Kamil Strzępek[1]

Cyberbezpieczeństwo Rzeczypospolitej Polskiej – podstawy prawne (międzynarodowe i krajowe)

Streszczenie

W związku z brakiem międzynarodowego konsensusu co do statusu prawnego cyberprzestrzeni, państwa skupiły się na regionalnej współpracy, dotyczącej przede wszystkim tzw. cyberbezpieczeństwa i jest to w tej chwili główny obszar regulacyjny cyberprzestrzeni. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 i 2022/2555 można uznać za wyraz idei solidarności cyfrowej państw członkowskich UE. Służą one urzeczywistnieniu celu jakim jest (bezpieczne) funkcjonowanie rynku wewnętrznego UE, wyrównują poziom wiedzy w poszczególnych państwach członkowskich z zakresu cyberbezpieczeństwa, stanowią podstawę przepisów krajowych dotyczących cyberbezpieczeństwa. Warto jednak wspomnieć, że określone w art. 5 i 26 Konstytucji RP zadania Sił Zbrojnych, m.in. ochrona niepodległości państwa i niepodzielności jego terytorium, są w Rzeczypospolitej Polskiej realizowane także przez Wojska Obrony Cyberprzestrzeni.

Słowa kluczowe

Cyberprzestrzeń, cyberbezpieczeństwo, Dyrektywy Parlamentu Europejskiego i Rady (UE), Konstytucja RP, Wojska Obrony Cyberprzestrzeni.

1. Wstęp

Uważa się, że termin „cyberprzestrzeń" pojawił się po raz pierwszy w fikcji, tj. w powieści *Neuromancer* Williama Gibsona z 1984 roku[2]. Termin ten można by uznać za „nieszczęśliwy", gdyż w powieści tej kojarzy się z wizją korporacyjnej hegemonii, inżynierii genetycznej, życia w paranoi i bólu, ale w rzeczywistości jest to termin, który nadaje nazwę nowemu etapowi, nowemu i nieodpartemu rozwojowi ludzkiej kultury i biznesu spod znaku technologii[3]. Oprócz tego, że po upływie 40 lat z terminem „cyberprzestrzeń" możemy spotkać się nie tylko w literaturze, ale i np. w kinie, termin ten objęty jest już także zakresem prawa.

---

[1] Dr Kamil Strzępek, adiunkt w Katedrze Prawa Dyplomatycznego i Dyplomacji Publicznej, Instytut Nauk Prawnych Uniwersytetu Kardynała Stefana Wyszyńskiego.

[2] Tak np. M. Benedikt, Cyberspace: First Steps, 1992, s. 1; M. Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, 2015, s. 72.

[3] M. Benedikt, *op. cit.*, s. 1.

Celem niniejszego tekstu jest ukazanie funkcjonujących w prawie międzynarodowym publicznym koncepcji prawnych cyberprzestrzeni oraz tego jak organizacje międzynarodowe (w szczególności ONZ i UE) dążą do zapewnienia cyberbezpieczeństwa swoich członków i jakie ma to przełożenie na ustawodawstwo Rzeczypospolitej Polskiej.

2. Koncepcje prawne cyberprzestrzeni

John P. Barlow, opisując cyberprzestrzeń, stwierdził: „Tworzymy świat, w którym każdy i wszędzie może wyrażać swoje przekonania, bez względu na to, jak bardzo są one osobliwe, bez obawy, że zostanie zmuszony do milczenia lub konformizmu. Wasze prawne koncepcje własności, ekspresji, tożsamości, przemieszczania i kontekstu nie mają do nas zastosowania. Wszystkie opierają się na materii, a tutaj nie ma materii”[4]. John P. Barlow uznawany był za zwolennika poglądu o suwerenności cyberprzestrzeni. Jego pogląd oparty był na dwóch zasadniczych założeniach. Po pierwsze, że cyberprzestrzeń różni się od rzeczywistych przestrzeni: jej aterytorialny, bezgraniczny i wszechobecny charakter odróżnia ją od fizycznych i ograniczonych przestrzeni, które podlegają regulacji prawnej[5]. Po drugie, że cyberprzestrzeń, wierna swojej pierwotnej koncepcji i projektowi, powinna pozostać przestrzenią otwartą, zdecentralizowaną i partycypacyjną, nieskrępowaną regulacjami prawnymi[6].

Pogląd, że cyberprzestrzeń jest objęta zakresem prawa, nie podlega już dyskusji. Niemniej jednak nadal nie ma wypracowanej uniwersalnej koncepcji cyberprzestrzeni w prawie międzynarodowym. Wyróżnić można jedynie pewne „podejścia” do kwestii cyberprzestrzeni prezentowane na poziomie ONZ i innych organizacji międzynarodowych, w tym Unii Europejskiej i Rady Europy.

W raporcie z 22 lipca 2015 r. Grupy Ekspertów Rządowych ds. rozwoju sytuacji w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego[7] stwierdzono m.in., że prawo międzynarodowe, w szczególności Karta Narodów Zjednoczonych, ma zastosowanie i jest niezbędne do utrzymania pokoju i stabilności oraz promowania otwartego, bez-

[4] J. P. Barlow, A Declaration of the Independence of Cyberspace https://www.eff.org/pl/cyberspace–independence (dostęp: 6 maja 2023 r.). W. Gibson tak opisywał cyberprzestrzeń: „Cyberprzestrzeń. Konsensualna halucynacja, doświadczana codziennie przez miliardy legalnych operatorów, w każdym narodzie, przez dzieci nauczane pojęć matematycznych… Graficzna reprezentacja danych pobranych z banków pamięci każdego komputera w systemie człowieka. Niewyobrażalna złożoność”, W. Gibson, Neuromancer, 1992, s. 69.

[5] N. Tsagourias, The legal status of cyberspace, (w:) N. Tsagourias, R. Buchan (red.), Research Handbook on International Law and Cyberspace, 2015, s. 13.

[6] *Ibidem*.

[7] Grupa została powołana na podstawie rezolucji Zgromadzenia Ogólnego ONZ z dnia 27 grudnia 2013 r. nr 68/243 dotyczącej rozwoju w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego.

piecznego, stabilnego, dostępnego i pokojowego środowiska technologii informacyjno-telekomunikacyjnych[8].

W raporcie z dnia 14 lipca 2021 r. Grupy Ekspertów Rządowych ds. kształtowania odpowiedzialnych zachowań państw w cyberprzestrzeni w kontekście bezpieczeństwa międzynarodowego[9] stwierdzono m.in., że zgodnie z celami ONZ, w tym z celem dotyczącym utrzymania międzynarodowego pokoju i bezpieczeństwa, państwa powinny współpracować w opracowywaniu i stosowaniu środków zwiększających stabilność i bezpieczeństwo korzystania z technologii informacyjno-komunikacyjnych oraz w celu zapobiegania praktykom, które zostały uznane za szkodliwe lub mogące stanowić zagrożenie dla zagrożenia dla międzynarodowego pokoju i bezpieczeństwa[10].

Wśród poglądów zaprezentowanych w doktrynie[11], dotyczących sposobu regulacji cyberprzestrzeni, wyróżnić można: te, które opowiadają się za instytucjonalizacją i przyjęciem międzynarodowych norm prawnych regulujących cyberprzestrzeń (w oparciu o konsensus międzynarodowy); te, które wskazują, że tylko państwa, jako podstawowe podmioty prawa międzynarodowego, mogą podejmować wysiłki w celu stworzenia niezbędnych uniwersalnych norm regulujących cyberprzestrzeń (w dużej mierze definiowanych przez interesy narodowe na szczeblu państwowym)[12]; te, które odmawiają stosowania jakichkolwiek norm w cyberprzestrzeni, odwołując się przy tym do wolności w Internecie (suwerenność cyberprzestrzeni)[13].

Wydaje się, iż obecnie przeważa pogląd zgodnie z którym prawo międzynarodowe nie zabrania państwu regulowania swojego „segmentu" cyberinfrastruktury (głównie chodzi o tzw. cyberbezpieczeństwo), aczkolwiek prawo to powinno być realizowane z uwzględnieniem zasad prawa międzynarodowego[14]. Wobec

[8] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 lipca 2015 r., A/70/174. Warto zauważyć, że organizacje wyspecjalizowane i jednostki pomocnicze ONZ generalnie nie używają terminu „cyberprzestrzeń" kiedy omawiają problemy związane z cyberprzestrzenią, ale raczej zwraca się uwagę na wykorzystanie tzw. technologii informacyjno-komunikacyjnych.

[9] Grupa została powołana na podstawie rezolucji Zgromadzenia Ogólnego ONZ z dnia 18 grudnia 2018 r. nr 73/266 dotyczącej kształtowania odpowiedzialnego zachowania państwa w cyberprzestrzeni w kontekście bezpieczeństwa międzynarodowego.

[10] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14 lipca 2021 r., A/76/135.

[11] Zob. taką klasyfikację poglądów zaproponowaną przez T.S. Wu, Cyberspace Sovereignty? – The Internet and The International System, Harvard Journal of Law and Technology 1997, nr 10.3, s. 648 i n. Za nim tak samo K. A. Ivanova, M. Zh. Myltykbaev, D. D. Shtodina, The Concept of Cyberspace in International Law, Law Enforcement Review 2022, nr 6.4, s. 37 i n.

[12] Np. J. A. Lewis, Sovereignty and the Role of Government in Cyberspace, The Brown Journal of World Affairs 2010, nr 16.2, s. 55 i n.

[13] Np. J. P. Barlow, *op. cit*., a ogólniej środowisko związane z Electronic Frontier Foundation.

[14] K. A. Ivanova, M. Zh. Myltykbaev, D. D. Shtodina, *op. cit*., s. 36. Podobnie K. Chałubińska-Jentkiewicz, Operations in Cyberspace vs Human Rights and Freedoms, Polish Political Yearbook 2022, nr 5, s. 2.

jednak braku międzynarodowego, powszechnego konsensusu w odniesieniu do statusu prawnego cyberprzestrzeni, państwa zmierzają w stronę regionalnej współpracy dotyczącej przede wszystkim cyberbezpieczeństwa i jest to w tej chwili główny obszar regulacyjny cyberprzestrzeni. Na najbardziej podstawowym poziomie cyberbezpieczeństwo można rozumieć jako: 1) poufność – zapewnienie, że informacji nie uzyska nikt niepowołany; 2) integralność – zagwarantowanie, że informacje nie będą zmieniały swej formy w sposób nieautoryzowany; 3) dostępność zagwarantowanie, że nie zostanie utracona możliwość korzystania z systemów, danych, informacji, zasobów[15].

3. Przepisy w Unii Europejskiej

W Unii Europejskiej przyjęto (wciąż jeszcze obowiązującą[16]) dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[17] (dalej „dyrektywa 2016/1148").

Dyrektywa ta m.in.:

– ustanowiła obowiązek dla wszystkich państw członkowskich UE przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych[18];
– powołała grupę współpracy, aby wspierać i ułatwiać strategiczną współpracę i wymianę informacji między państwami członkowskimi UE oraz rozwijać wśród nich zaufanie i pewność;

[15] Tak Ł. O l e j n i k, A. K u r a s i ń s k i, Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny, 2022, s. 25. Zob. też definicję opracowaną przez Międzynarodowy Związek Telekomunikacyjny (*International Telecomunication Union*): Cyberbezpieczeństwo to zbiór narzędzi, polityk, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, podejść do zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, gwarancji i technologii, które można wykorzystać do ochrony tzw. cyberśrodowiska, organizacji i zasobów użytkowników. Organizacja i zasoby użytkowników obejmują połączone urządzenia komputerowe, personel, infrastrukturę, aplikacje, usługi, systemy telekomunikacyjne oraz całość przesyłanych i/lub przechowywanych informacji w środowisku cybernetycznym. Cyberbezpieczeństwo dąży do zapewnienia osiągnięcia i utrzymania właściwości bezpieczeństwa organizacji i aktywów użytkowników przed odpowiednimi zagrożeniami bezpieczeństwa w cyberśrodowisku. Ogólne cele bezpieczeństwa obejmują: dostępność; integralność, która może obejmować autentyczność i niezaprzeczalność; poufność. Definicja opracowana przez Międzynarodowy Związek Telekomunikacyjny (*International Telecomunication Union*) https://www.itu.int/en/ITU–T/studygroups/com17/Pages/cybersecurity.aspx (dostęp: 6 maja 2023 r.).

[16] Zgodnie z art. 44 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2): „Dyrektywa (UE) 2016/1148 traci moc ze skutkiem od dnia 18 października 2024 r."

[17] Dziennik Urzędowy UE L 194/1 z dnia 19 lipca 2016 r.

[18] Zob. Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M. P. z 2019 r., poz. 1037).

– powołała sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (tzw. sieć CSIRT[19]);
– ustanowiła obowiązki dla państw członkowskich dotyczące wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz CSIRT mających zadania związane z bezpieczeństwem sieci i systemów informatycznych.

Podstawę prawną dyrektywy 2016/1148 stanowił art. 114 Traktatu o Funkcjonowaniu Unii Europejskiej[20], który umożliwia Parlamentowi Europejskiemu i Radzie przyjmowanie środków dotyczących zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które mają na celu ustanowienie i funkcjonowanie rynku wewnętrznego.

W aspekcie koncepcyjnym warto zwrócić uwagę na rodzaj aktu prawnego w którym – na poziomie Unii Europejskiej – uregulowano ww. kwestie. Dyrektywa, jako akt prawny, wiąże tylko państwa członkowskie do których jest adresowana i tylko w zakresie celów (rezultatu) jakie są w niej wskazane[21]. Z dokonanego wyboru formy prawnej, w której uregulowano ww. kwestie wynika, że Unia Europejska pozostawia organom państwa członkowskiego swobodę w doborze form i metod realizacji celów. Powstaje pytanie o ogólną koncepcję cyberprzestrzeni przyjętą na poziomie Unii Europejskiej. Z jednej strony dyrektywa 2016/1148 ustanawia (wciąż jeszcze) „(…) środki, mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii (…)”[22]. Wynika stąd, że dyrektywa 2016/1148 realizuje cel Unii Europejskiej. Skoro celem tym jest osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii Europejskiej, to znaczy, że w zakresie tego celu, w zakresie regulowanych zagadnień, przyjęto – na poziomie Unii Europejskiej – koncepcję wspólnej cyberprzestrzeni unijnej. W tym kontekście warto zwrócić też uwagę na art. 18. dyrektywy 2016/1148, który stanowi, że: „1. Na potrzeby niniejszej dyrektywy uznaje się, że dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym posiada główną jednostkę organizacyjną. Uznaje się, że dostawca usług cyfrowych posiada główną jednostkę organizacyjną w państwie członkowskim, gdy ma siedzibę zarządu w tym państwie członkowskim (…)”. Zgodnie z motywem 64. przyjęcia dyrektywy 2016/1148: „Jurysdykcję w odniesieniu do dostawców usług cyfrowych należy powierzyć tylko jednemu państwu członkowskiemu, w którym dany dostawca usług cyfrowych ma główną jednostkę organizacyjną w Unii, co z zasady odpowiada miejscu, gdzie dostawca usług ma siedzibę zarządu w Unii (…).” Z drugiej strony, zgodnie z motywem 8. przyjęcia dyrektywy 2016/1148: „Niniejsza dyrektywa

[19] Ang. *Computer Security Incident Response Teams*.
[20] Dziennik Urzędowy UE C 326 z dnia 26 października 2012 r.
[21] A. W r ó b e l, Stosowanie Prawa Unii Europejskiej przez sądy, tom I, Warszawa 2010, s. 64.
[22] Art. 1 dyrektywy 2016/1148.

pozostaje bez uszczerbku dla możliwości podjęcia przez każde z państw członkowskich środków niezbędnych do zapewnienia ochrony podstawowych interesów jego bezpieczeństwa, do ochrony porządku publicznego i bezpieczeństwa publicznego oraz do umożliwienia prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw (…)". Ww. fragment można uznać za wyraz zasady terytorialności, zgodnie z którą jurysdykcja państwa w odniesieniu do „przestępstw komputerowych" występuje, gdy dane przestępstwo popełnione jest na terytorium państwa.

W 2022 roku przyjęto Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148[23] (dalej „dyrektywa 2022/2555).

Dyrektywa 2022/2555 stanowi m.in. odpowiedź na fakt, iż wymogi w zakresie cyberbezpieczeństwa nałożone (w oparciu o dyrektywę 2016/1148) na podmioty świadczące usługi lub prowadzące działalność kluczową z ekonomicznego punktu widzenia różnią się znacznie – swoim rodzajem i poziomem szczegółowości, a także metodami nadzoru – w zależności od państwa członkowskiego[24]. Celem dyrektywy 2022/2555 jest m.in. wyeliminowanie takich rozbieżności między państwami członkowskimi, w szczególności przez określenie przepisów minimalnych dotyczących funkcjonowania skoordynowanych ram regulacyjnych i ustanowienie mechanizmów skutecznej współpracy między odpowiedzialnymi organami w poszczególnych państwach członkowskich.

Dyrektywa 2016/1148 niewątpliwie zapoczątkowała okres wzmożonych prac w obszarze regulacji cyberbezpieczeństwa w Unii Europejskiej[25]. Dyrektywa 2022/2555 eliminuje rozbieżności między państwami członkowskimi powstałe w związku z implementacją dyrektywy 2016/1148. Będą zapewne kolejne tego typu akty[26].

W omawianym aspekcie koncepcyjnym warto zwrócić uwagę, że w odniesieniu do kwestii jurysdykcji, dyrektywa 2022/2555 rozwija znacząco postanowienia dyrektywy 2016/1148. Przyjmuje ona ogólną zasadę, zgodnie z którą: „1. Podmioty objęte zakresem stosowania niniejszej dyrektywy uznaje się za podlegające jurysdykcji państwa członkowskiego, w którym mają miejsce prowadzenia działalności, z następującymi wyjątkami: a) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej uznaje się za podlegających jurysdykcji państwa

[23] Dziennik Urzędowy UE L 333/80 z dnia 27 grudnia 2022 r.
[24] Zob. np. Ł. O l e j n i k, A. K u r a s i ń s k i, *op. cit*., s. 119 i zawarte tam uwagi dotyczące obowiązku zgłaszania zajść cyberbezpieczeństwa.
[25] Zob. G. S z p o r, The Evolution of Cybersecurity Regulation in the European Union Law and its Implementation in Poland, Review of European and Comparative Law 2021, XLVI.3, s. 234.
[26] Zob. np. prace nad Aktem w sprawie cyberodporności (CRS).

członkowskiego, w którym świadczą usługi; b) dostawców usług DNS, rejestry nazw TLD, podmioty świadczące usługi rejestracji nazw domen, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, a także dostawców internetowych platform handlowych, wyszukiwarek internetowych lub platform usług sieci społecznościowych uznaje się za podlegających jurysdykcji państwa członkowskiego, w której mają główne miejsce prowadzenia działalności w Unii zgodnie z ust. 2; c) podmioty administracji publicznej uznaje się za podlegające jurysdykcji państwa członkowskiego, które je ustanowiło”[27].

W kontekście cyberprzestrzeni, państwa członkowskie UE rozróżniają aspekty wewnętrzne i zewnętrzne suwerenności. Niektóre z państw odwołują się do ogólnych zasad, tj. np. zasady terytorialności i skutku spowodowanego na ich terytorium (stanowisko Niemiec i Czech)[28]. Francja, Finlandia i Estonia pozostawiają sobie furtkę do rozważań o swojej jurysdykcji nad zdarzeniami mającymi miejsce poza ich terytorium[29]. Niewątpliwie kwestia suwerenności państwa, jego jurysdykcji, stanowi jedną z najważniejszych – także w kontekście rozważań o cyberbezpieczeństwie na poziomie Unii Europejskiej.

Aktem, o którym nie można zapomnieć, omawiając podstawy prawne regulacji w zakresie cyberbezpieczeństwa, jest też Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.[30]

4. Przepisy krajowe

Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[31] (dalej: ustawa KSC) wdrożyła dyrektywę 2016/1148 i tym samym stanowi kompleksowe uregulowanie krajowego systemu cyberbezpieczeństwa[32]. Podstawowym założeniem ustawy KSC jest współpraca podmiotów, które w ramach swojej działalności zajmują się reagowaniem na tzw. Incydenty Bezpieczeństwa Komputerowego, zarówno ze sobą jak i z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym ds. informatyzacji oraz Pełnomocnikiem ds. Cyberbezpieczeństwa, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym,

[27] Art. 26 dyrektywy 2022/2555.
[28] A.-M. Osula, A. Kasper, A. Kajander, EU Common position on international law and cyberspace, Masaryk University Journal of Law and Technology 2022, vol. 16, s. 97.
[29] *Ibidem*.
[30] Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r., poz. 728).
[31] Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (tekst jedn. Dz. U. z 2022 r., poz. 1863, 2666). Zob. też akty wykonawcze do ustawy KSC, które były niezbędne do pełnego wdrożenia dyrektywy 2016/1148.
[32] Krajowy system cyberbezpieczeństwa obejmuje swoim zakresem podmioty wskazane w art. 4 ustawy KSC.

realizując przy tym zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów[33].

W ustawie KSC znalazła się definicja pojęcia cyberbezpieczeństwo, zgodnie z którą, jest to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność danych lub związanych z nimi usług oferowanych przez te systemy. Definicja ta odpowiada definicjom formułowanym w doktrynie i tej opracowanej przez Międzynarodowy Związek Telekomunikacyjny (*International Telecomunication Union*) i nawiązuje do ogólnych celów cyberbezpieczeństwa, tj. poufności, integralności i dostępności. Ponadto, ustawa KSC określiła podmioty, które w ramach swojej działalności zajmują się reagowaniem na Incydenty[34] Bezpieczeństwa Komputerowego i są to: 1) CSIRT[35] GOV, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego; 2) CSIRT MON, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej; 3) CSIRT NASK, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Omawiając zagadnienie cyberbezpieczeństwa Rzeczypospolitej Polskiej nie można pominąć zadań Sił Zbrojnych RP. Wskazuje się[36], że Siły Zbrojne są tą częścią aparatu państwowego, na którą ustrojodawca nałożył szczególne obowiązki związane z realizacją zadań państwa określonych w art. 5 i 26 Konstytucji RP[37]. W Strategii Cyberbezpieczeństwa RP na lata 2019–2024 możemy przeczytać m.in., że: „Siły Zbrojne Rzeczypospolitej Polskiej, jako podstawowy element systemu obronnego państwa, powinny angażować się w działania w cyberprzestrzeni na tym samym poziomie co w powietrzu, na lądzie i na morzu, zarówno w czasie pokoju, wojny, jak i w sytuacji

[33] Zob. M. T o u m i, Zmiany w strukturze centralnej administracji publicznej w świetle ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r., Przegląd Prawa Konstytucyjnego 2021, nr 60.2, s. 331. Tam też szczegółowa analiza przepisów ustawy KSC.

[34] Pojęcie Incydentu także zostało zdefiniowane w omawianej ustawie KSC (art. 2 ustawy KSC).

[35] Zgodnie z terminologią przyjętą w dyrektywie 2016/1148 zostały one określone jako CSIRT (ang. *Computer Security Incident Response Teams*).

[36] Zob. np. B. B a n a s z a k, Konstytucja Rzeczypospolitej Polskiej. Komentarz, 2012, s. 192.

[37] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r., Nr 78 poz. 483 ze zm.). Art. 5 Konstytucji RP: „Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju". Art. 26 Konstytucji RP: „1. Siły Zbrojne Rzeczypospolitej Polskiej służą ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic. 2. Siły Zbrojne zachowują neutralność w sprawach politycznych oraz podlegają cywilnej i demokratycznej kontroli".

kryzysowej”[38]. W art. 15 ust. 4 pkt 2 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny[39] wskazano m.in., że Wojska Obrony Cyberprzestrzeni jako specjalistyczny komponent Sił Zbrojnych są właściwe do realizacji pełnego spektrum działań w cyberprzestrzeni, w szczególności w zakresie proaktywnej ochrony oraz aktywnej obrony elementów i zasobów cyberprzestrzeni kluczowych z punktu widzenia Sił Zbrojnych.

Niewątpliwie przemyślaną jest uwaga, że sam fakt posiadania aktu prawnego o siłach zbrojnych w cyberprzestrzeni, stanowi o tym, iż państwo uznaje swoją suwerenność w cyberprzestrzeni[40].

5. Podsumowanie

W związku z brakiem międzynarodowego konsensusu co do statusu prawnego cyberprzestrzeni, państwa skupiły się na regionalnej współpracy, dotyczącej przede wszystkim tzw. cyberbezpieczeństwa i jest to w tej chwili główny obszar regulacyjny cyberprzestrzeni. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 i 2022/2555 można uznać za wyraz idei solidarności cyfrowej państw członkowskich UE. Służą one urzeczywistnieniu celu jakim jest (bezpieczne) funkcjonowanie rynku wewnętrznego UE, wyrównują poziom wiedzy w poszczególnych państwach członkowskich z zakresu cyberbezpieczeństwa, stanowią podstawę przepisów krajowych dotyczących cyberbezpieczeństwa. Nie ma jednak jednolitego stanowiska państw członkowskich UE na temat zakresu ich jurysdykcji w cyberprzestrzeni w kontekście cyberbezpieczeństwa. Jest to podstawowa kwestia, a jej istotność ukazują także ewoluujące postanowienia dyrektyw 2016/1148 i 2022/2555. Być może próbą wyjścia z impasu mogłoby być przyjęcie określonej koncepcji – w pierwszej kolejności – w odniesieniu do granic cyberprzestrzeni albo ich braku. Następnie, dyrektywy unijne mogłyby dotyczyć przede wszystkim zagadnień odnoszących się do zagadnień z elementem „transgranicznym” (np. współpraca między państwami). Dopiero po takim określeniu ram koncepcyjnych możliwe jest ewentualne rozwijanie postanowień regulacji.

Określone w art. 5 i 26 Konstytucji RP zadania Sił Zbrojnych, m.in. ochrona niepodległości państwa i niepodzielności jego terytorium, są w Rzeczypospolitej Polskiej realizowane także przez Wojska Obrony Cyberprzestrzeni. Warto zwrócić uwagę, że w ww. przepisach określono obowiązki spoczywające na państwie. Jeśli jednak państwo ma być odpowiedzialne za

[38] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M .P. 2019 r., poz. 1037), s. 19.

[39] Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (tekst jedn. Dz. U. z 2022 r., poz. 2305 ze zm.).

[40] B. F a n, Cyberspace Sovereignty. Reflections on Building a Community of Common Future in Cyberspace, Springer 2018, s. 115.

realizację tych obowiązków, to musi być zdolne do ich wykonywania, w tym posiadać możliwość działania w sferach objętych przedmiotem regulacji.

Bibliografia

Literatura

1. Banaszak, B., Konstytucja Rzeczypospolitej Polskiej. Komentarz, Wydawnictwo C. H. Beck 2012.
2. Benedikt M., Cyberspace: First Steps, The MIT Press 1992.
3. Chałubińska-Jentkiewicz K., Operations in Cyberspace vs Human Rights and Freedoms, Polish Political Yearbook 2022, tom 5, s. 1–14.
4. Fan B., Cyberspace Sovereignty. Reflections on Building a Community of Common Future in Cyberspace, Springer 2018.
5. Gibson W., Neuromancer, Wydawnictwo Książnica 1992.
6. Ivanova K. A., Myltykbaev M. Zh., Shtodina D. D., The Concept of Cyberspace in International Law, Law Enforcement Review 2022, nr 6.4, s. 32–44.
7. Lakomy M., Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Wydawnictwo Uniwersytetu Śląskiego 2015.
8. Lewis J. A., Sovereignty and the Role of Government in Cyberspace, The Brown Journal of World Affairs 2010, nr 16.2, s. 55–65.
9. Olejnik Ł., Kurasiński A., Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny, PWN 2022.
10. Osula A.-M., Kasper A., Kajander A., EU Common position on international law and cyberspace, Masaryk University Journal of Law and Technology 2022, vol. 16, s. 89–123.
11. Szpor G., The Evolution of Cybersecurity Regulation in the European Union Law and its Implementation in Poland, Review of European and Comparative Law 2021, nr XLVI.3, s. 219–235.
12. Toumi M., Zmiany w strukturze centralnej administracji publicznej w świetle ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r., Przegląd Prawa Konstytucyjnego 2021, nr 60.2, s. 325–339.
13. Tsagourias N., The legal status of cyberspace, (w:) N. Tsagourias, R. Buchan (red.), Research Handbook on International Law and Cyberspace, Edward Elgar 2015.
14. Wróbel A., Stosowanie Prawa Unii Europejskiej przez sądy, tom I, Warszawa 2010.
15. Wu T.S., Cyberspace Sovereignty? – The Internet and The International System, Harvard Journal of Law and Technology 1997, nr 10.3, s. 647–666.

Akty prawne

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r., Nr 78 poz. 483 ze zm.).

2. Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (tekst jedn. Dz. U. z 2022 r., poz. 1863, 2666).
3. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (tekst jedn. Dz. U. z 2022 r., poz. 2305 ze zm.).
4. Traktat o Funkcjonowaniu Unii Europejskiej (Dziennik Urzędowy UE C 326 z dnia 26 października 2012 r.).
5. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dziennik Urzędowy UE L 194/1 z dnia 19 lipca 2016 r.).
6. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dziennik Urzędowy UE L 333/80 z dnia 27 grudnia 2022 r.).
7. Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r., poz. 728).

Dokumenty elektroniczne

1. Barlow J. P., A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation, https://www.eff.org/pl/cyberspace–independence (dostęp: 6 maja 2023 r.).
2. Międzynarodowy Związek Telekomunikacyjny (International Telecomunication Union), definicja pojęcia cyberbezpieczeństwo https://www.itu.int/en/ITU–T/studygroups/com17/Pages/cybersecurity.aspx (dostęp: 6 maja 2023 r.).

Pozostałe

1. Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, (M. P. z 2019 r., poz. 1037).
2. Rezolucja Zgromadzenia Ogólnego ONZ z dnia 27 grudnia 2013 r. dotycząca rozwoju w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego 68/243.
3. Rezolucja Zgromadzenia Ogólnego ONZ z dnia 18 grudnia 2018 r. dotycząca kształtowania odpowiedzialnego zachowania państwa w cyberprzestrzeni w kontekście bezpieczeństwa międzynarodowego 73/266.
4. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 lipca 2015 r., A/70/174.

5. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14 lipca 2021 r., A/76/135.

Cybersecurity of the Republic of Poland: (international and domestic) legal framework

Abstract

In the absence of an international consensus on the legal status of cyberspace, states have focused on regional cooperation for cybersecurity that has become a primary area of regulatory efforts for cyberspace. Directives 2016/1148 and 2022/2555 of the European Parliament and of the Council (EU) may be considered a manifestation of the idea of cyber solidarity among the EU Member States. The Directives are to meet the goal of the (secure) functioning of the EU internal market, to align the cybersecurity knowledge across Member States, and to form the basis for national cyber legislation. However, what is noteworthy is that the Armed Forces' tasks set out in Articles 5 and 26 of the Polish Constitution, including without limitation the safeguarding of the independence and integrity of Poland's territory, are also performed by the Cyberspace Defence Forces in the Republic of Poland.

Key words

Cyberspace, cyber security, European Parliament and Council (EU) Directives, Polish Constitution, Cyber Defense Forces.