwa komunikacji (e-komunikacji). W sytuacjach nadzwyczajnych może dojść do naruszenia prawa dostępu do informacji, wolności słowa czy pluralizmu mediów. Przedmiotem artykułu jest określenie zasad cyberbezpieczeństwa komunikacji społecznej w dobie dezinformacji i sztucznej inteligencji. Analiza tematu pozwoli odpowiedzieć na pytanie o zasadność wdrożenia tzw. polityk cyberbezpieczeństwa w komunikacji społecznej. Konieczne jest stworzenie optymalnych rozwiązań natury prawno-technologicznej, które z jednej strony zapewnią ochronę prawdy informacyjnej, z drugiej utrwalą działania na rzecz e-partycypacji społecznej i wolności słowa w internecie. Niewątpliwe w związku z algorytmizacją usług wzrasta potrzeba ochrony przed dezinformacją, tym samym ważne stają się kompetencje cyfrowe użytkowników cyberprzestrzeni. W opracowaniu omawia się zagadnienia odnoszące się do istoty cyberbezpieczeństwa w komunikacji społecznej, co pozwala na określenie standardów cyberbezpieczeństwa e-komunikacji. Przyjęta metoda badawcza obejmuje analizę podstawowych aktów prawnych oraz literatury przedmiotu.

Słowa kluczowe: cyberbezpieczeństwo; cyberzagrożenie; dezinformacja; informacja; komunikacja społeczna; sztuczna inteligencja; wolność słowa

„CYBERSECURE" SOCIAL COMMUNICATION IN THE AGE OF DISINFORMATION AND ARTIFICIAL INTELLIGENCE

Summary

The aim of this article is to identify the role played by ICT in the area of social communication. Recognising the particular virtues of innovative ICT solutions, it is necessary to analyse potential cyberthreats to the security of communication (e-communication). In extraordinate situations, the right of access to information, freedom of speech or media pluralism may be violated. The subject of this article is to define the principles of cybersecurity of social communication in the age of disinformation and artificial intelligence. By analysing the topic, the question of the legitimacy of the implementation of so-called cybersecurity policies in social communication will be answered. It is necessary to create optimal solutions of a legal-technological nature which, on the one hand, will ensure the protection of information truth and, on the other hand, will consolidate measures for social e-participation and freedom of speech on the Internet. Undoubtedly, due to the algorithmisation of services, the need to protect against disinformation is increasing, thus the digital competence of the users of cyberspace is becoming an important issue. The paper will discuss issues relating to the essence of cybersecurity in social communication, thus identifying standards for cybersecurity of e-communication. The research method adopted include an analysis of basic legal acts and the literature on the subject.

Keywords: cybersecurity; cyberthreat; disinformation; information; social communication; artificial intelligence; freedom of speech