
Dorota Hołub

ORCID: 0009-0005-0144-4038

Człowiek w cyberprzestrzeni – między wolnością a bezpieczeństwem. Ujmowanie problemu w USA

Wstęp

Obszarem aktywności człowieka, w którym szczególnie istotne staje się jego bezpieczeństwo, jest cyberprzestrzeń. W realiach idei Web 2.0 jednostka zajmuje w niej wyjątkową pozycję, stając się nie tylko użytkownikiem, lecz także współtwórcą tej rzeczywistości. Paradoksalnie globalne zagrożenie związane z pandemią COVID-19 sprawiło, że wirtualna rzeczywistość 2.0 stała się dla człowieka jeszcze atrakcyjniejszym środowiskiem aktywności. Jak każde miejsce, także i to niesie ze sobą określone zagrożenia dla bezpieczeństwa użytkownika. Rządy starają się regulować funkcjonowanie cyberprzestrzeni ze względu na bezpieczeństwo obywateli oraz państwa. Działania te mogą jednak prowadzić do ograniczenia swobody i wolności jednostki w internecie. W efekcie pojawia się trudny do rozwiązania dylemat między wolnością a bezpieczeństwem. Rodzi się więc pytanie: **czy regulowanie cyberprzestrzeni skutkuje zwiększeniem poziomu bezpieczeństwa człowieka w internecie, czy raczej głównym skutkiem jest ograniczenie ludzkiej ekspresji, wyrażania poglądów, ocen czy samego siebie?** Z tym zagadnieniem wiąże się również inne pytanie: **czy w imię bezpieczeństwa warto ograniczać wolność jednostki w cyberprzestrzeni?** W niniejszym artykule podjęto próbę odpowiedzi na powyższe pytania poprzez krytyczną

analizę amerykańskich aktów prawnych dotyczących funkcjonowania i wykorzystywania cyberprzestrzeni.

Znaczenie pierwszej poprawki

Podstawowe ramy wolności w USA zostały wyznaczone w treści pierwszych dziesięciu poprawek do Konstytucji Stanów Zjednoczonych, w szczególności pierwszej (Amendment I). Jej zapis, dotyczący ochrony wolności słowa i wyrażania opinii, obejmuje również cyberprzestrzeń. Zgodnie z tą zasadą jednostka posiada w internecie wolność wypowiedzi: ma prawo dzielić się swoimi myślami, opiniami i pomysłami w mediach społecznościowych, na stronach internetowych, blogach czy forach bez obawy przed państwową cenzurą. Władza nie może zakazywać czytania, oglądania ani słuchania treści publikowanych w witrynach internetowych, takich jak artykuły prasowe czy materiały audiowizualne. Dotyczy to także działalności mediów masowych, pod warunkiem że ich przekaz pozostaje zgodny z obowiązującym prawem. Ponadto, zgodnie z prawem do składania petycji oraz organizowania zgromadzeń, ludzie mogą wykorzystywać internet do organizowania się, uczestnictwa w inicjatywach społecznych (ruchach, stowarzyszeniach, organizacjach) oraz do wyrażania sprzeciwu wobec kwestii, z którymi się nie zgadzają.

Warto jednak zaznaczyć, że władze mogą interweniować w odniesieniu do wskazanych wolności, jeżeli treści publikowane w cyberprzestrzeni naruszają prawo, na przykład poprzez nawoływanie do przemocy, szerzenie mowy nienawiści czy zniesławienie¹.

Wolnościowe zasady pierwszej poprawki — zakazujące m.in. stosowania cenzury — ograniczają wyłącznie działania podmiotów państwowych na szczeblu federalnym i stanowym. Platformy mediów społecznościowych są natomiast podmiotami niepaństwowymi, a więc mogą zgodnie z prawem ustanawiać własne regulaminy i wytyczne, w tym moderować lub usuwać treści, a nawet blokować użytkowników².

W świetle pierwszej poprawki zabezpieczeniu przed odpowiedzialnością nadawców (właścicieli) treści internetowych za blokowanie na ich stronach (witrynach) nieodpowiednich materiałów służy art. 230 ustawy o telekomunikacji z 1996 roku (*Communications Decency Act*, Ustawa o przyzwoitości

¹ J. Horowitz (2021, 9 marca). *First Amendment, Censorship, and Private Companies: What Does „Free Speech” Really Mean?* Carnegie Library of Pittsburgh. <https://www.carnegielibrary.org/pl/the-first-amendment-and-censorship/> [dostęp: 20.02.2025].

² C. Newton (2020, 29 grudnia). *Everything you need to know about Section 230. The Verge*. <https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation> [dostęp: 20.02.2025].

w komunikacji)³. Zgodnie z zapisami tego artykułu podmioty te nie ponoszą odpowiedzialności za „(A) jakiekolwiek działanie podejmowane dobrowolnie w dobrej wierze w celu ograniczenia dostępu do materiałów lub ich dostępności, które dostawca lub użytkownik uważa za obsceniczne, lubieżne, wyuzdane, obrzydliwe, nadmiernie brutalne, nękające lub w inny sposób budzące sprzeciw, niezależnie od tego, czy takie materiały są chronione konstytucyjnie; lub (B) jakiekolwiek działanie podjęte w celu umożliwienia lub udostępnienia) dostawcom treści informacyjnych lub innym osobom środków technicznych ograniczających dostęp do materiałów opisanych w ust. 1”⁴. Ponadto artykuł ten chroni dostawców oraz użytkowników interaktywnych usług komputerowych przed traktowaniem ich jako wydawców lub autorów informacji dostarczonych przez innego dostawcę treści informacyjnych. Dzięki temu właściciele stron internetowych są zabezpieczeni przed pozwami w przypadku publikacji przez użytkowników treści nielegalnych, z wyjątkiem materiałów naruszających federalne prawo karne, w tym dotyczących naruszenia praw autorskich oraz pornografii⁵. Należy zwrócić uwagę, że amerykański ustawodawca duży nacisk kładzie na ochronę nieletnich przed dostępem do materiałów pornograficznych. Służą temu również zapisy Ustawy o Ochronie Prywatności Dzieci w Internecie (*Children’s Online Privacy Protection Act*, COPPA) z 1998 roku, zgodnie z którą operatorzy są zobowiązani do uzyskania zgody rodziców przed jakimkolwiek zbieraniem, wykorzystywaniem lub ujawnianiem danych osobowych dzieci. Obejmuje to również konieczność uzyskania zgody na wszelkie istotne zmiany w praktykach dotyczących gromadzenia, wykorzystywania lub ujawniania danych⁶. Ochronie prywatności wiadomości e-mail poświęcona została tzw.

³ Ustawa ta zmieniała Ustawę o komunikacji (*Communications Act*) z 1934 roku. Zob. *Communications Act of 1934*. <https://transition.fcc.gov/Reports/1934new.pdf> [dostęp: 20.02.2025].

⁴ *Ibidem*. Zgodnie z wykładnią Federalnej Komisji Komunikacji (*Federal Communications Commission*, FCC) pojęcia te definiuje się następująco: „Aby treść została uznana za obsceniczną, musi spełniać trzyczęściowy test ustalony przez Sąd Najwyższy: musi odpowiadać lubieżnym zainteresowaniom przeciętnej osoby; przedstawiać lub opisywać zachowanie seksualne w sposób »oczywiście obraźliwy« i jako całość nie mieć poważnej wartości literackiej, artystycznej, politycznej lub naukowej. Treści nieprzystoite przedstawiają narządy lub czynności seksualne lub wydalinicze w sposób, który jest ewidentnie obraźliwy, ale nie spełnia potrójnego testu obsceniczności. Do treści wulgarnych zalicza się język »rażąco obraźliwy«, który jest uznawany za uciążliwy dla społeczeństwa”. *Obscene, Indecent and Profane Broadcasts* (2021, 13 stycznia). *Federal Communications Commission*. <https://www.fcc.gov/consumers/guides/obscene-indecent-and-profane-broadcasts> [dostęp: 20.02.2025].

⁵ C. Newton (2020, 29 grudnia). *Everything you need...* Op. cit.

⁶ *Children’s Online Privacy Protection Rule. The Code of Federal Regulations*. <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312> [dostęp: 20.02.2025].

Ustawa o Przechowywanej Komunikacji (*Stored Communications Act, SCA*) stanowiąca część przyjętej w 1986 roku Ustawy o Prywatności Komunikacji Elektronicznej (*Electronic Communications Privacy Act, ECPA*).

Linia orzecznicza Sądu Najwyższego USA

Przykładem istnienia wątpliwości dotyczących zakresu ochrony wolności są sprawy, które toczyły się i toczą przed Sądem Najwyższym USA, w tym w szczególności dotyczące treści umieszczanych na forach społecznościowych.

Pierwszym przypadkiem dotyczącym mediów społecznościowych, który trafił do Sądu Najwyższego USA w 2017 roku, była sprawa *Lestera Packinghama przeciwko Karolinie Północnej*⁷. Skarżący był osobą skazaną wcześniej za przestępstwo o charakterze seksualnym. Został aresztowany za naruszenie prawa stanu, które uniemożliwiało przestępcy seksualnemu dostęp do serwisów społecznościowych, a polegało to na umieszczeniu na własnym profilu na Facebooku postu, w którym oskarżony dziękował Bogu za anulowanie mandatu za wykroczenie drogowe. Packingham argumentował, że ustawa narusza jego prawa gwarantowane przez pierwszą poprawkę. Ostatecznie Sąd Najwyższy USA uznał: „Prawo stanu Karolina Północna, zabraniające zarejestrowanym przestępcom seksualnym dostępu do różnych stron internetowych, na których nieletni są aktywni i mają konta, niezależnie od tego, czy przestępca seksualny wszedł bezpośrednio w interakcję z nieletnim, narusza pierwszą poprawkę”⁸.

Gdy w 2015 roku członkowie Państwa Islamskiego w Iraku i Syrii (ISIS) dokonali zamachu terrorystycznego w Paryżu, w którym zginął m.in. Nohemi Gonzalez, jego rodzina wystąpiła z oskarżeniem przeciwko Google. Zarzucano firmie bezpośrednią i wtórną odpowiedzialność za atak terrorystyczny oraz akceptację filmów ISIS umieszczanych na należącej do Google platformie YouTube. Sąd jednak orzekł, że platformy internetowe nie ponoszą odpowiedzialności za treści publikowane przez użytkowników⁹.

Podobna sprawa dotyczyła zamachu terrorystycznego dokonanego w Stambule w 2017 roku. Jedną z ofiar był Nawras Allassaf, którego rodzina złożyła pozew przeciwko platformom społecznościowym: Facebook Inc., Google Inc. i Twitter Inc., oskarżając te podmioty o „udzielenie znacznej pomocy ISIS w przeprowadzeniu tego aktu międzynarodowego terroryzmu”.

⁷ *Packingham v. North Carolina* (2017). Oyez. <https://www.oyez.org/cases/2016/15-1194> [dostęp: 20.02.2025].

⁸ *Ibidem*.

⁹ D. Dwyer, P. See (2023, 21 lutego). *Family of American terror victim asks Supreme Court to curb immunity for social media*. ABC News. <https://abcnews.go.com/Politics/family-american-terror-victim-asks-supreme-court-curb/story?id=96463560> [dostęp: 20.02.2025].

Jednocześnie rodzina zabitego twierdziła, że wiedziały one, iż „ISIS używa ich platform do rekrutowania ludzi i zbierania funduszy na przeprowadzanie ataków, przy czym nie wykryły i nie usunęły ich kont, postów i filmów”. Ponadto respondenci twierdzili, że algorytm „rekomendacji” tych firm dopasowywał treści ISIS do użytkowników, którzy prawdopodobnie byliby zainteresowani ich postami¹⁰. W 2023 roku Sąd Najwyższy stwierdził w tej sprawie, że „fakt, iż niektórzy źli aktorzy wykorzystali te platformy, nie był wystarczający, aby stwierdzić, że oskarżeni świadomie udzielili znacznej pomocy, a tym samym pomogli i podlegali do czynów tych przestępców”. W opiniach dotyczących tego orzeczenia wskazano, iż ma ono duże znaczenie, gdyż wzmacnia zasadę, że platformy internetowe nie powinny ponosić ciężaru monitorowania i cenzurowania treści generowanych przez użytkowników. Uznano, że taka interpretacja przyczynia się do ochrony wolności słowa użytkowników internetu i pozwala uniknąć nadmiernej odpowiedzialności przez podmioty świadczące usługi komunikacyjne lub pośredników¹¹.

Pozwy przeciwko platformom społecznościowym składane są również przez instancje stanowe. W 2023 roku Meta (Facebook) zgodziła się zapłacić odszkodowanie w ramach ugody w sprawie naruszenia prywatności użytkowników Facebooka. W 2022 roku prokurator generalny Teksasu Ken Paxton złożył pozew przeciwko Mecie, zarzucając jej nielegalne gromadzenie i wykorzystywanie danych biometrycznych mieszkańców stanu bez ich zgody, co naruszało ich prawo do prywatności¹². Dane te miały służyć funkcjonowaniu systemu rozpoznawania twarzy. W 2022 roku, wskutek pozwu złożonego przez czterdzieści stanów przeciwko Google w związku z naruszeniem prawa do prywatności poprzez lokalizowanie użytkowników bez ich zgody, firma zgodziła się wypłacić odpowiednie odszkodowanie. Podkreślano przy tym, że działanie to naruszało prawo do prywatności oraz było wykorzystywane przez policję w celu określenia miejsca pobytu przestępców¹³.

Po śledztwie wszczętym w 2021 roku ponad trzydzieści stanów USA, w tym Nowy Jork i Kalifornia, złożyło w październiku 2023 roku federalny

¹⁰ *Twitter v. Taamneh* (2023). Global Freedom of Expression. <https://globalfreedomofexpression.columbia.edu/cases/twitter-v-taamneh/> [dostęp: 20.02.2025].

¹¹ *Twitter Inc, v Taamneh et al* (2023). Sąd Najwyższy USA. https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf [dostęp: 20.02.2025].

¹² *Attorney General Ken Paxton Secures \$1.4 Billion Settlement with Meta Over Its Unauthorized Capture of Personal Biometric Data in Largest Settlement Ever Obtained from An Action Brought by A Single State* (2024, 30 lipca). Texas Office of the Attorney General. <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture> [dostęp: 20.02.2025].

¹³ *40 states settle Google location-tracking charges for \$392M* (2022, 14 listopada). Independent. <https://www.independent.co.uk/news/google-ap-princeton-b2224868.html> [dostęp: 20.02.2025].

pozew zbiorowy przeciwko firmie Meta Platforms Inc. (Facebook, Instagram). Oskarżono ją o celowe projektowanie swoich platform w sposób uzależniający dla dzieci i młodzieży, co przyczynia się do pogorszenia ich zdrowia psychicznego. Dodatkowo zarzucano firmie nielegalne gromadzenie danych osobowych dzieci poniżej 13. roku życia bez zgody rodziców, co narusza federalne przepisy dotyczące ochrony prywatności dzieci w internecie. W pozwie wskazano, że Meta zlekceważyła swoje obowiązki wynikające z COPPA, nielegalnie gromadząc dane osobowe swoich najmłodszych użytkowników bez zgody ich rodziców. Ponadto Meta reklamowała i kierowała swoje platformy mediów społecznościowych do dzieci poniżej 13. roku życia, będąc jednocześnie świadoma, że dzieci te korzystają z jej usług¹⁴.

Interesującym przypadkiem dotyczącym ochrony wolności jednostek oraz bezpieczeństwa narodowego w USA jest funkcjonowanie społecznościowego medium TikTok na terenie tego kraju. Oprócz problemu zagrożeń dla bezpieczeństwa USA ze strony chińskiego podmiotu, którego właścicielem jest ByteDance Ltd., podkreśla się naruszanie przepisów o prywatności dzieci poniżej 13. roku życia. W związku z tym w 2024 roku Departament Sprawiedliwości wspólnie z Federalną Komisją Handlu (FTC) złożył pozew cywilny w amerykańskim sądzie okręgowym dla Centralnego Okręgu Kalifornii przeciwko TikTok Inc., ByteDance Ltd. i ich podmiotom za naruszenie ustawy o ochronie prywatności dzieci w internecie¹⁵.

Wcześniej, z obawy o bezpieczeństwo danych amerykańskich urzędników, do których dostęp mogła potencjalnie uzyskać strona chińska, uchwalono w grudniu 2022 roku *No TikTok on Government Devices Act*. Ustawa wymagała usunięcia aplikacji TikTok z systemów informatycznych agencji federalnych oraz z telefonów i komputerów. Ponadto poszczególne stany USA mogły wprowadzać własne, rozszerzone zakazy korzystania z TikToka na urządzeniach rządowych.

Najbardziej istotnym działaniem zmierzającym do neutralizacji zagrożeń związanych z funkcjonowaniem TikToka w USA było uchwalenie w 2024

¹⁴ *Final Meta Multistate Complaint*, N.D. Cal. (2023). State of California Department of Justice – Office of the Attorney General. <https://oag.ca.gov/system/files/attachments/press-docs/FINAL%20Meta%20Multistate%20Complaint%2C%20N.D.%20Cal.%20%28REDACTED%2C%20CONFORMED%29.pdf> [dostęp: 20.02.2025].

¹⁵ *Justice Department Sues TikTok and Parent Company ByteDance for Widespread Violations of Children's Privacy Laws* (2024, 2 sierpnia). U.S. Department of Justice. <https://www.justice.gov/archives/opa/pr/justice-department-sues-tiktok-and-parent-company-bytedance-widespread-violations-childrens> [dostęp: 20.02.2025]; *UNITED STATES OF AMERICA, Plaintiff, v. BYTEDANCE LTD., a Cayman Islands company; BYTEDANCE INC., a Delaware corporation; TIKTOK LTD., a Cayman Islands company; TIKTOK INC., a California corporation; TIKTOK PTE. LTD., a Singapore company; and TIKTOK U.S. DATA SECURITY INC., a Delaware corporation.* <https://www.justice.gov/archives/opa/media/1362606/> [dostęp: 20.02.2025].

roku ustawy *An Act to protect the national security of the United States from the threat posed by foreign adversary controlled applications, such as TikTok and any successor application or service and any other application or service developed or provided by ByteDance Ltd. or an entity under the control of ByteDance Ltd.* Zgodnie z jej zapisami zabraniano dystrybucji, utrzymywania lub świadczenia usług hostingu internetowego dla zagranicznych aplikacji kontrolowanych przez przeciwnika¹⁶. TikTok zakwestionował ustawę, powołując się na pierwszą poprawkę, gdyż — zdaniem strony — akt ograniczał wolność uczestniczenia w publicznej przestrzeni. Jednakże Sąd Najwyższy USA uznał w styczniu 2025 roku, że akt ten nie narusza pierwszej poprawki¹⁷. Z kolei prezydent Donald Trump 20 stycznia 2025 roku podpisał rozporządzenie wykonawcze wstrzymujące zakaz działania TikToka na 75 dni, „aby dać (...) administracji możliwość określenia właściwego sposobu postępowania w odniesieniu do TikToka”. Wcześniej zasugerował, aby ByteDance przekształcił platformę w spółkę *joint venture* kontrolowaną w co najmniej 50% przez interesy amerykańskie¹⁸.

Bezpieczeństwo państw oraz danych osobowych urzędników było przyczyną wprowadzenia częściowych zakazów korzystania z TikToka na urządzeniach służbowych pracodawców, urzędników państwowych i innych pracowników w Wielkiej Brytanii, Australii, Austrii, Belgii, Kanadzie, Danii, Estonii, Francji, Holandii, Łotwie, Irlandii, Nowej Zelandii, Norwegii i na Maltcie¹⁹. Przeciwko TikTokowi w grudniu 2024 roku Komisja Europejska wszczęła postępowanie w związku z obawami o wykorzystywanie platformy do ingerowania w wybory prezydenckie w Rumunii. Postępowanie miało dotyczyć systemów rekomendacji TikToka, w szczególności ryzyka związanego ze skoordynowaną nieautentyczną manipulacją lub zautomatyzowaną

¹⁶ *Protecting Americans from Foreign Adversary Controlled Applications Act*. Kongres Stanów Zjednoczonych. <https://www.congress.gov/bill/118th-congress/house-bill/7521/text> [dostęp: 20.02.2025].

¹⁷ M. Zahn (2024, 6 grudnia). *Federal appeals court rejects TikTok's bid to overturn US ban*. ABC News. <https://abcnews.go.com/Business/tiktok-loses-challenge-law-requiring-sale-ban/story?id=116527211> [dostęp: 20.02.2025].

¹⁸ A. Pequeño, M.W. Roeloffs (2025, 14 lutego). *TikTok Ban Timeline: TikTok Returns to U.S. App Stores — For Now*. Forbes. <https://www.forbes.com/sites/antoniopequenoi/2025/02/14/tiktok-ban-timeline-tiktok-returns-to-us-app-stores-for-now/> [dostęp: 20.02.2025]; *Application of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok* (2025, 20 stycznia). White House. <https://www.whitehouse.gov/presidential-actions/2025/01/application-of-protecting-americans-from-foreign-adversary-controlled-applications-act-to-tiktok/> [dostęp: 20.02.2025].

¹⁹ N. Bhalla (2025, 14 lutego). *US TikTok ban: Which other countries have banned the app?* Context. <https://www.context.news/big-tech/us-tiktok-ban-which-other-countries-have-banned-the-app> [dostęp: 20.02.2025].

eksploatacją usługi, a także polityką TikToka w zakresie reklam politycznych i płatnych treści politycznych²⁰.

Regulacją, która bezpośrednio dotyczyła bezpieczeństwa państwa, była uchwalona po atakach terrorystycznych z 11 września 2001 roku ustawa *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* z 2001 roku (Patriot Act)²¹. Jej zapisy ograniczały przede wszystkim ochronę prywatności użytkowników cyberprzestrzeni. Umożliwiała pozyskiwanie informacji o użytkownikach internetu bez ich wiedzy. Artykuł 215 pozwalał Federalnemu Biuru Śledczemu (FBI) na uzyskanie dostępu do danych osobowych, w tym historii przeglądania, zapisów bankowych oraz informacji telekomunikacyjnych, bez konieczności wykazywania podejrzenia przestępstwa. Natomiast art. 505 umożliwiał żądanie informacji o użytkownikach od firm internetowych bez konieczności zgody sądu, przy czym podmioty objęte takim żądaniem miały zakaz informowania użytkowników o tym, że ich dane zostały przekazane służbom. Ustawa Patriot Act wygasła w 2015 roku, a zawarte w niej rozwiązania w formie zreformowanej znalazły się w uchwalonej w tym samym roku ustawie *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act* z 2015 r. (znanej pod skróconą nazwą jako akronim pełnego tytułu – Freedom Act). Akty te stanowią przykład konieczności ograniczania wolności człowieka (prywatności) na rzecz ogólnego bezpieczeństwa narodowego.

Powyższe, wybrane rozwiązania normatywne wskazują na dwa główne problemy dotyczące wolności jednostki w aspekcie jej bezpieczeństwa oraz bezpieczeństwa ogólnonarodowego (państwa). Do najważniejszych kwestii należą: wolność dostępu i korzystania z cyberprzestrzeni, w tym z aplikacji i platform społecznościowych; wolność wypowiedzi; zachowywania prywatności; ochrony nieletnich przed treściami nieodpowiednimi (np. pornografią) oraz ochrony danych osobowych, w tym danych biometrycznych. Z drugiej strony istotnym problemem pozostaje ochrona bezpieczeństwa państwa przed zagrożeniami związanymi z wykorzystaniem cyberprzestrzeni do działalności przestępczej, w tym terrorystycznej. Kwestia ta stanowi podstawowy wektor działań instytucji państwowych, które podejmują działania inwigilacyjne wobec obywateli, a tym samym ograniczające ich prawo do prywatności.

²⁰ *Commission opens formal proceedings against TikTok on election risks under the Digital Services Act* (2024, 17 grudnia). Komisja Europejska. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487 [dostęp: 20.02.2025].

²¹ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*. Kongres Stanów Zjednoczonych. <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm> [dostęp: 20.02.2025].

Rola organizacji pozarządowych w ochronie wolności w cyberprzestrzeni

Spółeczeństwo obywatelskie, starając się, by instytucje państwa nie nadużywały swoich uprawnień do ograniczania wolności człowieka, w tym w cyberprzestrzeni, podejmuje szereg inicjatyw organizacyjnych, tworząc odpowiednie podmioty (stowarzyszenia, fundacje). Szeroką działalność na rzecz praw i wolności prowadzi w USA Amerykańska Unia Swobód Obywatelskich (American Civil Liberties Union, ACLU). Prawa i wolności w internecie stanowią jeden z obszarów jej aktywności²². Pierwsza poprawka do Konstytucji USA stanowi fundament pracy dziennikarskiej. Ochroną tego środowiska zajmuje się Freedom of the Press Foundation (FPF), która powstała w 2012 roku.

Organizacją skupiającą się na kwestiach cyfrowych i technologicznych w kontekście praw obywatelskich oraz działaniach na rzecz przejrzystych regulacji dotyczących prywatności w sieci, wolności wypowiedzi i praw konsumentów, jest powstałe w 1994 roku Centrum Demokracji i Technologii (Center for Democracy & Technology, CDT)²³. CDT sprzeciwia się ograniczaniu dostępu do sieci i naruszaniu prywatności ze strony instytucji państwowych. Założona w 1990 roku Electronic Frontier Foundation (EFF) prowadzi działalność promującą prywatność użytkowników oraz wolność wypowiedzi, a także dostęp do technologii (*open source*)²⁴. Interesujące jest to, że organizacja łączy kwestie wolności jednostki z jej bezpieczeństwem, pojmowanym jako wolność od nadzoru instytucji państwa. W tym celu udostępnia materiały szkoleniowe służące wzmacnianiu świadomości technologicznej w zakresie ochrony prywatności w cyberprzestrzeni²⁵.

Wolności jednostki funkcjonującej w cyberprzestrzeni poświęcone są działania organizacji związanych ze środowiskiem akademickim. Uniwersytet Columbia (Columbia University) i John S. and James L. Knight Foundation w 2016 roku powołały Knight First Amendment Institute, którego celem jest badanie i popularyzowanie wolności obywatelskich w zakresie wolności słowa i pierwszej poprawki w cyberprzestrzeni²⁶. Z kolei działające przy Middle Tennessee State University Centrum Wolności Słowa (Free Speech Center, FSC) jako swój główny cel wskazuje popularyzację wiedzy na temat

²² ACLU (2025). <https://www.aclu.org/> [dostęp: 20.02.2025].

²³ *Who We Are?* Center for Democracy & Technology. <https://cdt.org/who-we-are/> [dostęp: 20.02.2025].

²⁴ *About EFF* (2025). EFF. <https://www.eff.org/about> [dostęp: 20.02.2025].

²⁵ *Tools from EFF's Tech Team*. Federal Communications Commission. <https://www.eff.org/pages/tools> [dostęp: 20.02.2025].

²⁶ *About the Knight Institute* (2025). <https://knightcolumbia.org/page/about-the-knight-institute> [dostęp: 20.02.2025].

pierwszej poprawki i Karty praw Stanów Zjednoczonych poprzez edukację, informowanie i angażowanie obywateli²⁷. Szczególny nacisk na działania w środowisku akademickim kładzie Foundation for Individual Rights in Education (FIRE, obecnie Foundation for Individual Rights and Expression), poszerzając zakres działań poza środowisko akademickie²⁸. Jej celem od 1999 roku jest ochrona wolności słowa w przestrzeni akademickiej, a także poza nią. Interesujące są badania FIRE dotyczące praw jednostki w mediach społecznościowych²⁹.

Promujące aktywizm, szczególnie skupiony wokół konkretnych inicjatyw dotyczących wolności w cyberprzestrzeni, organizacje pozarządowe to przede wszystkim założona w 2011 roku Fight for the Future³⁰ oraz Access Now³¹. Pierwsza z nich postrzega cyberprzestrzeń jako dogodną płaszczyznę aktywizmu politycznego, stąd wspiera inicjatywy angażujące użytkowników internetu wokół istotnych społecznie kwestii związanych np. z emancypacją kobiet czy ochroną środowiska naturalnego. Jednym z postulatów aktywizmu internetowego jest wprowadzenie w USA zasad neutralności sieci (*Net Neutrality*). Idea ta dotyczy równego traktowania całego ruchu internetowego przez dostawców internetu (ISP – Internet Service Providers) bez blokowania, spowalniania lub faworyzowania określonych usług, aplikacji czy stron internetowych. Próba zaimplementowania tej idei została przeprowadzona w USA przez Federal Communications Commission (FCC) w 2015 roku, chociaż zasady neutralności sieci sformułowano w tej instytucji jeszcze w 2005 roku. Wyartykułowano wówczas kilka kardynalnych zasad tej idei. Konsumenci mają prawo do: dostępu do legalnych treści internetowych według własnego wyboru; uruchamiania aplikacji i korzystania z usług według własnego wyboru, z zastrzeżeniem potrzeb organów ścigania; podłączania wybranych przez siebie urządzeń, które nie szkodzą sieci; konkurencji między dostawcami sieci, dostawcami aplikacji i usług oraz dostawcami treści³². Według zwolenników neutralności sieci zasada ta promuje wolność słowa, a ponadto uniemożliwia dostawcom usług internetowych uzyskanie uprawnień do regulowania lub zakazywania tego, co ich klienci widzą, do czego mają dostęp

²⁷ *About the Free Speech Center* (2025). <https://firstamendment.mtsu.edu/about-the-free-speech-center/> [dostęp: 20.02.2025].

²⁸ *FIRE Fights for Your Rights*. Foundation for Individual Rights and Expression. <https://www.thefire.org/about-us> [dostęp: 20.02.2025].

²⁹ *FIRE Report on Social Media* (2025). Foundation for Individual Rights and Expression. <https://www.thefire.org/research-learn/fire-report-social-media-2024> [dostęp: 20.02.2025].

³⁰ *Fight for the Future*. <https://www.fightforthefuture.org/> [dostęp: 20.02.2025].

³¹ *Access Now* (2025). <https://www.accessnow.org/> [dostęp: 20.02.2025].

³² *Before the Federal Communications Commission Washington, D.C. 20554* 1. <https://docs.fcc.gov/public/attachments/fcc-05-151a1.pdf> [dostęp: 20.02.2025].

lub co czytają w internecie³³. Zasady wprowadzone przez FCC w 2015 roku zostały już dwa lata później cofnięte. W 2024 roku FCC ponownie podjęła tę kwestię, wprowadzając zasady zgodne z oczekiwaniami użytkowników³⁴.

Polityka mediów społecznościowych (*Social Media Policy*)

W kontekście wolności jednostki do wyrażania opinii interesującą kwestią jest wprowadzanie w sektorze państwowym i prywatnym przez poszczególne podmioty tzw. polityki mediów społecznościowych (*Social Media Policy*). Przyjmowane przez te podmioty polityki dotyczące mediów społecznościowych stanowią katalog zasad postępowania pracowników w cyberprzestrzeni, określający zakazy i nakazy w odniesieniu do wypowiedzi, które w jakikolwiek sposób dotyczyłyby miejsca zatrudnienia. Fundamentalnym celem tworzenia tego typu unormowań jest przede wszystkim troska o kwestie wizerunkowe. Należąca do największych podmiotów gospodarczych w USA firma Walmart³⁵ w swojej polityce dotyczącej mediów społecznościowych wskazuje na dwie kwestie, które dotyczą profili firmowych na Facebooku (Meta), X (dawniej Twitter), YouTube, Instagramie, Snapchacie, LinkedInie i Medium oraz prywatnych profili pracowników³⁶. Podstawową wytyczną dla pracowników jest zakaz ujawniania poufnych informacji biznesowych oraz niewypowiadania się w imieniu Walmartu bez zgody firmy, zwłaszcza że posiada ona „dedykowany zespół, którego zadaniem jest odpowiadanie na zapytania klientów lub krytykę”³⁷. Wszelka krytyka pracowników wobec pracodawcy powinna być kierowana do firmy z wykorzystaniem środków i kanałów specjalnie do tego stworzonych: „(...) zachęcamy do kierowania skarg lub obaw dotyczących pracy lub środowiska pracy do zespołu zarządzającego sklepem za pomocą ustalonego procesu Open Door lub WalmartOne.com”³⁸.

³³ R. Awati, K. Gerwig (2024, 2 maja). *Net neutrality*. TechTarget. <https://www.techtarget.com/searchnetworking/definition/Net-neutrality> [dostęp: 20.02.2025].

³⁴ *Why the FCC's Net Neutrality Rules Were Struck Down, FCC Restores Net Neutrality* (2025, 7 stycznia). Perkins Coie. <https://perkinscoie.com/insights/update/why-fccs-net-neutrality-rules-were-struck-down> [dostęp: 20.02.2025]; *FCC Restores Net Neutrality* (2024). Federal Communications Commission. <https://www.fcc.gov/document/fcc-restores-net-neutrality-0> [dostęp: 20.02.2025].

³⁵ *Largest American companies by market capitalization* (2025). Marketcap. <https://companiesmarketcap.com/usa/largest-companies-in-the-usa-by-market-cap/> [dostęp: 20.02.2025].

³⁶ *Walmart Social Media Policy & Guidelines*. Walmart. <https://www.swaybase.com/social-media-policy-directory/walmart> [dostęp: 20.02.2025].

³⁷ *Ibidem*.

³⁸ *Ibidem*.

Z kolei Intel w swoich zasadach podkreśla rolę osób związanych z tą firmą, stwierdzając, że każda z nich jest „(...) zarówno osobą w najlepszej pozycji, aby powiedzieć światu, dlaczego Intel jest tak niesamowitym miejscem do życia, jak i osobą najlepiej przygotowaną do ochrony Intel przed krzywdą”³⁹. Podstawową zasadą dotyczącą publikowania opinii pracowników w mediach społecznościowych jest podkreślenie, że nie są one opiniami firmy, lecz indywidualnymi poglądami użytkowników. Ponadto wskazuje się, aby nazwy profili w mediach społecznościowych nie zawierały nazwy firmy. W ramach uczciwości w biznesie wskazuje się, by pracownicy powstrzymywali się od krytykowania konkurentów, partnerów biznesowych oraz produktów Intela. Tak jak w innych politykach mediów społecznościowych, kluczową kwestią jest zachowanie poufności. Firma podkreśla: „Komunikacja zewnętrzna nigdy nie powinna zawierać informacji tajnych lub zastrzeżonych, a media społecznościowe nie są wyjątkiem. Nie publikuj informacji tajnych lub zastrzeżonych, w tym informacji oznaczonych jako Intel »Poufne«, »Ścisłe tajne«, »Poufne« lub »Tylko wewnętrzne«”⁴⁰. Stara się również związać pracownika odpowiedzialnością za dobro firmy, zachęcając do reagowania w przypadku niewłaściwego postępowania współpracowników: „Jeśli widzisz, że koledzy lub współpracownicy angażują się w ryzykowne praktyki związane z mediami społecznościowymi, daj nam znać. Wyślij wiadomość e-mail na adres social.media@intel.com i poproś o wskazówki”⁴¹.

Interesujące jest to, że cały tekst związany z wytycznymi polityki w sprawie mediów społecznościowych posiada charakter silnie koncyliacyjny, a jego autorzy często posługują się zwrotami typu „prosimy” czy „wskazujemy”. Mimo to Intel ostrzega, iż monitoruje media społecznościowe, a każdy pracownik ponosi osobistą odpowiedzialność za swoje słowa. W zasadzie tekst ma charakter apelu, a nie groźby. Co więcej, we wstępie Intel zachęca swoich pracowników do aktywności w mediach społecznościowych, jednocześnie apelując o wspieranie wizerunku firmy.

Odmienne styl przekazu prezentuje katalog zasad sformułowany przez Nike, w którym zastosowano sformułowania nakazowe – „nie powinienes” lub „nie używaj”⁴². Pracownik nie powinien upubliczniać informacji dotyczących firmy, w tym danych osobowych, prawnych i poufnych, ani „używać serwisów społecznościowych do jakichkolwiek wewnętrznych lub związanych z pracą działań ani do omawiania poufnych lub zastrzeżonych informacji

³⁹ *Intel Social Media Guidelines*. Intel. <https://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html> [dostęp: 20.02.2025].

⁴⁰ *Ibidem*.

⁴¹ *Ibidem*.

⁴² *Nike Social Media Policy*. Nike. <https://businessnikeassignment.weebly.com/personal--professional.html> [dostęp: 20.02.2025].

korporacyjnych”⁴³. Istotną informacją przekazywaną pracownikom jest uświadomienie, że reprezentują Nike, dlatego uwagi dotyczą konieczności posługiwania się językiem pozbawionym treści obraźliwych. Podobnie jak w przypadku Intela, Nike ostrzega swoich pracowników o monitorowaniu mediów społecznościowych i ponoszeniu odpowiedzialności za własne słowa.

Zasadniczo w treści wstępów do dokumentów zawierających wytyczne dla pracowników firm przyznaje się, że media społecznościowe stanowią istotne miejsce wymiany informacji i kontaktów. Podkreśla się również, że popiera się aktywność w mediach społecznościowych, pod warunkiem że uwzględnia ona troskę o wizerunek firm, w których pracownicy są zatrudnieni.

Zakończenie

Rozwój technologii cyfrowych, poszerzanie możliwości wykorzystywania cyberprzestrzeni, w tym w szczególności mediów społecznościowych oraz systemów informatycznych, niesie ze sobą pozytywne zmiany dotyczące aktywności społecznej jednostek, ale również negatywne – związane z zagrożeniami bezpieczeństwa zarówno jednostek, jak i instytucji państwa. Próby regulowania tej sfery przez państwo, motywowane względami bezpieczeństwa, napotykają jednocześnie na opór części społeczeństwa, dla którego wszelkie regulacje dotyczące sfery cyber stanowią zagrożenie dla praw i wolności człowieka.

Z powyższego wywodu wynika, że wolność człowieka w cyberprzestrzeni, pomimo prób regulowania jej przez państwo, jest w USA bardzo silnie umocowana w zapisach pierwszej poprawki oraz przepisach ustawowych. Potwierdzają to sentencje wyroków Sądu Najwyższego USA w sprawach dotyczących platform społecznościowych. Wskazuje to również na pewną przewagę praw jednostki nad zasadami bezpieczeństwa państwa.

Bibliografia

- 40 states settle Google location-tracking charges for \$392M (2022, 14 listopada). Independent. <https://www.independent.co.uk/news/google-ap-princeton-b2224868.html> [dostęp: 20.02.2025].
- About EFF (2025). EFF. <https://www.eff.org/about> [dostęp: 20.02.2025].
- About the Free Speech Center (2025). <https://firstamendment.mtsu.edu/about-the-free-speech-center/> [dostęp: 20.02.2025].

⁴³ Ibidem.

- About the Knight Institute* (2025). <https://knightcolumbia.org/page/about-the-knight-institute> [dostęp: 20.02.2025].
- Access Now* (2025). <https://www.accessnow.org/> [dostęp: 20.02.2025].
- ACLU* (2025). <https://www.aclu.org/> [dostęp: 20.02.2025].
- Amendment I, Constitution of the United States*. <https://www.senate.gov/about/origins-foundations/senate-and-constitution/constitution.htm> [dostęp: 20.02.2025].
- An Act To prohibit certain individuals from downloading or using TikTok on any device issued by the United States or a government corporation*. Kongres Stanów Zjednoczonych. <https://www.congress.gov/bill/117th-congress/senate-bill/1143> [dostęp: 20.02.2025].
- Application of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok* (2025, 20 stycznia). White House. <https://www.whitehouse.gov/presidential-actions/2025/01/application-of-protecting-americans-from-foreign-adversary-controlled-applications-act-to-tiktok/> [dostęp: 20.02.2025].
- Attorney General Ken Paxton Secures \$1.4 Billion Settlement with Meta Over Its Unauthorized Capture of Personal Biometric Data in Largest Settlement Ever Obtained from An Action Brought by A Single State* (2024, 30 lipca). Texas Office of the Attorney General. <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture> [dostęp: 20.02.2025].
- Awati R., Gerwig K. (2024, 2 maja). *Net neutrality*. TechTarget. <https://www.techtarget.com/searchnetworking/definition/Net-neutrality> [dostęp: 20.02.2025].
- Before the Federal Communications Commission Washington, D.C. 20554 1*. <https://docs.fcc.gov/public/attachments/fcc-05-151a1.pdf> [dostęp: 20.02.2025].
- Bhalla N. (2025, 14 lutego). *US TikTok ban: Which other countries have banned the app?* Context. <https://www.context.news/big-tech/us-tiktok-ban-which-other-countries-have-banned-the-app> [dostęp: 20.02.2025].
- Children's Online Privacy Protection Rule*. The Code of Federal Regulations. <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312> [dostęp: 20.02.2025].
- Commission opens formal proceedings against TikTok on election risks under the Digital Services Act* (2024, 17 grudnia). Komisja Europejska. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487 [dostęp: 20.02.2025].
- Communications Act of 1934*. <https://transition.fcc.gov/Reports/1934new.pdf> [dostęp: 20.02.2025].
- Dwyer D., See P. (2023, 21 lutego). *Family of American terror victim asks Supreme Court to curb immunity for social media*. ABC News. <https://abcnews.go.com/Politics/family-american-terror-victim-asks-supreme-court-curb/story?id=96463560> [dostęp: 20.02.2025].
- FCC Restores Net Neutrality* (2024). Federal Communications Commission. <https://www.fcc.gov/document/fcc-restores-net-neutrality-0> [dostęp: 20.02.2025].
- Fight for the Future*. <https://www.fightforthefuture.org/> [dostęp: 20.02.2025].
- Final Meta Multistate Complaint, N.D. Cal.* (2023). State of California Department of Justice – Office of the Attorney General. <https://oag.ca.gov/system/files/>

- attachments/press-docs/FINAL%20Meta%20Multistate%20Complaint%2C%20N.D.%20Cal.%20%28REDACTED%2C%20CONFORMED%29.pdf [dostęp: 20.02.2025].
- FIRE Fights for Your Rights*. Foundation for Individual Rights and Expression. <https://www.thefire.org/about-us> [dostęp: 20.02.2025].
- FIRE Report on Social Media* (2025). Foundation for Individual Rights and Expression. <https://www.thefire.org/research-learn/fire-report-social-media-2024> [dostęp: 20.02.2025].
- Horowitz J. (2021, 9 marca). *First Amendment, Censorship, and Private Companies: What Does “Free Speech” Really Mean?* Carnegie Library of Pittsburgh. <https://www.carnegielibrary.org/pl/the-first-amendment-and-censorship/> [dostęp: 20.02.2025].
- Intel Social Media Guidelines*. Intel. <https://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html> [dostęp: 20.02.2025].
- Justice Department Sues TikTok and Parent Company ByteDance for Widespread Violations of Children’s Privacy Laws* (2024, 2 sierpnia). U.S. Department of Justice. <https://www.justice.gov/archives/opa/pr/justice-department-sues-tiktok-and-parent-company-bytedance-widespread-violations-childrens> [dostęp: 20.02.2025].
- Kinal J. (2018). *Web 2.0 próba chronologizacji i konceptualizacji zjawiska*. „Przestrzeń Społeczna (Social Space)”, 2 (16), s. 67-80.
- Largest American companies by market capitalization* (2025). Marketcap. <https://companiesmarketcap.com/usa/largest-companies-in-the-usa-by-market-cap/> [dostęp: 20.02.2025].
- Newton C. (2020, 29 grudnia). *Everything you need to know about Section 230*. The Verge. <https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation> [dostęp: 20.02.2025].
- Nike Social Media Policy*. Nike. <https://businessnikeassignment.weebly.com/personal-professional.html> [dostęp: 20.02.2025].
- Obscene, Indecent and Profane Broadcasts* (2021, 13 stycznia). Federal Communications Commission. <https://www.fcc.gov/consumers/guides/obscene-indecent-and-profane-broadcasts> [dostęp: 20.02.2025].
- Packingham v. North Carolina* (2017). Oyez. <https://www.oyez.org/cases/2016/15-1194> [dostęp: 20.02.2025].
- Pequeño A., Roeloffs M.W. (2025, 14 lutego). *TikTok Ban Timeline: TikTok Returns to U.S. App Stores — For Now*. Forbes. <https://www.forbes.com/sites/antoniopequenoiv/2025/02/14/tiktok-ban-timeline-tiktok-returns-to-us-app-stores-for-now/> [dostęp: 20.02.2025].
- Protecting Americans from Foreign Adversary Controlled Applications Act*. Kongres Stanów Zjednoczonych. <https://www.congress.gov/bill/118th-congress/house-bill/7521/text> [dostęp: 20.02.2025].
- TikTok Inc., et al., Petitioners*. Sąd Najwyższy USA. https://www.supremecourt.gov/opinions/24pdf/24-656_ca7d.pdf [dostęp: 20.02.2025].
- Tools from EFF’s Tech Team*. Federal Communications Commission. <https://www.eff.org/pages/tools> [dostęp: 20.02.2025].

- Twitter Inc. v Taamneh et al* (2023). Sąd Najwyższy USA. https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf [dostęp: 20.02.2025].
- Twitter v. Taamneh* (2023). Global Freedom of Expression. <https://globalfreedomofexpression.columbia.edu/cases/twitter-v-taamneh/> [dostęp: 20.02.2025].
- UNITED STATES OF AMERICA, Plaintiff, v. BYTEDANCE LTD., a Cayman Islands company; BYTEDANCE INC., a Delaware corporation; TIKTOK LTD., a Cayman Islands company; TIKTOK INC., a California corporation; TIKTOK PTE. LTD., a Singapore company; and TIKTOK U.S. DATA SECURITY INC., a Delaware corporation.* <https://www.justice.gov/archives/opa/media/1362606/> [dostęp: 20.02.2025].
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.* Kongres Stanów Zjednoczonych. <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm> [dostęp: 20.02.2025].
- Walmart Social Media Policy & Guidelines.* Walmart. <https://www.swaybase.com/social-media-policy-directory/walmart> [dostęp: 20.02.2025].
- Who We Are?* Center for Democracy & Technology. <https://cdt.org/who-we-are/> [dostęp: 20.02.2025].
- Why the FCC's Net Neutrality Rules Were Struck Down, FCC Restores Net Neutrality* (2025, 7 stycznia). Perkins Coie. <https://perkinscoie.com/insights/update/why-fccs-net-neutrality-rules-were-struck-down> [dostęp: 20.02.2025].
- Zahn M. (2024, 6 grudnia). *Federal appeals court rejects TikTok's bid to overturn US ban.* ABC News. <https://abcnews.go.com/Business/tiktok-loses-challenge-law-requiring-sale-ban/story?id=116527211> [dostęp: 20.02.2025].

Streszczenie

Cyberprzestrzeń stanowi dla człowieka obszar, w którym może on realizować swoje społeczne potrzeby, aktywnie uczestniczyć w rzeczywistości wirtualnej jako członek społeczności 2.0. To obszar, który wiąże się nie tylko z realizacją zasad wolności, ale także z zagrożeniami dla bezpieczeństwa zarówno jednostki, jak i państw. W przestrzeni tej szczególnie silnie uwidacznia się dylemat związany z wyborem pomiędzy bezpieczeństwem a wolnością. Istotnym problemem jest wyważenie, w jakim stopniu można ograniczyć wolność w internecie na rzecz bezpieczeństwa, a także jak bardzo można ingerować w cyberprzestrzeń, by – ograniczając wolność użytkowników internetu – chronić inne wartości, takie jak bezpieczeństwo pozostałych użytkowników.

Istotnym zagadnieniem dotyczącym cyberprzestrzeni jest ochrona nie tylko państw, ale i innych podmiotów, w tym gospodarczych. Stąd pojawia się pytanie, jakie regulacje państwo ustanawia w celu kontroli internetu. Wolność wypowiedzi, badań, wyrażania opinii jest gwarantowana konstytucyjnie, lecz konieczne jest społeczne monitorowanie realizacji tego prawa w kontekście rzeczywistości polityczno-społecznej. W związku z tym przedstawiono działalność organizacji oraz ruchów obrony praw i wolności.

Interesującym przykładem szerokiego ujmowania zakresu wolności i bezpieczeństwa jednostki w aspekcie funkcjonowania internetu są Stany Zjednoczone Ameryki Północnej, gdzie podstawą wolności jednostki w cyberprzestrzeni jest pierwsza poprawka do Konstytucji USA. Instytucje państwa, chroniąc jego bezpieczeństwo, wykorzystują możliwości, jakie dają im odpowiednie regulacje do

kontroli i przeciwdziałania zagrożeniom ze strony portali społecznościowych (np. TikTok). Dla podmiotów gospodarczych istotna jest aktywność ich pracowników w przestrzeni mediów społecznościowych.

Celem niniejszego artykułu jest wykazanie, że swobody i wolności jednostki w USA posiadają bardzo silne umocowanie zarówno w zapisach prawa, jak i w praktyce orzeczniczej. Potwierdzeniu tej hipotezy służyła analiza dokumentów i aktów prawnych, takich jak Konstytucja USA, ustawy, regulacje *Social Media Policy* oraz orzeczenia Sądu Najwyższego USA.

The Individual in Cyberspace – Between Freedom and Security. Approaching the Issue in the USA

Abstract

Cyberspace serves as a domain where individuals can fulfill their social needs and actively participate in virtual reality as members of the 2.0 community. This space is not only associated with the principles of freedom but also with security threats, both for individuals and states. In this domain, the dilemma between security and freedom becomes particularly evident. A crucial issue is determining to what extent freedom on the internet can be limited for the sake of security and how much intervention in cyberspace is justified to protect other values, such as the safety of other users.

An essential aspect of cyberspace is the protection not only of states but also of other entities, including economic actors. This raises the question of what regulations governments establish to control the internet and counteract threats. Freedom of speech, research, and opinion is constitutionally guaranteed, yet social oversight of the enforcement of these rights in the political and social reality is necessary. Therefore, the activities of organizations and movements dedicated to defending rights and freedoms are presented.

A particularly interesting example of the broad approach to individual freedom and security in the context of the internet is the United States of America. There, the foundation of individual freedom in cyberspace is the First Amendment to the U.S. Constitution. On the other hand, state institutions, while protecting national security, use regulatory tools to monitor and counter threats posed by social media platforms such as TikTok. For economic entities, the online activity of their employees in social media is also of great importance.

The aim of this article is to demonstrate that individual freedoms and rights in the U.S. are firmly grounded both in legal provisions and in the jurisprudence of the U.S. Supreme Court. This hypothesis is supported by an analysis of legal documents and acts such as the U.S. Constitution, laws, social media regulations, and Supreme Court rulings.

Słowa kluczowe: bezpieczeństwo, cyberprzestrzeń, internet, pierwsza poprawka, prawa i wolności

Keywords: security, cyberspace, internet, First Amendment, rights, and freedoms