
DOI: 10.4467/29567610PIB.25.046.23031

dr Katarzyna Bakalarczyk-Burakowska

ORCID 0000-0002-2649-0779

dr Marcin Mazurek

Akademia Wymiaru Sprawiedliwości,

ORCID 0000-0002-8159-3762

CYBERPRZESTRZEŃ W POLSKIM I MIĘDZYNARODOWYM PORZĄDKU PRAWNYM

CYBERSPACE IN THE POLISH AND INTERNATIONAL LEGAL ORDER

Streszczenie

Przedmiotem badań jest kwestia prawnego uregulowania cyberprzestrzeni w międzynarodowym i polskim prawodawstwie. Problem ten jest aktualny ze względu na dynamiczny rozwój technologii informatycznych i szerokie wykorzystaniem Internetu. W globalnej cyberprzestrzeni nie ma próżni prawnej, ale obecnie nie ma uniwersalnych ram prawnych zarządzania cyberprzestrzenią. Główny problem badawczy sprowadza się do pytania, czy możliwe jest takie uregulowanie prawne aktywności w cyberprzestrzeni, aby było ono satysfakcjonujące dla wszystkich jej użytkowników z punktów widzenia bezpieczeństwa? W poszukiwaniu odpowiedzi na problem badawczy przyjęto metodę badań teoretycznych, a w ich obszarze zastosowano metody kwerendę i analizy dokumentów. Za pomoc tych metod uzyskano dane dotyczące prawnych uwarunkowań, organizacji i funkcjonowania systemu zarządzania bezpieczeństwem informacji w skali globalnej i poszczególnych państwach. Przyjęte metody teoretyczne związane były z: syntezą, analogią, metodami statystycznymi, indukcją i dedukcją. Badania dostarczyły bogatego, aczkolwiek niejednoznacznego materiału. Mnogość istniejących koncepcji na uporządkowanie cyberprzestrzeni rodzi określone konsekwencje – brak jednolitych regulacji w prawie międzynarodowym.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, normy prawne, prawo krajowe, prawo międzynarodowe.

Summary

The subject of this research is the legal regulation of cyberspace in international and Polish law. This issue is relevant due to the dynamic development of information technology and the widespread use of the Internet. There is no legal vacuum in global cyberspace, but there is currently no universal legal framework for cyberspace governance. The main research problem comes down to the question of whether it is possible to legally regulate activities in cyberspace in such a way that it would be satisfactory for all its users from the security point of view?

In seeking an answer to the research problem, a theoretical research approach was adopted, employing query and document analysis. These methods provided data on the legal framework, organization, and operation of information security management systems globally and in individual countries. The theoretical methods employed included synthesis, analogy, statistical methods, induction, and deduction. The research provided rich, albeit ambiguous, evidence. The multitude of existing concepts for organizing cyberspace has specific consequences: a lack of uniform regulations in international law.

Keywords: cyberspace, cybersecurity, legal norms, national law, international law.

Wstęp

Przedmiotem badań, podjętych przez autorów jest kwestia prawnego uregulowania cyberprzestrzeni w międzynarodowym i polskim prawodawstwie. Problem ten jest aktualny ze względu na dynamiczny rozwój technologii informatycznych i szerokie wykorzystaniem Internetu. W globalnej cyberprzestrzeni nie ma próżni prawnej, ale obecnie nie ma uniwersalnych ram prawnych zarządzania cyberprzestrzenią.

Przed badaniami postawiono dwa zasadnicze cele:

1. Poznawczy – zaprezentowanie aktualnych rozwiązań prawnych dotyczących bezpieczeństwa w cyberprzestrzeni podejmowanych przez instytucje w ramach Organizacji Narodów Zjednoczonych (ONZ), regionalne i wyspecjalizowane organizacje międzynarodowe oraz wybrane państwa, w tym Polskę oraz identyfikację szans i zagrożeń wynikających z tych dotychczasowych rozwiązań w kontekście zapewnienia bezpieczeństwa użytkowników cyberprzestrzeni.
2. Utylitarny – wskazanie kierunków optymalnych działań i rozwiązań, które mogłyby przyczynić się podniesienia poziomu bezpieczeństwa w cyberprzestrzeni oraz modyfikacji programów edukacyjnych i audytów realizowanych przez podmioty odpowiedzialne za bezpieczeństwo.

Główny problem badawczy sprowadza się do pytania:

Czy możliwe jest takie uregulowanie prawne aktywności w cyberprzestrzeni, aby było ono satysfakcjonujące dla wszystkich jej użytkowników z punktów widzenia bezpieczeństwa?

Na podstawie wstępnych studiów i analizy dostępnej literatury sformułowano następującą główną hipotezę roboczą:

Bezpieczeństwo w cyberprzestrzeni, pomimo podejmowanych przez państwa i instytucje międzynarodowe intensywnych wysiłków prawno-organizacyjnych, jest wciąż niezadowolające, zaś wdrażane systemy bezpieczeństwa są często niekompletne, obciążone wieloma mankamentami, a w rezultacie nie w pełni chronią prywatność użytkowników.

W poszukiwaniu odpowiedzi na problem badawczy przyjęto metodę badań teoretycznych, a w ich obszarze zastosowano metody: kwerendę i analizy dokumentów. Za pomoc tych metod uzyskano dane dotyczące prawnych uwarunkowań, organizacji i funkcjonowania systemu zarządzania bezpieczeństwem informacji w skali globalnej i poszczególnych państwach. Przyjęte metody teoretyczne związane były z: syntezą, analogią, metodami statystycznymi, indukcją i dedukcją.

Praca składa się z czterech zasadniczych części. W pierwszej części omówiono pojęcie i istotę cyberprzestrzeni wskazując, że mnogość definicji, podejść oraz jej cechy jak m.in. transgraniczność sprawiają, że zagwarantowanie bezpieczeństwa jest dość trudne. W drugiej części pokazano w jaki sposób i w jakim kierunku na przestrzeni ostatnich dekad ewoluowały rozwiązania dotyczące cyberprzestrzeni podejmowane przez instytucje i organizacje międzynarodowe i wybrane państwa. W trzeciej części scharakteryzowano polskie wysiłki ustawodawcze na rzecz uporządkowania działań użytkowników w cyberprzestrzeni i zapewnienia im bezpieczeństwa. W czwartej, ostatniej części podjęto próbę identyfikacji głównych problemów, które uniemożliwiają pełne, satysfakcjonujące, a przede wszystkim uniwersalne rozwiązania prawne, zapewniające bezpieczeństwo w cyberprzestrzeni. Praca kończy się wnioskami wynikającymi z badań.

Pojęcie i istota cyberprzestrzeni

Termin *cyberprzestrzeń* nie ma jednej akceptowanej na całym świecie definicji, chociaż czasami jest utożsamiany z Internetem lub cyfrowym światem wirtualnym. Większość autorów podkreśla, że termin ten został użyty po raz pierwszy w 1984 r. przez pisarza literatury science fiction Williama Gibsona w jego powieści *Neuromancer*¹. Istnieją jednak opinie, że pojęcie cyberprzestrzeni pojawiło się wcześniej, w powieściach Vernora Vinge'ego (*True Names*) oraz Johna M. Forda (*Web of Angels*). Niewątpliwie jednak Gibson spopularyzował

1 W. Gibson, *Neuromancer*, Ace Books, Nowy York 1984.

ten termin najpierw w *Burning Chrome* w 1982 r., a dwa lata później w *Neuromancer*, a zarazem był przedstawicielem nowego nurtu literackiego tzw. cyberpunku².

Paradoksalnie, przy analizie słowa *cyberprzestrzeń* odnotowujemy, że pojęcie, które w potocznym rozumieniu kojarzy z królestwem ostatecznej wolności, jest etymologicznie związane z koniecznością, kontrolą. Słowo to jest bowiem połączeniem dwóch części: pierwsza *cyber*, wywiedziona z cybernetyki, którą można określić jako *porównawcze badanie automatycznej komunikacji i kontroli funkcji żywych ciał oraz systemów mechanicznych i elektrycznych, takich jak komputery*³. Pochodzi od greckiego słowa *kybernētēs*, co można tłumaczyć jako *sternik, sterować*. Drugi człon to *przestrzeń* będąca *tym, w czym ciała materialne mają rozszerzenie* lub *oznacza przedział czasu, odnoszący się do francuskiego *espace*, łacińskiego *spatium* i greckiego *spaein*, czyli rysować. Zatem nawet w korzeniach etymologicznych cyberprzestrzeni mamy do czynienia z ambiwalencją, dotyczącą możliwości i ograniczeń, maszyn i ciał, przestrzeni i czasu⁴.*

Autorzy prac dotyczących cyberprzestrzeni podejmują próby jej definicji z różnych perspektyw. Wydaje się, iż wszystkie wysiłki można podzielić na trzy grupy:

- podejścia techniczne (technologiczne, fizyczne);
- podejścia teoretyczne (społeczne, informacyjne, psychologiczne, filozoficzne);
- podejścia pragmatyczne.

Zwrócić uwagę należy na podejścia pragmatyczne, charakterystyczne dla urzędowych dokumentów, związanych z formułowaniem strategii (polityki) cyberbezpieczeństwa na szczeblu państwa. Pogląd przyjęty w *Strategii Bezpieczeństwa Narodowego Stanów Zjednoczonych Ameryki 2022* nawiązuje do technicznej koncepcji cyberprzestrzeni, umieszczonej w słowniku Departamentu Obrony, traktując cyberprzestrzeń jako jedną z dziedzin zapewniających stabilność i bezpieczeństwo narodu amerykańskiego oraz obronę infrastruktury i instytucji krytycznych dla funkcjonowania kraju przed cyberatakami⁵. W Strategii uwytklono fakt, że jako otwarte społeczeństwo Stany Zjednoczone mają wyraźny interes we wzmacnianiu norm, które łagodzą cyberzagrożenia i zwiększają

2 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, s. 72.

3 D. Lyon, *Beyond Cyberspace: Digital Dreams and Social Bodies*, Information Technology Education and Society, January 2015. https://www.researchgate.net/publication/255609059_Beyond_Cyberspace_Digital_Dreams_and_Social_Bodies/link/54106f3c0cf2f2b29a410b13/download [dostęp: 8.03.2025 r.].

4 Tamże, s. 2.

5 *National Security Strategy*, October 2022, <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf> [dostęp: 11.03.2025 r.].

stabilność w cyberprzestrzeni. Zadeklarowano dalsze propagowanie przestrzegania, zatwierdzonych przez Zgromadzenie Ogólne ONZ, ram odpowiedzialnego zachowania państw w cyberprzestrzeni, które uznają, że prawo międzynarodowe obowiązuje w Internecie tak samo jak poza nim.

Podobnie, ale nieco szerzej, pojęcie cyberprzestrzeni zarysowano w brytyjskiej *Narodowej Strategii Cyberbezpieczeństwa na lata 2016–2021 (National Cyber Security Strategy 2016–2021)* przyjmując, iż jest to *współzależna sieć infrastruktur technologii informacyjnej, która obejmuje Internet, sieci telekomunikacyjne, systemy komputerowe, urządzenia połączone z Internetem oraz wbudowane procesory i kontrolery. Może również odnosić się do wirtualnego świata lub domeny jako doznanej zjawiska lub abstrakcyjnej koncepcji*⁶.

Ogólnie rzecz biorąc, w dokumentacji bezpieczeństwa różnych krajów cyberprzestrzeń jest postrzegana jako przestrzeń zależna od wzajemnie połączonych elementów fizycznych, które tworzą globalną sieć informacyjną. W miarę jak społeczeństwa wkraczają w ten nowy obszar, strategie bezpieczeństwa charakteryzują ją jako przestrzeń kluczową i niezbędną dla bezpieczeństwa i obrony. Dostrzega się jej ponadterytorialność i mnogość aktorów. Cyberprzestrzeń jawi się tu jako fizyczne środowisko, tworzone przez połączenie fizycznych systemów i sieci, zarządzane przez reguły ustalone w oprogramowaniu i protokołach komunikacyjnych.

Reasumując, w ślad za B.P. Medeirossem i L.R.F. Goldonim, można przyjąć, że cyberprzestrzeń to wyjątkowa dziedzina sztucznych interakcji międzyludzkich, częściowo oddzielona od elementów fizycznych, która przenika tradycyjne domeny. Istnieje dzięki połączeniu różnych warstw: technologicznej, technicznej i personalnej. Ma wyjątkowe cechy, które są możliwe dzięki częściowej niematerialności i ekspansywnej wzajemnej łączności. Cyberprzestrzeń nieustannie ewoluuje wraz z postępem technologicznym, zaś korzystający z niej uczestnicy kształtują ją tak, aby spełniała najbardziej zróżnicowane potrzeby⁷.

Istotę cyberprzestrzeni do pewnego stopnia wyraża dwuczłonowość tego określenia: *cyber+przestrzeń*. *Cyber*, jak już wyjaśniono, można tłumaczyć jako kierowanie, sterowanie, pilotowanie, ale w ostatnim czasie opisuje raczej to, co należy do świata cyfrowego, wirtualnego, a więc niematerialnego. Z kolei *przestrzeń* nabiera znaczenia fizycznej materii. Innymi słowy mamy do czynienia z wzajemnym przenikaniem dwóch światów – materialnego i niematerialnego⁸.

Należy podkreślić, iż jeszcze do lat 70. ubiegłego wieku pojęciu *przestrzeń* przypisywano ściśle geometryczne znaczenie, prezentując ją jako pusty obszar.

6 HM Government, *National Cyber Security Strategy 2016–2021*, p. 75; https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/national_cyber_security_strategy.pdf [dostęp: 1.03.2025 r.].

7 B.P. Medeiros, L.R.F. Goldoni, *The Fundamental Conceptual Trinity of Cyberspace*, „ContextoInternacional” vol. 42(1) Jan/Apr 2020, s. 31.

8 A. Cicognani, *On the Linguistic Nature of Cyberspace and Virtual Communities*, *Virtual Reality* 1998, No 3, s. 16–24.

W zastosowaniach naukowych towarzyszyły mu na ogół inne określenie, jak przestrzeń Euklidesa czy przestrzeń nieskończona, a ogólne wrażenie było takie, że pojęcie przestrzeni posiada wyłącznie wymiar matematyczny, prawie nikt nie wspominał o przestrzeni społecznej. Po raz pierwszy francuski socjolog i filozof Henri Lefebvre próbował przedstawić pojęcie przestrzeni za pomocą terminologii nauk społecznych, uważając ideę i koncepcję przestrzeni za otwartą na teorie inne niż matematyczne i przypisał jej charakter materii⁹. H. Lefebvre wyróżniał trzy rodzaje przestrzeni:

- przestrzeń fizyczną – natura, kosmos;
- przestrzeń psychiczną (mentalną), w tym logiczne i formalne abstrakcje;
- przestrzeń społeczną – interakcje społeczne¹⁰.

Żadna z nich nie jest odseparowana od pozostałych, a więc pojedynczo nie wyczerpują opisu pojęcia *przestrzeni* jako takiej. Nie są samodzielne, ale ze sobą powiązane; razem kształtują złożoność natury przestrzeni i jej zmiennych. Według Lefebvre`a, przestrzeni interakcji społecznych nie można traktować jako oddzielonej od natury czy logicznych abstrakcji. To samo można powiedzieć o cyberprzestrzeni – nie możemy uważać, że jest oddzielona od przestrzeni fizycznej, psychicznej czy społecznej.

Cechą, którą uwypuklają niemal wszyscy autorzy, jest deterytorializacja cyberprzestrzeni, co należy rozumieć przemieszczanie się poza terytorium, opuszczanie terytorium. Innym słowy, jest pozbawiona granic i zdecentralizowana, co sprawia, że niemożliwa jest jej tradycyjna kontrola i nadzór. Równocześnie jest ona powszechnie dostępna, a jej charakter jest płynny i elastyczny¹¹.

Analizując istotę cyberprzestrzeni opisywaną w polskich opracowaniach warto odnotować próbę jej usystematyzowania przez M. Lakomego, który wyróżnił zestaw cech cyberprzestrzeni jako nowego wymiaru bezpieczeństwa państw¹²:

- jest to przestrzeń niematerialna, której trudno przypisać atrybuty z tradycyjnego, znanego świata fizycznego; istnieją dwie sytuacje, kiedy cyberprzestrzeń może ujawniać swój materialny charakter, a mianowicie: zniszczenie fizycznej infrastruktury oraz cyberatak, który uszkodzi (zmanipuluje) dane na ściśle określonym komputerze; Jako że komputer posiada przynależność prawną i miejsce terytorialne więc związek między cyberprzestrzenią a wymiarem fizycznym jest oczywisty;

9 Tamże, s. 17.

10 H. Lefebvre, *The construction of space*, Oxford: Blackwell 1991, za: A. Cicognani, *On the Linguistic Nature of Cyberspace and Virtual Communities*, s. 17.

11 P. Podrecki, *Prawo Internetu*, Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2007, s. 20.

12 M. Lakomy, op.cit., s. 85-102.

- w cyberprzestrzeni jest utrudniona identyfikacja sprawców, a więc – co było już szerzej omówione – mamy do czynienia z łatwością zachowania anonimowości, a tym samym bezkarności;
- niskie koszty wejścia i działania w cyberprzestrzeni – uwypukla się ten atrybut w kontekście prowadzonej cyberwojny podkreślając, że skuteczny wrogi atak może przeprowadzić jedna osoba z dostępem do komputera, nie potrzebne są więc ogromne nakłady finansowe na zbrojenia; ta cecha cyberprzestrzeni czyni ją szczególnie atrakcyjną dla terrorystów;
- w cyberprzestrzeni z uwagi na wskazane wcześniej cechy niemożliwe jest stworzenie systemów wczesnego ostrzegania przez atakami;
- w tej domenie, dzięki postępowi rewolucji informatycznej, łatwiej jest manipulować pojedynczymi ludźmi i dużymi grupami społecznymi oraz prowadzić działania propagandowe;
- cyberprzestrzeń znacznie utrudnia realizację współpracy międzynarodowej; wynika to z faktu, iż sieci teleinformatyczne stanowiące tradycyjny kanał komunikacji między państwami mogą być celem ataku, a ponadto ochrona sojuszników w cyberprzestrzeni jest znacznie bardziej skomplikowana; ponadto, podkreśla M. Lakomy, na płaszczyźnie międzynarodowej nie wypracowano powszechnie akceptowanych zasad współpracy i zwalczania cyberzagrożeń;
- cyberprzestrzeń, z punktu widzenia bezpieczeństwa, jest przestrzenią, w której łatwiej prowadzić atak aniżeli defensywę, natomiast trudniej odstraszać przeciwnika w tradycyjnym, militarnym rozumieniu tego określenia.

Podsumowując rozważania o istocie cyberprzestrzeni warto zauważyć, iż domena rozwinęła się wraz z Internetem. Dzięki niej możliwe jest szybkie i sprawne wytwarzanie, gromadzenie, przetwarzane oraz wymiana różnego rodzaju informacji powstających w ramach współpracy zachodzącej między systemami teleinformatycznymi. W przestrzeni wirtualnej możliwe są też wirtualne spotkania¹³. Cyberprzestrzeń to ważny obszar aktywności ludzkiej. Jej transgraniczność sprawia jednak, że zagwarantowanie bezpieczeństwa jest dość trudne. Dodatkowo sytuacji nie ułatwia fakt, iż nie ma wspólnego podejścia w zakresie zapewnienia bezpieczeństwa uregulowanego na poziomie prawa międzynarodowego, mimo przepisów gwarantujących osobom fizycznym możliwość bezpiecznego przetwarzania danych osobowych, zarówno w przestrzeni europejskiej, jak i w przestrzeni międzynarodowej¹⁴.

13 *Bezpieczeństwo infrastruktury krytycznej, wymiar teleinformatyczny*, red. J. Świątkowska, Instytut Kościuszki, Kraków 2014, s. 94.

14 A. Stępień, *Bezpieczeństwo danych osobowych w cyberprzestrzeni - Big Data*, „Przedsiębiorczość i Zarządzanie” 2018, nr 2, s. 50.

Ewolucja regulacji cyberprzestrzeni

Wraz z dynamicznym rozwojem technologii informatycznych i szerokim wykorzystaniem Internetu, kwestia regulacji cyberprzestrzeni staje się coraz poważniejszym światowym problemem. Trzeba przyznać, że w globalnej cyberprzestrzeni nie ma próżni prawnej, ale obecnie nie sposób mówić o istnieniu uniwersalnych ram prawnych zarządzania cyberprzestrzenią. Ogólnie ujmując, obecny proces tworzenia reguł w globalnej cyberprzestrzeni jest kształtowany przez trzy czynniki: powiązane instytucje w ramach Organizacji Narodów Zjednoczonych (ONZ), ustawodawstwo regionalnych i wyspecjalizowanych organizacji międzynarodowych oraz wszelkie inne działania podejmowane przez interesariuszy z różnych krajów.

Organizacja Narodów Zjednoczonych, jak zauważył M. Lakomy, wprawdzie problematyką bezpieczeństwa w cyberprzestrzeni zainteresowała się już w latach 80. XX wieku, ale niemal do końca lat 90. *raczej sporadycznie odnosiła się do wyzwań dla bezpieczeństwa teleinformatycznego, traktując te zagadnienia raczej jako pewną ciekawostkę niż rzeczywisty problem*¹⁵. Sytuacja uległa poprawie na przełomie XX i XXI wieku. W ramach ONZ istnieją cztery główne instytucje, zajmujące się procesem tworzenia przepisów dotyczących cyberprzestrzeni:

- Światowy Szczyt Społeczeństwa Informatycznego (WSIS);
- Grupa Ekspertów Rządowych (GGE) ds. Bezpieczeństwa Informacji;
- Grupa Ekspertów ONZ ds. Zwalczanie Cyberprzestępczości – działająca w ramach Komisji ONZ ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości w Sprawach Karnych (CCPCJ);
- Międzynarodowy Związek Telekomunikacyjny (*International Telecommunication Union - ITU*).

Podsumowując wysiłki ONZ na rzecz uregulowania cyberprzestrzeni należy stwierdzić, iż była jedną z pierwszych organizacji, która podjęła tę kwestię w swoich pracach, odegrała istotną rolę w edukacji i podnoszeniu świadomości społeczeństw na temat zagrożeń, które generuje cyberprzestrzeń. Należy jednak pamiętać, iż ONZ i jej agendy jako takie były zbyt mało decyzyjne, ich aktywność zależała od przyzwolenia, interesów i ambicji poszczególnych państw członkowskich, zwłaszcza wielkich mocarstw.

Do organizacji regionalnych, które zajmują się prawnym uporządkowaniem cyberprzestrzeni należy przede wszystkim zaliczyć Radę Europy i Unię Europejską. Charakteryzując koncepcję regulacji cyberprzestrzeni przez Unię Europejską należy mieć na względzie, iż jej dokumenty normatywne,

15 M. Lakomy, op.cit., s. 335-336.

w przeważającej części odnoszą się do cyberbezpieczeństwa oraz ochrony danych osobowych.

Europejskie uprawnienia regulacyjne, opierają się na traktatach europejskich i założeniu, że wolność jednostki i odpowiedzialność społeczna są równie ważne¹⁶. W ostatnich latach Rada Europy, Rada Europejska, Parlament Europejski i Komisja sformułowały zbiór zasad, które odzwierciedlają ideę społeczeństwa cyfrowego, zorientowanego jednocześnie na jednostkę i dobro wspólne. Dlatego też nowe technologie ocenia się na podstawie tego, czy sprzyjają demokracji i czy ich stosowanie jest zgodne z prawami człowieka. Środki regulacyjne wywołują szanse i zagrożenia związane z technologią, z interesami przedsiębiorstw, konsumentów, państw i społeczeństwa obywatelskiego. Dobrym przykładem takiego podejścia regulacyjnego jest komunikat UE w sprawie sztucznej inteligencji (AI). Sztuczna inteligencja nie jest rozumiana jako cel sam w sobie, ale jako *narzędzie działające w służbie ludzkości i dobra publicznego*¹⁷. W raporcie końcowym grupy ekspertów powołanej przez Komisję i opublikowanej w kwietniu 2019 r. podkreślono potrzebę zachowania ludzkiej niezależności w korzystaniu z AI, unikania krzywdzenia ludzi oraz ogólnego poszanowania zasad sprawiedliwości i zrozumiałości¹⁸.

Pomimo ogólnego europejskiego konsensusu co do potrzeby ścisłego powiązania regulacji cyberprzestrzeni z wolnością rynku, ochroną danych i bezpieczeństwem danych, nadal nie ma zgody co do sposobu pogodzenia krajowych standardów bezpieczeństwa z liberalną logiką rynkową UE¹⁹.

Wraz z łączeniem i przenikaniem się rynków usług cyfrowych, można zaobserwować na całym świecie ewolucję różnych modeli regulujących cyberprzestrzeń. Zachodni model otwartych i liberalnych społeczeństw wydaje się coraz bardziej interoperacyjny z modelem chińskim, który jednak jest podobny do modeli istniejących w Rosji, Iranie i niektórych państwach arabskich, charakteryzujących się autorytarną rejestracją przestrzeni cyfrowej i pretensjami do ich legalizacji na globalną skalę²⁰. Niektóre państwa członkowskie UE już próbują obrać nieliberalne ścieżki regulowania cyberprzestrzeni. Biorąc pod uwagę zasygnalizowane różnice, istotne wydaje się pytanie: Czy Europa powinna trzymać się konsekwentnej polityki suwerenności cyfrowej w tej kwestii? Jeśli odpowiedzieć na nie twierdząco, to w konsekwencji należałoby założyć, iż

16 Art. 2. Traktatu o Unii Europejskiej, Dz. Urz. UE 2016 C 202, s. 1.

17 European Commission, *Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions Artificial Intelligence for Europe*, Brussels, 25.4.2018 COM(2018) 237 final.

18 European Commission, *Expert Group on Liability and New Technologies Formation, Liability for Artificial Intelligence and Other Emerging Digital Technologies*, © European Union, 2019, <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> [dostęp: 7.04.2021 r.].

19 A. Bendiek, M. Schallbruch, *Europe's Third Way in Cyberspace. What Part Does the New EU Cybersecurity Act Play?*, Stiftung Wissenschaft und Politik, 2019, No 52, s. 4, <https://www.swp-berlin.org/10.18449/2019C52/> [dostęp 8.03.2025 r.].

20 Tamże, s. 6.

powinna rozwijać własne mobilne sieci danych 6G, własnego Google, własnego WhatsApp itp. Idea wydaje się na pierwszy rzut oka atrakcyjna, ale długoterminowe konsekwencje strategicznej autonomii cyfrowej mogą być obciążone ryzykiem – zarówno w zakresie polityki innowacyjności, jak i bezpieczeństwa.

UE ma własny zestaw wartości i lokuje je w centrum swojej polityki. Demonstruje swoją suwerenność cyfrową, włączając te wartości do swoich przepisów dotyczących produktów cyfrowych i sposobu ich używania, a także kontrolując i wdrażając innowacje. Jednak dążenie do modelu całkowitej suwerenności cyfrowej grozi konfrontacją, ponieważ koncepcja ta koncentruje się na obronie terytorialnej i protekcjonizmie, a więc paradoksalnie wywołuje zjawiska, które UE programowo zwalcza²¹.

W tym kontekście celem Unii Europejskiej jest połączenie suwerenności cyfrowej ze strategiczną współzależnością. Strategiczna współzależność to koncepcja, która uznaje, że w kontekście globalizacji i cyfryzacji poleganie na bezpieczeństwie zasobów, łańcuchach produkcyjnych i otwartości rynku to tylko część istotnych czynników. Bezpieczeństwa obecnie nie można osiągnąć samodzielnie, ale w wyniku procesu integracji gospodarczej i politycznej oraz rosnącej współzależności. Wzajemne uznawanie certyfikatów bezpieczeństwa, produktów cyfrowych, zastępuje konfrontacyjne granice. Integracja europejska jest najlepszym przykładem tego, jak współzależność przyniosła Europie pokój i stabilność.

Jednak istnieją opinie, że europejskie podejście jest naiwne, a wysokie standardy UE w zakresie ochrony danych i bezpieczeństwa informacji stawiają ją w niekorzystnej sytuacji konkurencyjnej. Stąd dystans Unii do Stanów Zjednoczonych i Chin będzie się zwiększał. Sugeruje się, że konsumenci nie są gotowi płacić za wyższe standardy. Bliższa analiza tych argumentów ujawnia, że nie są w pełni uzasadnione. Po pierwsze, Europa nie jest w stanie wyznaczać własnych standardów, ponieważ standardy nie są ustalane na jej jednolitym rynku, ale na rynku światowym. Po drugie, Stany Zjednoczone i Chiny będą dominować tak długo, jak długo będą oferować produkty o lepszych parametrach. Po trzecie, nie jest prawdą jakoby konsumenci nie chcieli uznawać standardów etycznych za cechę produktu i odpowiednio za nie płacić. RODO pokazało, że Europa jest w stanie samodzielnie wyznaczać wysokie standardy i zapewnić ich stosowanie w całej Europie. Normy europejskie ochrony danych osobowych przejmuje Japonia, dostosowując się do prawa europejskiego, podobnie jak Indie, a od 2020 r. również Brazylia. Dla wielu globalnie działających korporacji bardziej efektywne jest stosowanie regulacji unijnych niż operowanie różnymi standardami na różnych rynkach. Można więc mówić o efekcie brukselskim, który zapewnia że wysokie standardy zastępują niskie.

21 Tamże, s. 6.

Cyberprzestrzeń w polskim porządku prawnym

Polska, podobnie jak większość krajów na świecie, obiektywnie znajduje się w cyberprzestrzeni, rozumianej nie jako ściśle zakreślony fizycznie obszar, ale raczej jako środowisko programowe, które nie sposób opisać za pomocą typowych fizycznych miar, które nie poddaje się podziałowi geograficznemu między państwa. Podkreślić przy tym należy, iż uczestnictwo poszczególnych państw w cyberprzestrzeni nie jest jednakowe, bowiem zależy ono – ujmując w dużym uproszczeniu – od poziomu rozwoju technologii informacyjno-komunikacyjnych, kultury informacyjnej i wielu innych czynników. Teoretycznie można założyć sytuację, w której możliwe jest całkowite, częściowe lub znaczne ograniczenie aktywności instytucji państwa i obywateli w cyberprzestrzeni (niektóre państwa autorytarne podejmują takie wysiłki w praktyce), ale niesie to określone konsekwencje polityczne, gospodarcze i cywilizacyjne.

Efektywne wydzielenie krajowej cyberprzestrzeni możliwe byłoby przez fizyczne wyłączenie się z sieci globalnej, co w konsekwencji kreowałoby zupełnie niezależne od siebie, niekompatybilne krajowe cyberprzestrzenie.

W zasadzie od 2009 r. w polskim prawodawstwie podejmowano próby zdefiniowania czym jest cyberprzestrzeń i zakreślenia jej ram; działania te były powodowane troską o zapewnienie bezpieczeństwa państwa i jego obywateli w tej nowej domenie. Po raz pierwszy pojęciem cyberprzestrzeń posłużono się w przygotowanym pod auspicjami Ministerstwa Spraw Wewnętrznych i Administracji *Rządowym programie ochrony cyberprzestrzeni RP na lata 2009–2011*. Pierwsza ustawowa definicja cyberprzestrzeni została wprowadzona w 2011 r. w ustawie o zmianie ustawy o stanie wojennym²². W tym akcie prawnym zdefiniowano *cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniem i wymianą informacji nimi oraz relacjami z użytkownikami*, odsyłając do ustawy o informatyzacji działalności podmiotów, realizujących zadania publiczne w sprawie definicji systemu teleinformatycznego.

Nie oznacza to, iż cyberprzestrzeń była polskiemu ustawodawcy nieznana. Według J. Przyklenk, która prowadziła badanie sposobów konceptualizacji pojęcia cyberprzestrzeni w polskim dyskursie parlamentarnym, już wcześniej, od 2001 r., w oficjalnych dokumentach, wprawdzie sporadycznie, ale pojawiały się przywołania cyberprzestrzeni *często w kontekście zgłaszanej konieczności przystosowania prawa polskiego do obowiązujących regulacji europejskich (...) bądź w kontekstach luźno związanych z samą sferą cyfrową*²³.

22 Ustawa z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. Nr 222, poz. 1323).

23 J. Przyklenk, *Cyberprzestrzeń w polskim dyskursie parlamentarnym*, „Forum Lingwistyczne” 2020, nr 7, s. 22.

Kolejne dokumenty normatywne (*Rządowy program ochrony cyberprzestrzeni na lata 2011–2016*, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*) w zasadzie powielają takie ujęcie cyberprzestrzeni.

Należy przy tym odnotować próby wyodrębnienia z globalnej cyberprzestrzeni – cyberprzestrzeni Rzeczypospolitej Polskiej. W *Rządowym programie ochrony cyberprzestrzeni RP na lata 2009–2011* cyberprzestrzeń RP zdefiniowano jako *przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa*, natomiast w kolejnej edycji tego programu na lata 2011–2016 za cyberprzestrzeń RP uznano *cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)*²⁴.

Próby wydzielania i zamknięcia w określonych ramach terytorialnych cyberprzestrzeni RP są zrozumiałe z punktu widzenia kreślonych strategii bezpieczeństwa, ale budzą wątpliwości wobec faktu, co do którego zgodni są wszyscy znawcy problematyki, że cyberprzestrzeń nie ma granic terytorialnych, a więc posiada wymiar ponadnarodowy. Pierwsza przytoczona definicja cyberprzestrzeni RP, jak podkreśla J. Wasilewski, wydaje się być całkowicie *nieefektywna z uwagi na brak jakichkolwiek kryteriów, które pozwalałyby na wydzielenie z ogólnoswiatowej cyberprzestrzeni, tylko tych zasobów, których zarząd pozostaje w gestii jednego rządu*²⁵. Druga definicja wprawdzie rozszerza zakres polskiej cyberprzestrzeni o jednostki funkcjonujące poza granicami, ale wprowadzając te pozytywne zmiany, ponownie podjęto próbę fizycznego podziału nie-fizycznej przestrzeni cyfrowej.

W dnia 30 października 2019 r. uchwałą nr 125 Rady Ministrów przyjęto *Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*; tym samym straciła moc uchwała nr 52 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022²⁶. Cyberprzestrzeń w nowej strategii określono jako *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 2070, z późn. zm.)*, wraz z powiązaniem między nimi oraz relacjami z użytkownikami – zgodnie z art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych

24 *Rządowy program ochrony cyberprzestrzeni na lata 2011–2016*, Ministerstwo Spraw Wewnętrznych i Administracji Warszawa czerwiec 2010. Dostępny na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [dostęp: 9.03.2025 r.].

25 J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawne i kryminalistyczne*, Praca doktorska, Wydział Prawa Uniwersytetu w Białymstoku, 2018. s. 64.

26 Monitor Polski z dnia 30 października 2019 r., poz. 1037.

*i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2017 r. poz. 1932)*²⁷. Zmiana po dwóch latach strategii zapewne była podyktowana faktem wejścia w życie w 2018 r. ustawy o krajowym systemie cyberbezpieczeństwa²⁸.

Wydaje się, iż autorzy najnowszej *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024* dostrzegli nieefektywność wysiłków mających na celu wydzielenie odrębnej cyberprzestrzeni RP i nie posługują się tym terminem.

Analizując rozwiązania ustawowe dotyczące regulowania cyberprzestrzeni należy wymienić ustawę z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, chociaż nie zawarto w niej definicji samej cyberprzestrzeni. Ustawa określa natomiast organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu; sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy; zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej²⁹. Ponadto sprecyzowano w niej definicję cyberbezpieczeństwa.

J. Wasilewski analizując polskie podejście do cyberprzestrzeni zwrócił uwagę na najistotniejsze jego cechy³⁰:

- cyberprzestrzeń jest traktowana jako wydzielony logiczny obszar;
- ma charakter ponadnarodowy;
- tworzą ją systemy teleinformatyczne połączone sieciami telekomunikacyjnymi, w tym z sieciami poza granicami kraju;
- działania w cyberprzestrzeni, poza wymianą informacji, mogą obejmować wytwarzanie, modyfikowanie, odczytywanie;
- dwustronne powiązanie działań w cyberprzestrzeni z działaniami w fizycznej rzeczywistości.

Jednocześnie podkreślił, że *cyberprzestrzeń to nie tylko suma fizycznych składników – systemów, sieci, oprogramowania oraz przetwarzanych w nich informacji. To nie proste odwołanie do Internetu – choć niewątpliwie to właśnie Internet jest obecnie ilościowo najistotniejszym składnikiem cyberprzestrzeni, mieszczącym się w każdej omawianej definicji oraz będącym wymienianym wprost w części z nich. Cyberprzestrzeń to również nie suma operacji wykonywanych przez użytkowników w sieciach. Istotę cyberprzestrzeni tworzy koncepcja powołania do życia swojego rodzaju równoległego środowiska, które jest nowym wymiarem dla ludzkich działań*³¹.

27 Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*.

28 Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023 r. poz. 913).

29 Art. 1 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa.

30 J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, nr 9, s. 231.

31 Tamże, s. 231.

W polskim prawodawstwie istnieje szereg aktów prawnych regulujących określone działania w cyberprzestrzeni bądź penalizujących przestępstwa w tej domenie. Nie wchodząc głębiej w materię stricte prawną warto w tym miejscu zaznaczyć, iż polskie ustawodawstwo dość elastycznie i na ogół terminowo reaguje na zmiany, jakie zachodzą w domenie cyfrowej. Interesujące spostrzeżenia o obecności cyberprzestrzeni w debacie publicznej wyartykułowała J. Przyklenk. Po pierwsze, w dyskusjach parlamentarnych, co również przekładało się na stanowione prawo, postrzegana była w kategoriach zagrożenia, ataku, towarzyszył jej kontekst militarny³². Po drugie, z upływem czasu i dynamicznym rozwojem tej domeny następowało przeniesienie zainteresowania państwa z ogólnych prób przybliżenia cyberprzestrzeni do jej skonkretyzowanej specyfikacji³³. Wreszcie, po początkowych próbach przekształcania cyberprzestrzeni li tylko w język aktów prawnych dotyczących bezpieczeństwa narodowego, pojawiły się propozycje i rozwiązania skierowane do uczestników cyberprzestrzeni, obejmujące ich edukację oraz wsparcie w codziennym funkcjonowaniu w świecie cyfrowym. Jednocześnie tej zmianie towarzyszyło zachwianie wiary w możliwość prawnego podporządkowania sobie cyberprzestrzeni, przekonanie o nieszczelności polskich systemów bezpieczeństwa cyfrowego³⁴.

4. Problemy z prawnym uregulowaniem cyberprzestrzeni

Cyberprzestrzeń jest domeną, w której nie ma jednolitych międzynarodowych norm prawnych, regulujących problem jurysdykcji. Jak podkreśla J. Worona *niewielkie szanse na zmianę status quo w najbliższym czasie powodują, że wiele państw rozciąga swoją jurysdykcję na czyny dokonywane w cyberprzestrzeni. Wydaje się, że trend ten będzie się utrzymywał dopóty dopóki nie zostanie przyjęte racjonalne rozstrzygnięcie problemu*³⁵.

Przyczyn takiego stanu rzeczy jest wiele, a niektóre dość oczywiste, jak transgraniczność, zdecentralizowany charakter, elastyczność, anonimowość cyberprzestrzeni – które utrudniają, jeśli nie całkowicie wykluczają, wypracowanie przejrzystych, powszechnie akceptowanych norm prawnych. Wydaje się, iż o wiele istotniejsze są jeszcze dwa uwarunkowania, a mianowicie:

- trend wskazujący, że Internet i technologie informacyjno-komunikacyjne stoją w obliczu trudnych i zniechęcających zmian, w tym demograficznych, technologicznych oraz wyzwań politycznych;

32 J. Przyklenk, *op.cit.*, s. 30.

33 Tamże.

34 Tamże, s. 31.

35 J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Praca doktorska, Wydział Prawa Uniwersytetu Białostockiego, 2017, s. 147.

- Internet i technologie informacyjno-komunikacyjne przeżywają kryzys związany z utratą zaufania oraz umacnianiem się koncepcji suwerennego państwa w cyberprzestrzeni³⁶.

Odnosząc się do pierwszego trendu należy odnotować, że do sieci wkracza coraz więcej krajów chcących mieć wpływ na funkcjonowanie Internetu i jego wartości, a jednocześnie w cyberprzestrzeń wkraczają miliardy ludzi z krajów rozwijających się z własnymi wymaganiami, aspiracjami i oczekiwaniami. Zarówno w krajach rozwiniętych, jak i rozwijających się kierunek rozwoju Internetu w coraz większym stopniu wyznacza nowe pokolenie tzw. milenialsów (*Millennials*), które dorastało w Internecie. Czerpie ono poczucie wolności z Internetu, a nie z samochodów czy innych starszych technologii, które wyzwoliły ich rodziców³⁷. Ci nowi, pełnoprawni obywatele Internetu różnie reagują na postrzegane zagrożenia, takie jak masowa inwigilacja lub cyberataki wojskowe. Dla agencji wywiadowczej lub marketera Facebook jest wspaniałym źródłem informacji, ale dla cyfrowego tubylca może być miejscem prywatnym, jak sypialnia, a nie rodzajem biznesu.

Jeśli chodzi o drugi trend to, paradoksalnie, w miarę jak coraz więcej ludzi korzysta z Internetu, a nowoczesne gospodarki zwiększają swoją zależność od niego – cieszy się coraz mniejszym zaufaniem³⁸. Przyczyny tych obaw i braku zaufania są oczywiste: masowe naruszenia bezpieczeństwa danych, które ujawniają prywatność milionów ludzi; wtargnięcia do nawet najsilniej bronionych miejsc na świecie, takich jak Biały Dom; destrukcyjne ataki na infrastrukturę energetyczną; rewelacje E. Snowdena o masowej inwigilacji obywateli³⁹; powszechne, komercyjne gromadzenie danych osobowych przez firmy o nieprzejrzystych politykach prywatności.

Utrata zaufania jest trudna do odrobienia, ponieważ cyberprzestrzeń i Internet nie mają rozwiniętej struktury zarządzania, a to, co mają, znajduje się w ogniu krytyki. Kraje wyznające inne wartości niż amerykańscy twórcy Internetu chcą mieć wpływ na to, jaki powinien być Internet, jakie wartości powinien wzmacniać i jak powinien działać. Czasy, kiedy rządy narodowe pozostawały w tej kwestii względnie bezczynne, minęły. Internet nie jest już miejscem bez granic, ponieważ państwa utrzymują, że suwerenność ma znaczenie i popierają zarówno dyplomację i siłę w cyberprzestrzeni – jak

36 J. Healey, *A Nonstate Strategy for Saving Cyberspace*, *A Nonstate Strategy for Saving Cyberspace*, Atlantic Council, Strategy Paper, January 2017, s. 11–12.

37 L. Bershidsky, *Millennials Want Apps, Not Cars*, BloombergView, July 15, 2014, <http://www.bloombergview.com/articles/2014-07-15/millennials-want-apps-not-cars> [dostęp: 15.03.2025 r.].

38 J. Healey, op.cit., s. 12.

39 W czerwcu 2013 r. Edward Snowden, formalnie pracownik firmy konsultingowej Booz Allen Hamilton, w rzeczywistości pracujący dla oddziału Narodowej Agencji Bezpieczeństwa (NSA) na Hawajach w rozmowie z reporterem brytyjskiej gazety „The Guardian” w Hong Kongu ujawnił informacje o nielegalnej działalności inwigilacyjnej NSA wobec obywateli USA, państw i organizacji i osób za granicą.

zamykanie szkodliwych blogerów, pornografów internetowych lub hackerów, którzy łamią lokalne prawa lub obyczaje. Ten nacisk państw na suwerenność może powstrzymać Internet przed naturalnym rozwojem, przez narzucanie mu sztucznych granic państwowych. Konsekwencją może być to, że zamiast jednej sieci międzynarodowej Internet może się przekształcić w twór, który będzie bardziej przypominał krajowe sieci kolejowe lub telefoniczne, łączące oddzielne wyspy, z których każda jest ściśle kontrolowana przez rząd narodowy⁴⁰.

We współczesnej międzynarodowej debacie o cyberprzestrzeni i cyberbezpieczeństwie kluczowego znaczenia nabiera koncepcja odpowiedzialnego zachowania państwa⁴¹. Termin ten został wprowadzony do problematyki międzynarodowego cyberbezpieczeństwa w 2013 r. w – przytaczanym wcześniej – raporcie Grupy Ekspertów Rządowych ONZ (UNGGE)⁴². Szybko rozprzestrzenił się dzięki licznym oświadczeniom rządowym. Paryski Apel o Zaufanie i Bezpieczeństwo w Cyberprzestrzeni 2018 (*The 2018 Paris Call for Trust and Security in Cyberspace*) zachęcał do szerokiej akceptacji i wdrażania międzynarodowych norm odpowiedzialnego zachowania, a także środków budowy zaufania w cyberprzestrzeni⁴³.

Praktyka dopiero pokaże czym dokładnie jest odpowiedzialne zachowanie państwa i jaki jest jego związek z prawem międzynarodowym. Europa może dać mocny przykład, bowiem państwa europejskie utrzymują wyższe standardy zachowania. W związku z tym odpowiedzialne zachowanie państwa można interpretować jako najlepsze praktyki prawa międzynarodowego. Koncepcja odpowiedzialnego zachowania państwa może również stać się najgorszą praktyką prawa międzynarodowego, jeśli będzie określać minimum tego, co zgodnie z prawem można przyjąć jako dopuszczalną praktykę. W tym drugim przypadku akcent na dobrowolność może być rozumiany jako próba odrzucenia możliwości zastosowania niektórych międzynarodowych norm i standardów w kontekście partykularnych interesów narodowych związanych z technologiami informacyjno-komunikacyjnymi⁴⁴.

Kluczową kwestią dotyczącą wytyczenia norm prawa międzynarodowego w odniesieniu do cyberprzestrzeni jest to, gdzie powinna przebiegać granica między tym, co należy uzgodnić między państwami, a tym, co powinno się pozostawić do jednostronnej interpretacji każdego państwa. Przykładem może być tu zasada suwerenności państwa. Ma ona wiele wymiarów, bowiem sama natura suwerenności nie została rozstrzygnięta: podczas gdy niektóre

40 J. Healey, op.cit, s. 13.

41 E. Tikk, *International Law in Cyberspace: Mind the gap*, Cyber Policy Institute, March 2020, s. 6.

42 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, General Assembly UN, A68/98, June 24, 2013.

43 *Paris Call for Trust and Security in Cyberspace*, 2018, <https://pariscall.international/en/> [dostęp: 12.03.2025 r.].

44 E. Tikk, op.cit., s. 8.

państwa i uczeni uważają ją za zasadę, inni traktują ją jako regułę prawa międzynarodowego⁴⁵. Na przykład Francja niedawno zdefiniowała suwerenność jako regułę prawa międzynarodowego, podczas gdy Wielka Brytania uważa ją tylko za zasadę. Nie ma też zgody co do zakresu tej zasady, czyli tego, co stanowi suwerenność państwa w cyberprzestrzeni. Ponadto istnieje wiele podejść do naruszenia suwerenności terytorialnej w wyniku operacji cybernetycznych. Przebijają się trzy główne poglądy na tę kwestię:

- wszelkie operacje cybernetyczne przenikające do obcego systemu mogą stanowić naruszenie suwerenności; jest to podejście francuskie, ale można traktować jako stanowisko państw o absolutystycznej interpretacji suwerenności;
- cyberoperacja przenikająca do obcego systemu stanowi naruszenie suwerenności tylko wtedy, gdy wyrządza szkody; jest to podejście przyjęte w Tallin Manual 2.0 i przez Stany Zjednoczone⁴⁶;
- suwerenność terytorialna nie może zostać naruszona przez operację cybernetyczną, chyba że stanowi ona naruszenie zasady nieinterwencji; takie jest na przykład podejście brytyjskie.

Ten przykład niewątpliwie pokazuje różne podejście państw i naukowców do określonej normy prawa międzynarodowego. Jednak co ważne, stawia również pytanie o zdolność prawa międzynarodowego do regulowania wszelkich działań, w tym wrogich, w cyberprzestrzeni. Wobec braku przepisów i norm prawa międzynarodowego odnoszących się do cyberprzestrzeni, argumenty na temat dowolnego artykułu Karty Narodów Zjednoczonych stają się jego subiektywną oceną, a nie jego szczególnego zastosowania w cyberprzestrzeni.

Warto zaznaczyć, iż stosowanie prawa międzynarodowego i zasad prawnych w cyberprzestrzeni to temat, który wywołuje zamieszanie, wątpliwości i niekończące się dyskusje między prawnikami od momentu pojawienia się Internetu i jego internacjonalizacji. Debata na temat tego, czy cyberprzestrzeń stanowi całkowicie nową dziedzinę, która wymaga fundamentalnie innych praw, ujawnia podstawowe podziały ideologiczne⁴⁷. Z jednej strony społeczność euroatlantycka kierowana przez Stany Zjednoczone uważa, ogólnie rzecz biorąc, że działania w cyberprzestrzeni nie wymagają nowych przepisów, a istniejące regulacje prawne są wystarczające. Z drugiej strony wiele innych państw, na czele Rosją i Chinami, ma przekonanie, że nowe międzynarodowe instrumenty prawne są niezbędne do zarządzania ogólnym bezpieczeństwem informacji,

45 Tamże, s. 9.

46 Tallin Manual 2.0 to eksperckie opracowanie dotyczące stosowania prawa międzynarodowego do cyberwojny i cyberkonfliktów. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press 2017, wyd. II.

47 K. Giles, *Prospects for The Rule of Law in Cyberspace*, Strategic Studies Institute, U.S. Army War College, January 2017, s. 1.

w tym w dynamicznie zmieniającej się cyberprzestrzeni. Obecny stan regulacji w cyberprzestrzeni oceniany jest przez liczne analogie. Domenę porównuje się do początków kształtowania się przepisów drogowych czy prawa morskiego. W każdym z tych przypadków normy oparte na zaufaniu przekształciły się w zwyczaje, a ostatecznie zostały skodyfikowane jako prawo. Rosja twierdzi, że wyzwania, jakie stwarza cyberprzestrzeń, są zbyt pilne, aby czekać na rozwój prawa zwyczajowego, tak jak miało to miejsce w innych dziedzinach; zamiast tego potrzebne są pilne działania.

Warto więc skupić się na kwestii potrzeby bądź braku potrzeby nowego traktatu dotyczącego zarządzania cyberprzestrzenią. Obecny trend w dwustronnym i regionalnym wdrażaniu środków budowy zaufania, ustanawiania norm i definiowania zagrożeń przyczynia się niewątpliwie do zwiększenia bezpieczeństwa cybernetycznego. Jednak nie wpływa to zasadniczo na fundamentalne rozbieżności w koncepcjach cyberbezpieczeństwa między wspólnotą euroatlantycką a państwami takimi jak Rosja i Chiny. Chociaż w pewnym stopniu można temu zaradzić, likwidując duże różnice interpretacji podstawowych pojęć cyberzagrożeń w umowach dwustronnych między Rosją i Chinami z takimi samymi umowami zawartymi z państwami zachodnimi, to pozostaje faktem, że rozbieżność pojęciowa sprzyja nieporozumieniom. Dla przykładu różnice w interpretacji tego, co stanowi wrogie działanie w cyberprzestrzeni, budzą obawy, bowiem jakiś kraj może uważać, że jest w konflikcie z innym, podczas gdy ów inny jest tego nieświadomy⁴⁸.

Pozostając przy kwestiach kontrowersyjnych warto zwrócić uwagę, iż przy negocjacjach i dyskusjach o kształcie cyberprzestrzeni dochodzi do zderzenia dwóch wartości: suwerenności państwa i praw obywateli. Zasady i przepisy wypracowane w drodze negocjacji między państwami mogą być nadużywane przez reżimy autorytarne do tłumienia aspiracji własnych społeczeństw i pozbawiania ich prywatności oraz innych praw człowieka. Ustanowienie zobowiązań do przestrzegania prawa międzynarodowego przewiduje również nadzór państwowy i jurysdykcję nad terytorium krajowym, co może niestety umacniać źle rozumianą suwerenność. Stąd każde porozumienie międzynarodowe powinno zakładać i taką sytuację, że formułowane w nim postulaty o wzmożonej kontroli nad złośliwymi działaniami może dać państwom narodowym władzę do prześladowania obywateli w Internecie. Postrzeganie przez Rosję, Chiny i podobnie zarządzane państwa, nieograniczonego przepływu informacji i opinii – zwłaszcza za pośrednictwem mediów społecznościowych – jako zagrożenia dla bezpieczeństwa, powoduje ich ciągłe wysiłki na rzecz ograniczenia wolności wypowiedzi w Internecie. Ich dążenie do totalnego uregulowania bezpieczeństwa informacji, a zwłaszcza przekonywanie in-

48 Tamże, s. 31.

nych krajów do wspierania ich inicjatyw, stanowią wyzwanie dla wolności w Internecie. Stąd, ogólnie ujmując, konieczne jest opieranie się działaniom Rosji, Chin i innych krajów zmierzających do wprowadzenia przepisów, które wymuszałyby kontrolę treści⁴⁹.

Istotną przeszkodą na drodze budowy kompleksowego porozumienia i zaufania w cyberprzestrzeni jest zjawisko, które określa się niekiedy bałkanizacją lub rozszczepieniem Internetu⁵⁰. Ujawnienie przez Edwarda Snowdena procedury masowego gromadzenia danych przez Stany Zjednoczone, a także szkody, jakie ów procedur wniósł dla bezpieczeństwa narodowego USA i sojuszników, wzmocniły argumenty za suwerennością w cyberprzestrzeni i koncepcją, którą przyjęły m.in. Rosja, Chiny, tzn. narodową przestrzeń informacyjną. Decyzja Europejskiego Trybunału Sprawiedliwości z września 2015 r. o zakończeniu porozumienia tzw. bezpiecznej przystani (*Safe Harbor Agreement*) stanowi ważny precedens w tym procesie. Brak zaufania do firm amerykańskich i rządu USA w zakresie przechowywania danych obywateli zmusił kraje europejskie do rozwiązania umowy ze Stanami Zjednoczonymi w sprawie przechowywania danych⁵¹. Wprawdzie ich decyzja została przedstawiona jako pozytywna dla obywateli UE, to stanowiła również precedens dla dalszej bałkanizacji Internetu. W konsekwencji o suwerenność i kontrolę nad cyberprzestrzenią zabiegają rządy niedemokratyczne.

Dążenie do decentralizacji globalnego Internetu nie jest wszak powszechne. W Brazylii, po głośnych protestach, odrzucono propozycję ustawodawstwa nakazującego przechowywanie wszystkich danych sieciowych na terytorium kraju. Firmy, jak np. Google utrzymywały, że musiałyby dokonać kosztownych inwestycji w centra serwerów na terytorium Brazylii. Istniało więc paradoksalnie niebezpieczeństwo, że inne korporacje całkowicie zrezygnują z działalności w Brazylii, nieumyślnie ograniczając jeszcze bardziej wolność w Internecie⁵². Rosja nie miała jednak takich obiekcji i skorzystała z okazji, aby wprowadzić środki bezpieczeństwa osobowego w ustawodawstwie, mającym na celu zapobieganie naruszeniom w krajowej przestrzeni informacyjnej. Przepisy dotyczące lokalizacji danych w Rosji weszły w życie 1 września 2015 r.⁵³.

49 Tamże, s. 32.

50 Tamże, s. 33.

51 M. Bauer, *EU-US Safe Harbour and forced data localisation: lessons from Russia*, EurActiv, October 18, 2015, <https://www.euractiv.com/section/justice-home-affairs/opinion/eu-us-safe-harbour-and-forced-data-localisation-lessons-from-russia/> [dostęp: 15.03.2025 r.]. Umowa Safe Harbor była zbiorem zasad regulujących wymianę danych między Stanami Zjednoczonymi Ameryki a Unią Europejską (i Szwajcarią). W dniu 6 października 2015 r. Europejski Trybunał Sprawiedliwości orzekł jej nieważność. Orzeczenie doprowadziło do utworzenia Tarczy Prywatności UE-USA (*UE-US Privacy Shield*).

52 A. Boadle, *Brazil to drop local data storage rule in Internet bill*, Reuters, March 18, 2014. <https://www.reuters.com/article/uk-brazil-internet/brazil-to-drop-local-data-storage-rule-in-internet-bill-idUKBREA2I04320140319> [dostęp: 15.03.2025 r.].

53 K. Giles, *Prospects for The Rule of Law in Cyberspace*, s. 33.

Podjęcie kluczowych państwowych graczy do międzynarodowej legitymizacji lub zakazu działalności w cyberprzestrzeni dostarcza ważnych wskazówek dotyczących tego, jak postrzegają tę aktywność w kontekście własnych zachowań. Zróżnicowane postawy wobec tego, co jest, a co nie jest prawnie dopuszczalne w tej domenie, prowadzi do wniosku, iż potencjalni przeciwnicy kształtują swój potencjał w cyberprzestrzeni w zupełnie inny sposób, nade wszystko mentalny i kulturowy. Inaczej czynią to Rosja i Chiny, zgoła odmiennie od Stanów Zjednoczonych i jej zachodnich sojuszników. Oprócz sporu w sprawie nowych przepisów, w międzynarodowej dyskusji istnieje fundamentalny rozłam na temat tego, co dokładnie powinno stanowić nielegalne zachowanie w cyberprzestrzeni. Rosyjska i chińska polityka bezpieczeństwa informacji wyraża holistyczne podejście do przeciwdziałania zagrożeniom informacyjnym, w szczególności przez rozpoznanie problemu szkodliwych treści. Chociaż demokracje zachodnie prezentują liberalny pogląd na cyberprzestrzeń, to należy zaznaczyć, że jego podstawowe założenie, a mianowicie, że wolność słowa i swobodny przepływ informacji w Internecie jest świętością, zostało w niektórych kręgach zakwestionowane w obliczu niewłaściwego wykorzystywania tych wartości przez Rosję, Chiny czy Państwo Islamskie.

Podsumowanie

Analiza poglądów na regulację oraz wykorzystanie cyberprzestrzeni dostarcza bogatego, aczkolwiek niejednoznacznego materiału. Mnogość koncepcji rodzi określone konsekwencje – brak jednolitych regulacji cyberprzestrzeni w prawie międzynarodowym. Z drugiej strony postulat stworzenia jakiegoś jednego (może kilku) rozwiązania prawnego, chociaż pozornie atrakcyjny i nośny, wcale nie jest taki oczywisty dla wszystkich uczestników cyberprzestrzeni, zwłaszcza państwowych. Dialog pomiędzy rządami jest zdominowany przez silnie obecne interesy polityczne, a zatem brakuje mu szczegółów i obszaru kompromisu. Ponadto nie ma zgody co do tego, gdzie winna przebiegać granica między tym, co należy uzgodnić między państwami, a tym, co powinno się pozostawić do jednostronnej interpretacji każdego z nich. Wreszcie nie wszystkie państwa są przekonane co do potrzeby ustanowienia jakichś jednolitych, uniwersalnych uregulowań prawnych.

Niezależnie od stanowisk poszczególnych państw, istnieją dodatkowe trudności z prawnym ujarzmieniem cyberprzestrzeni – obiektywne i subiektywne. Do tych pierwszych należałoby zaliczyć immanentne cechy cyberprzestrzeni, które nie sposób wykorzenić, a więc transgraniczność, niematerialność, zdecentralizowany charakter, anonimowość itp. Subiektywne to zjawiska, które występują z różnym natężeniem i ewoluują. Należą do nich rosnące aspiracje wolnościowe nowego pokolenia, które dorastało w Internecie, „przynależy” do

świata cyfrowego, traktuje go jako oazę swojej prywatności i czerpie z niego poczucie wolności. Z drugiej strony cyberprzestrzeń, ściślej Internet, cieszy się coraz mniejszym zaufaniem. Wynika to m.in. z masowego naruszenia bezpieczeństwa danych, destrukcyjnych ataków hackerskich na instytucje, infrastrukturę krytyczną i ludzi, z masowej inwigilacji obywateli przez państwa. To sprzeczne zjawiska, ale paradoksalnie mocno z sobą powiązane.

W cyberprzestrzeni dochodzi do zderzenia podstawowych wartości: suwerenności państwa i jego bezpieczeństwa z prawami człowieka, zwłaszcza prawem do wolności, ale także bezpieczeństwa państwa z prawem obywateli do zachowania prywatności. Te konflikty będą przedmiotem dalszych rozważań, ale w tym miejscu należy zasygnalizować kilka ich aspektów. Odnosząc się do pierwszego zderzenia, należy zaznaczyć, że wypracowane w dobrej wierze porozumienia międzynarodowe mogą być wykorzystywane przez niedemokratyczne rządy do tłumienia aspiracji wolnościowych własnych społeczeństw i pozbawiania ich prywatności oraz innych praw człowieka.

Jeśli chodzi o drugi rodzaj konfliktu (bezpieczeństwo vs. prywatność) to wynika on z faktu, iż wszechobecnie technologie głęboko zintegrowały się z codziennym życiem. W rezultacie, w coraz większym stopniu polegamy na cyberprzestrzeni w zakresie interakcji społecznych, gospodarczych i politycznych. Sieć stanowi platformę dla całego szeregu krytycznych sektorów i usług, takich jak opieka zdrowotna, żywność i woda, finanse, technologie informacyjne i komunikacyjne, bezpieczeństwo publiczne, energia i usługi komunalne, produkcja, transport i administracja. Jednocześnie cyberprzestrzeń podlega w coraz większym stopniu wyrafinowanym i ukierunkowanym zagrożeniom; nasze rosnące uzależnienie od cyberprzestrzeni naraża prywatność, stwarza nowe i znaczące luki w zabezpieczeniach. Państwo w imię bezpieczeństwa, pragnąc przeciwdziałać tym zagrożeniom, chcąc też chronić obywateli przed terroryzmem i innymi rodzajami przestępstw, proponuje programy masowej inwigilacji jako środka przykrego, ale – w jego ocenie – koniecznego do zapewnienia szeroko pojmowanego bezpieczeństwa. Jednak w gruncie rzeczy jest to niczym innym niż ograniczeniem prawnych mechanizmów ochrony prywatności. Warto więc w dalszym toku badań dokonać oceny, czy działania władz publicznych w cyberprzestrzeni sprzyjają ochronie prywatności, w tym bezpieczeństwu danych osobowych, czy też są dla niej największym zagrożeniem.

Bibliografia

1. Bendiek A., Schallbruch M., *Europe's Third Way in Cyberspace. What Part Does the New EU Cybersecurity Act Play?*, „Stiftung Wissenschaft und Politik” 2019, No 52.
2. Cicognani A., *On the Linguistic Nature of Cyberspace and Virtual Communities*, “Virtual Reality” 1998, No 3.
3. Gibson W., *Neuromancer*, Ace Books, Nowy York 1984.
4. Giles K., *Prospects for The Rule of Law in Cyberspace*, Strategic Studies Institute, U.S. Army War College, January 2017.
5. Healey J., *A Nonstate Strategy for Saving Cyberspace*, Atlantic Council, Strategy Paper, January 2017.
6. Medeiros B.P., Goldoni L.R.F., *The Fundamental Conceptual Trinity of Cyberspace*, „ContextoInternacional” vol. 42(1) Jan/Apr 2020, s. 31–54.
7. Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
8. Lefebvre H., *The construction of space*, Oxford: Blackwell 1991.
9. Lyon D., *Beyond Cyberspace: Digital Dreams and Social Bodies*, Information Technology Education and Society, January 2015.
10. Przyklenk J., *Cyberprzestrzeń w polskim dyskursie parlamentarnym*, „Forum Lingwistyczne” 2020, nr 7.
11. Podrecki P., *Prawo Internetu*, Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2007.
12. Stępień A., *Bezpieczeństwo danych osobowych w cyberprzestrzeni – Big Data*, „Przedsiębiorczość i Zarządzanie” 2018, nr 2.
13. Świątkowska J., (red.), *Bezpieczeństwo infrastruktury krytycznej, wymiar teleinformatyczny*, Instytut Kościuszki, Kraków 2014.
14. Tikk E., *International Law in Cyberspace: Mind the gap*, Cyber Policy Institute, March 2020.
15. Wasilewski J., *Cyberprzestępczość – wybrane aspekty prawnekarne i kryminalistyczne*, Praca doktorska, Wydział Prawa Uniwersytetu w Białymstoku, 2018.
16. Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, nr 9, s. 231.
17. Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Praca doktorska, Wydział Prawa Uniwersytetu Białostockiego, 2017.
18. Worona J., *Cyberprzestrzeń a prawo międzynarodowe: status quo i perspektywy*, Wolters Kluwer, Warszawa 2020.
19. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press 2017, wyd. II.

Akty prawne

1. Traktat o Unii Europejskiej, Dz. Urz. UE 2016 C 202
2. Ustawa z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. Nr 222, poz. 1323).
3. Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023 r. poz. 913).

Raporty i dokumenty instytucjonalne

1. European Commission, *Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions Artificial Intelligence for Europe*, Brussels, 25.4.2018 COM(2018) 237 final.
2. European Commission, *Expert Group on Liability and New Technologies Formation, Liability for Artificial Intelligence and Other Emerging Digital Technologies*, European Union, 2019,
3. HM Government, *National Cyber Security Strategy 2016–2021*.
4. Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*.
5. *National Security Strategy*, October 2022,
6. *Rządowy program ochrony cyberprzestrzeni na lata 2011–2016*, Ministerstwo Spraw Wewnętrznych i Administracji Warszawa czerwiec 2010.
7. *Paris Call for Trust and Security in Cyberspace*, 2018,

Netografia

1. M. Bauer, *EU-US Safe Harbour and forced data localisation: lessons from Russia*, EurActiv, October 18, 2015, <https://www.euractiv.com/section/justice-home-affairs/opinion/eu-us-safe-harbour-and-forced-data-localisation-lessons-from-russia/> [dostęp: 15.03.2025 r.].
2. L. Bershidsky, *Millennials Want Apps, Not Cars*, BloombergView, July 15, 2014, <http://www.bloombergview.com/articles/2014-07-15/millennials-want-apps-not-cars> [dostęp: 15.03.2025 r.].
3. A. Boadle, *Brazil to drop local data storage rule in Internet bill*, Reuters, March 18, 2014. <https://www.reuters.com/article/uk-brazil-internet/brazil-to-drop-local-data-storage-rule-in-internet-bill-idUKBREA2I04320140319> [dostęp: 15.04.2025 r.].
4. https://www.researchgate.net/publication/255609059_Beyond_Cyberspace_Digital_Dreams_and_Social_Bodies/link/54106f3c0cf2f2b29a410b13/download [dostęp: 8.03.2025 r.].